ISSN 2676-9042

Vol 4, No 2, 2022.

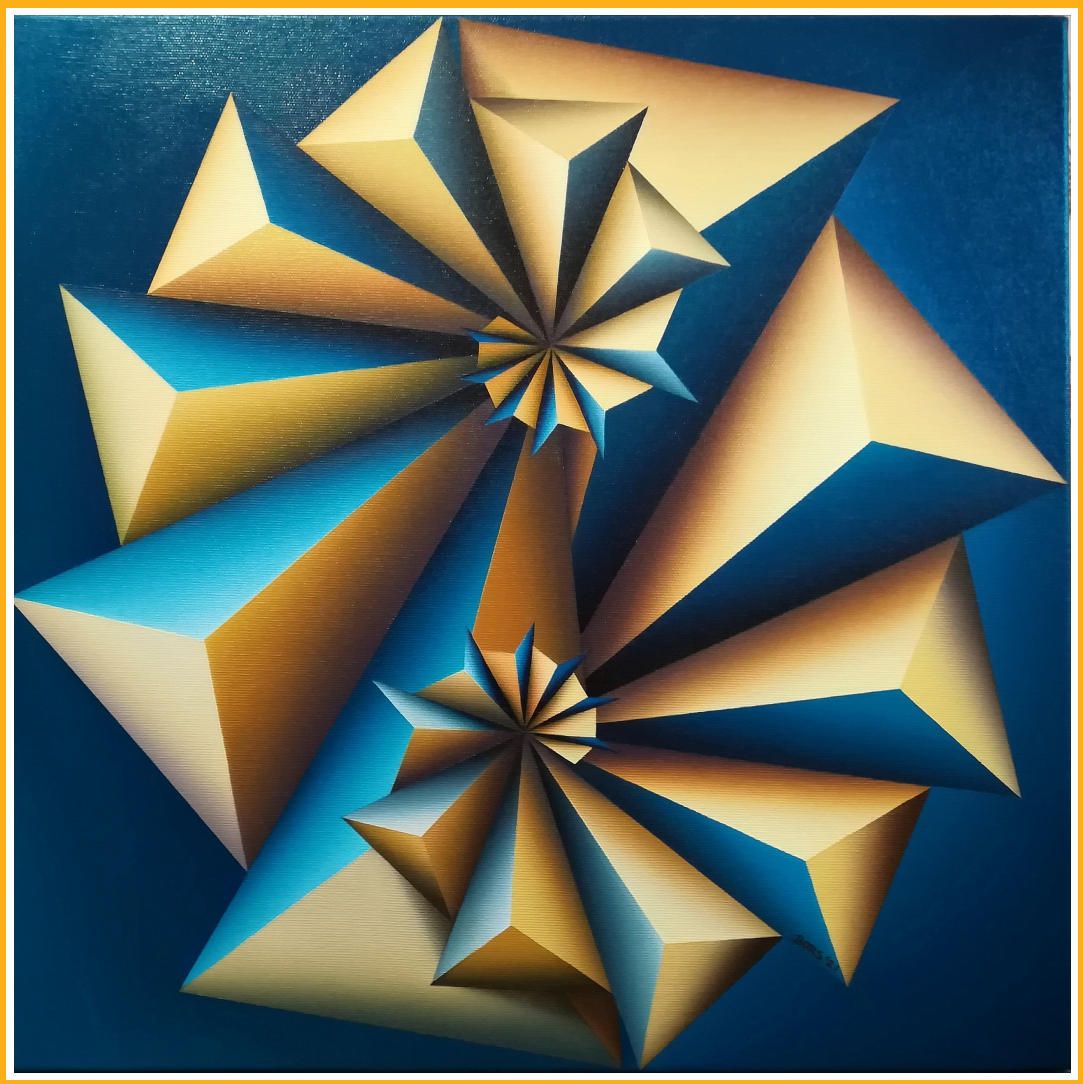
2022, IV. évf. 2. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata



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

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

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	Élelmiszerbiztonság
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

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.

Articles in the Safety and Security Sciences Review are archived in the Digital Archives of Óbuda University (ÓDA). 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.

A Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek. 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

Vol 4, No 2, 2022. | **2022. IV. évf. 2. szám**

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

BOZSIK Nándor

bozsik.nandor@uni-obuda.hu

Nándor BOZSIK studied technical studies in the field of electrical engineering. He specializes in energy security and renewable energy monitoring systems. Many settlements and institutions have been involved in energy modernization over the last twenty years. Its developments and designs have mainly covered the modernization of photovoltaic systems and lighting. He is currently a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda, his research area is energy security and renewable energy management.

BOZSIK Nándor műszaki tanulmányait villamosmérnöki tudományok területén végezte. A szakterülete az energiabiztonság és a megújuló energiák felügyeleti rendszere. Számos település és intézmény energetikai korszerűsítésben vett részt az utóbbi húsz év során. A fejlesztései és kivitelezései főleg a fotovoltaikus rendszerek és a világítás korszerűsítésre terjedtek ki. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója, kutatási területe az energiabiztonság és a megújuló energiák menedzsmentje.

FÁBIÁN Péter

fabianpeter@topcopgroup.com

After graduating from military high school and then college, he worked for many years as a criminal intelligence officer at various police departments. He has been working as a leader and expert in the private security sector for more than 20 years. Security consultant for several large multinational companies. He is an expert at the PTE Center for Defense Research. He is a doctoral candidate at the Doctoral School of Security Sciences of the University of Óbuda. His research topic is private security and terrorism. He holds degrees as a police officer, criminologist, lawyer and national security analyst. He is currently a postgraduate student in Cyber Security at the University of Óbuda.

Katonai középiskolai, majd főiskolai tanulmányai után sok évig bűnügyi hírszerzőként dolgozott a Rendőrség különböző szerveinél. Több, mint 20 éve a magánbiztonsági szektorban dolgozik vezetőként, szakértőként. Több multinacionális nagyvállalat biztonsági tanácsadója. A PTE Védelmi Kutatások Központ szakértője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorjelöltje. Kutatási témája a magánbiztonság és a terrorizmus. Rendőrtisz, kriminológus, jogász és nemzetbiztonsági elemző diplomával rendelkezik. Jelenleg az Óbudai Egyetem Kiberbiztonsági posztgraduális képzés hallgatója.

FRIGYIK András

frigyik.andras@uni-obuda.hu

After receiving his Masters Degree in Engineering from the Technical University of Budapest, specializing in Integrated Circuit Design and Artificial Intelligence. Later he gained his PhD degree in Mathematics (area: Inverse Problems) from University of Washington, Seattle, WA. His supervisor was Günther UHLMANN. He got his first postdoctoral position at Purdue University, West Lafayette, IN at the Department of Mathematics while for his second postdoctoral position he went back to University of Washington, but this time to the Department of Computer Science. He took up a permanent position at Pécs University and later moved to Óbuda University, where he currently resides.

A Budapesti Műszaki Egyetemen szerzett Villamosmérnöki diplomát Integrált áramkör tervezés és Mesterséges intelligencia szakirányokon. Később az Egyesült Államokbeli University of Washington (Seattle, WA) matematika tanszékén doktorált Günther UHLMANN vezetése alatt, az inverz problémák témakörében. Az első posztdoktori pozícióját a szintén Egyesült Államokbeli Purdue University (West Laffayet, IN) matematikai tanszékén töltötte. A másodikhoz a University of Washington informatikai (Computer Science) tanszéke adott otthont. Onnan a Pécsi Egyetem Matematikai és Informatikai Intézetébe került. Jelenleg az Óbudai Egyetemen tanít.

GULYÁS Olivér

gulyaso@gmail.com

Oliver GULYÁS PhD student. Studied at the Foreign School of Economics in Budapest and the University Paris 1 Panthéon – Sorbonne. Started his PhD studies at the Óbuda University Doctoral School for Safety and Security Sciences in 2021. After finishing MSc. studies, he was working in the banking sector, after more than 15 years started to work as an advisor. In his role as an advisor, he did not leave the financial sector, he is still working with banks or for banks. As an advisor he was involved in the "creation" of a unified new bank where he had the opportunity to have an insight into the vulnerability of the organisations more than before and experienced the everyday operational problems. It was at the final phase of this transformation when the COVID-19 pandemic broke out, this imposed new threats to the still fragile system. It was then he decided to deep dive in the cybersecurity. With the guidance of Dr. habil. Gabor KISS he is trying to identify the actual issues of cybersecurity, in particular its impact on the financial sector.

GULYÁS Olivér PhD tanuló. A Külkereskedelmi Főiskola, majd azt követően a Paris 1 – Panthéon Sorbonne egyetemen tanult. 2021-ben kezdte el PhD tanulmányait az Óbudai Egyetem Biztonságtudományi doktori iskolájában. Egyetemi tanulmányai elvégzése után a bankszektorban helyezkedett el, majd több mint 15 év után tanácsadással kezdett el foglalkozni. Tanácsadóként sem távolodott el a pénzügyi szektortól, továbbra is bankoknak vagy bankokkal dolgozik. Már tanácsadóként egy egyesített, új bank „létrehozásában" vett részt, amikor az addiginál jobban belelátott a szervezetek sérülékenységébe, megtapasztalhatta a mindennapos működési problémákat. Ennek az átalakulásnak a végén tört ki a COVID-19 járvány, ami újabb problémákat keletkeztetett a még törékeny rendszerben. Ekkor fogalmazódott meg benne annak az igénye, hogy mélyebben is beleássa magát a kiberbiztonság témájába. Az egyetemen Dr. habil. KISS Gábor útmutatása mellett próbálja feltérképezni a kiberbiztonság aktuális kérdéseit, különös tekintettel a pénzügyi szektorra gyakorolt hatásaira.

HEITLERNÉ LEHOCZKY Mária

maria.lehoczky@gmail.com

Maria HEITLER LEHOCZKY certified psychologist, certified marketing communication economist, certified Total Quality Management specialist, professional crisis therapy consultant (personal and group counselling), accredited interpersonal skills development trainer, organisation developer consultant. PhD student at the Doctoral School on Safety and Security Sciences of Óbuda University. Lecturer at Budapest Business School. One of the founding members of Artificial Intelligence Workshop at the Óbuda University. Member of the Hungarian Psychological Association. Her field of research is the study of the psychological mechanisms of economic processes from multidisciplinary perspective, including psychological aspects of artificial intelligence, cyberpsychology (psychology of cybersecurity), organizational psychology, career psychology, psychological capital, psychological wellbeing.

HEITLERNÉ LEHOCZKY Mária okleveles pszichológus, marketingkommunikáció szakközgazdász, Total Quality Management szakközgazdász, egyéni és csoportos krízislélektani tanácsadó és konzultáns, akkreditált interperszonális készségfejlesztő tréner, szervezetfejlesztő konzultáns Az Óbudai Egyetem Biztonságtudományi Doktori iskolájának hallgatója. A Budapesti Gazdasági Egyetem oktatója. Az Óbudai Egyetem Mesterséges Intelligencia Műhelyének egyik alapító tagja. A Magyar Pszichológia Társaság tagja. Kutatási területe a gazdasági folyamatok pszichológiai mechanizmusainak vizsgálata (gazdaságpszichológia) multidiszciplináris megközelítéssel, amely magában foglalja a mesterséges intelligencia pszichológiai vonatkozásait, kiberbiztonság pszichológia tényezőit (kiberpszichológia), a szervezetpszichológiát, a karrierpszichológiát, a pszichológiai tőkét, a pszichológia jóllétet.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR communications engineer, certified communications specialist, head of electronic information security, doctor of economics (PhD), cybernetic, consultant, coach, mediator. His research interests include the social aspects and economic impacts of the digital age, in particular the human dimension of information security, the development of information security awareness, human-robot interaction, smart city, artificial intelligence, social credit system, and domotics. He is a senior research fellow at the Óbuda University, leader of Artificial Intelligence Workshop, lecturer and supervisor at the Doctoral School on Safety and Security Sciences, and at the National University of Public Service Doctoral School of Military Engineering. He is an examiner for professional qualification exams. He is a senior consultant, mediator and coach of PREMA Consulting, expert of the Hungarian Military Society and the National Association of Human Professionals. He 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), 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, a domotika. Az Óbudai Egyetem tudományos főmunkatársa, a Mesterséges Intelligencia Műhely vezetője, az Egyetem Biztonságtudományi Doktori Iskolájának és a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának az oktatója, témavezetője. Elnök a szakmai képesítő vizsgákon. A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

NYÁRI Norbert

nyari.norbert@uni-obuda.hu

So far, I have studied mainly in the field of informatics, I have degrees in engineering, teaching and computer science. I have been working as a software developer for more than 10 years at a budgetary institution of the Hungarian public administration. Due to my studies and professional experience, I have extensive knowledge in the fields of application development, information security, and psychology. The aim of my doctoral research is to find tools, methods and solutions for strengthening the information security of the Hungarian public administration.

Eddigi tanulmányaimat alapvetően informatikai területen végeztem, rendelkezem mérnöki, tanári, programtervezői diplomákkal. Több mint 10 éve dolgozom szoftverfejlesztőként a magyar közigazgatás egyik költségvetési szervénél. Tanulmányaimnál és szakmai tapasztalatomnál fogva széleskörű ismeretekkel rendelkezem az alkalmazásfejlesztés, az információbiztonság, valamint a pszichológia területén. Doktori kutatásom célja a magyar közigazgatás információbiztonságának erősítését szolgáló eszközök, módszerek, megoldások felkutatása.

RÁCZ Ervin

racz@uni-obuda.hu

Dr. Ervin RÁCZ was born in Budapest in 1973. He received his MSc degree as teacher of physics and mathematics, and his PhD degree in physics from the University of Szeged (USZ), Szeged, Hungary in 1999 (József Attila University as predecessor of the USZ) and 2006, respectively. He has been working on the field of laser light – matter introduction such as investigation of nonlinear laser plasma phenomena in high intensity laser generated plasmas. Keeping this field as field of interest, in 2006 he joined the

Dr. RÁCZ Ervin 1973-ban született Budapesten. Felsőfokú tanulmányait a József Attila Tudományegyetemen végezte. 1999-ben szerezte meg egyetemi diplomáját okleveles fizika-matematika szakos középiskolai tanárként. A diplomaszerzés évében jelentkezett a szegedi egyetem PhD doktori iskolájába fizikatudomány tématerületen, ahová felvételt is nyert. PhD doktori munkája során lézerplazma fizikával, pontosabban nagyintenzitású lézerek által keltett szilárdtest lézerplazmákban megjelenő nemlineáris

Department of Physics, Charles Rhodes' laboratory at the University of Illinois at Chicago (UIC), Chicago, USA. He started his work as research specialist, but in 2008 he was visiting research assistant professor and later has been a research assistant professor at the UIC since 2010. Between 2006 and 2011 his research interests include experimental laser-plasma physics, high intensity excimer-based lasers, high intensity Ti:Sa-KrF solid state-hybrid laser systems. Since 2011 September, he works at the Óbuda University at the Kandó Kálmán Faculty of Electrical Engineering in Budapest. Parallel to the teaching activity, he works on the investigation of solar (PV) panels operation in function of the irradiating light parameters focusing on silicone-based solid state PV panels and dye sensitized solar cells. For this science he uses experimental and theoretical methods, too. He is very proud of that, between 2012 and 2018 he was one of the members of the founding board and founding council of the ELI ALPS (Extreme Light Infrastructure Attosecond Light Pulse Source) Research Institute in Szeged, Hungary.

plazma folyamatokkal foglalkozott. PhD értekezését e területen 2006-ban védte meg a Szegedi Tudományegyetemen. 2006. októberétől post. doc. munkatársként a chicagói University of Illinois Egyetem nagy lézeres laboratóriumába került, ahol hűtött xenon gáz jetekben kelthető röntgenlézer keltésével és a tűszerű roncsoló röntgen impulzusok karakterizálásával foglalkozott. Az ott töltött közel 6 év alatt látogató tudományos munkatárs, majd a laboratóriumi kísérletek igazgatójaként tevékenykedett. 2011 őszétől jelenleg is az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karán dolgozik. Oktatási feladatai mellett jelenlegi munkahelyén napelemeket érő besugárzások és a napelemek villamos működése közötti kapcsolatot kutatja kísérletes és elméleti módszerekkel. 2012-2018 között lézeres és lézeres alkalmazások szakértőként részt vett a szegedi ELI ALPS Lézeres Kutatóintézet létrehozásában, mert 2012-tól tagja volt a kutatóintézet létrehozásának tudományos és technikai, technológiai terveit készítő először kis majd nagy munkacsoportnak.

SIMON Mátyás

matyas.simon86@gmail.com

I graduated from the Faculty of Natural Sciences of the University of Pécs in 2011 as a graduate environmental researcher, and from 2017 I also have the qualification of an environmental expert. Subsequently, I supplemented my studies with a secondary qualification in occupational safety and fire protection. In 2020, I also successfully completed the training of a senior occupational safety specialist at the Budapest University of Technology. I started my professional career at Semmelweis University in 2013 as an environmental lecturer, and then I was appointed head of department, deputy director, and is currently headed by the Semmelweis University Directorate of Security Technology. During my career so far, I have had the opportunity to gain extensive experience in the fields of environmental, work, fire, property protection and dangerous goods transport (ADR). I am currently pursuing my studies as a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda.

A Pécsi Tudományegyetem Természettudományi Karán végeztem 2011-ben, mint okleveles környezetkutató, 2017-től környezetvédelmi szakértői jogosultsággal is rendelkezem. Ezt követően tanulmányaimat középfokú munkavédelmi és tűzvédelmi szakképesítéssel egészítettem ki. 2020-ban a Budapesti Műszaki Egyetem felsőfokú munkavédelmi szakember képzését is sikeresen elvégeztem. A szakmai pályafutásomat 2013-ban a Semmelweis Egyetemen kezdtem meg környezetvédelmi előadóként, majd megbízást kaptam osztályvezető, igazgatóhelyettes pozícióra, jelenleg a Semmelweis Egyetem Biztonságtechnikai Igazgatóság vezetésével bíztak meg, mint igazgató. Eddigi pályafutásom során alkalmam volt széleskörű tapasztalatokat szerezni a környezetmunka-, tűz-, vagyonvédelem és veszélyes áruszállítás (ADR) szakterületén. Tanulmányaimat jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatójaként folytatom.

SZABÓ László András

szabolandras.kmo@gmail.com

András László SZABÓ has more than twenty years of experience in property protection and mechanical safety protection, he had his own developments and

SZABÓ László András több mint húsz éves vagyonvédelmi és mechanikus biztonságvédelmi tapasztalattal rendelkezik, saját fejlesztései, találmányai vol-

inventions. Since 2008, he has deepened his degree in security management with a degree in law enforcement administration, began his career as a criminologist and scientist at the Doctoral School of Public Administration at the University of Public Administration, and then at the Doctoral School on Safety and Security at the University of Óbuda. His research interests include international migration and criminal policy, as well as security management and innovation opportunities in managing migration.

tak. 2008 óta elmélyedt a biztonságmenedzsment területén végzettségei rendészeti igazgatásszervező biztonsági szakon, kriminológus és tudományos pályáját a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolájában kezdte, majd az Óbudai Egyetem Biztonságtudományi Doktori iskolájában folytatja. Kutatási területe a nemzetközi migráció és a kriminálpolitika, illetve a biztonságmenedzsment és az innovációs lehetőségek a migráció kezelésében.

VALOCIKOVÁ, Cyntia

valocikova.cyntia@uni-obuda.hu

VALOCIKOVÁ, Cyntia graduated with a master's degree in business development at Keleti Faculty of Business and Management of Obuda University (2018) and is currently a PhD student at the Doctoral School on Safety and Security Sciences. During her master's degree, her research moved in the direction of social sciences, and her research experience elaborated. She improved her skills through several domestic and foreign conferences, academics trips and TDKs, and then at the OTDK in 2019 she took second place in the Sociology of Economics section. During her doctoral studies, her field of research changed; however, she continued her work in social sciences and economics. Research focuses on altruism and the dangers of selflessness. The current direction of research is the exploitation of selfless behavior on the Internet, through fraud and deception. However, the research deal with the traditional turnout of altruism, with its development, and incorporation into online interfaces.

VALOCIKOVÁ, Cyntia okleveles közgazdászként végzett vállalkozásfejlesztés mesterszakon az Óbudai Egyetem Keleti Károly Gazdasági Karán (2018), jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza. A mesterképzés alatt kutatása a társadalomtudományok irányába mozdult, kutatási tapasztalatát széles körben hasznosította. Számos hazai és külföldi konferencián, tanulmányúton, TDK-n részt vett, majd 2019-ben az OTDK-n tanulmányával második helyezést ért el a Gazdaságszociológia szekcióban. A doktori képzés alatt kutatási területe változott, azonban továbbra is a társadalom és gazdaságtudományokra épül. A kutatás középpontjában az altruizmus és az önzetlenséggel járó veszélyek állnak. A kutatás jelenlegi iránya az önzetlen viselkedés internetes kihasználása, csalások, megtévesztések révén. A kutatás azonban foglalkozik az altruizmus hagyományos megjelenésével, fejlődésével és beépülésével az online felületekbe.

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

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

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 experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

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

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

Vol 4, No 2, 2022. | **2022. IV. évf. 2. szám**

CONTENT | TARTALOM

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

EVOLUTION OF CYBERSECURITY AND THE CYBERSECURITY IN THE BANKING SECTOR UNTIL TODAY

A KIBERBIZTONSÁG ÉS A BANKI KIBERVÉDELEM FEJLŐDÉSE NAPJAINKIG

GULYÁS Olivér[1]

Abstract

Cybercrime appeared long before the birth of the Internet. From the early times, computers and networks were used to "produce," store, and transmit data. In the first period, therefore, the only motivation was to steal the data. Before the birth of the Internet, cybercrime was local. With the birth of the email in the '80s the attacks spread particularly hard. In the '90s, the web browsers helped carrying out the attacks. The next significant wave can be attributed to the rise of social media. By sharing all kinds of information about ourselves, it has opened a Pandara's box for personal data and digital data theft. The last major development was the "institutionalization" of cybercrime. The criminals are no longer pimpled teenagers hiding under dark hoods (as people have imagined), but extensive teams operating as international companies, often backed by states. The aim of the article is to present the development of cybersecurity, the cybersecurity in the banking sector, from the early phase to the present day.

Keywords

history of cybercrime, evolution of cybersecurity

Absztrakt

A kiberbűnözés már jóval az internet megszületése előtt megjelent. A korai időktől a számítógépeket és a hálózatokat az adatok „gyártására", tárolására és továbbítására használták. Az első időszakban még csak az adatok eltulajdonítása volt a motiváció. Az internet megjelenése előtt ez még lokális, helyhez kötött bűnelkövetés volt. A 80-as években az email megjelenése különösen nagyot lökött a támadások elterjedésén. A 90-es években a webes böngészők megjelenése segítette a támadások elkövetését. A következő hullám a közösségi média térnyeréséhez köthető. Azzal, hogy az emberek mindenféle információt osztanak meg magukról, megnyitotta a személyes adat és a digitális adatlopás Pandóra-szelencéjét. Az utolsó nagy fejlődési lépés a kiberbűnözés „intézményesedése" volt. A bűnözők már nem sötét szobákban, kapucni alatt rejtőzködő pattanásos tinédzserek (ahogy ezt az emberek elképzelték), hanem nemzetközi cégekként működő kiterjedt csapatok, akiket sokszor államok támogatnak. A cikk célja bemutatni a kiberbiztonság, azon belül is a banki kibervédelem fejlődésének lépéseit a korai fázistól napjainkig.

Kulcsszavak

kiberbűnözés történelme, kiberbiztonság fejlődése

[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbuda University Doctoral School for Safety and Security Sciences | doktorjelölt, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az életet alakító nagy törvényszerűségek közül a newtoni hatás és ellenhatás törvény számos területen jön észrevétlenül szembe velünk. Az elmélet egy kicsavart formája, amikor valaki kitalál vagy felfedez valamit, akkor előbb vagy utóbb egy másik ember kitalálja, hogyan lehetne ellopni azt. Amikor az első ember a fizetési kötelezettségét írásba foglalta, abból később megszületett a váltót. Nem kellett sok idő hozzá, hogy egy másik ember rájöjjön, hogyan lehetne a váltót hamisítani. Természetesen az, hogy egy tolvaj megpróbálja ellopni az értékeinket vagy jószágunkat magával hozza azt is, hogy mások megpróbálják megakadályozni azt, hogy az előbbiek ellopják, meghamisítsák azt. Talán ez az elmélet nem fog belekerülni az egyetemes világfejlődés tanok közé, de mégis a direkt kiváltó oka volt a biztonságtechnika kialakulásának.

A bankbiztonság és a kibervédelem története is valahol azzal kezdődött, hogy egyre inkább elterjedt az elektronikus, digitális eszközök alkalmazása. Amikor az eszközét használni kezdte nyilván már az elejétől készült arra, hogy ezt ne lehessen ellopni, de az igazi éles teszt az az volt, amikor tényleg megpróbálták a rendszert feltörni.

A pénzügyi termékek megjelenése majd rohamos fejlődése magával hozta a pénzügyi termékek eltulajdonítási módjának fejlődését, ami viszont magával hozta az eltulajdonítás elleni védelem fejlődését is. Ezen a ponton érkezünk meg a (bank)biztonság megszületéséhez.

A történelem megmutatta, hogy nincsen feltörhetetlen és ellophatatlan rendszer, de az emberek mindig is törekedtek erre – de legalábbis mindig is azt hitték, hogy megtalálták a legjobb módszert.

A cikk célja, hogy az események láncolatát számba vegye és a végén megmutassa, hogyan jutottunk el a biztonságtechnika és azon belül a kibervédelem jelen szintjére. Jelen cikk része egy nagyobb, a pénzintézetek kiberbiztonságát vizsgáló kutatásnak.

BIZTONSÁGRA TÖREKEDÉS, MINT ALAPSZÜKSÉGLET

A biztonságra törekedés az ember alapvető igényeihez tartozik. Az emberek törekednek arra, hogy elkerüljék a veszélyt, megvédjék testi épségüket vagy anyagi javaikat – miután a fiziológiai szükségleteiket már kielégítettek.

1. ábra: Maslow motivációs piramisa, forrás: http://www.azirastukreben.hu/maslow-motivacios-piramisa [1]

A biztonságra való igény már az őskortól meghatározta a működésünket. A szerszámokat és később a fegyvereket az ősember nemcsak az élelem megszerzésére, de saját maga megvédésére is használta. Szintén a biztonságát (is) szolgálta a tűz használata. Mielőtt megtanulta volna a tűzgyújtást, a tűz megőrzésével biztosította a „fűtéshez" szükséges meleget. Szintén a biztonságra való törekvése volt a farkas „domesztikációja révén" háziasított kutya. A kutya nemcsak a vadászatban segített az embernek, hanem védte annak házát is [2]. Már a korai időktől maga a lakhely (barlang, védett üregek stb.) kiválasztásában is a biztonságra való törekvés volt a meghatározó motiváció.

Az ókorban a közösségbe szerveződés már megteremti az alapját a bonyolultabb biztonságtechnikának is. A technika színvonalának, a társadalom szervezettségének emelkedésével vált lehetővé bonyolultabb biztonsági technológiák megjelenése.

A középkor volt az, ahol az állami szervezetek, birodalmak fejlődése magasabb szintre emelte a biztonságtechnika eszköztárát. Utak, úthálózatok, városok, városállamok, vagy akár a templomok és az ott használt harangok, amivel a veszedelmet jelezték mind lépések voltak egy komplexeb biztonságtechnikai rendszer irányába.

Az általános biztonságra törekvésen felül az emberek szerették volna a jószágaikat, értékeiket is biztonságban tudni. A bankbiztonság és azon belül a banki kiberbiztonság kialakulásának történelmét ezért valahol a pénz kialakulásánál kell kezdeni.

PÉNZ ÉS A PÉNZÜGYI RENDSZEREK KIALAKULÁSA

A bankok és a banki szolgáltatások megjelenését, majd azt követően a bankbiztonság megszületését valahol a pénz kialakulásánál kell kezdeni. A pénz kialakulását a legtöbb elmélet a cserekereskedelem kialakuláshoz köti. Amikor a korabeli emberek már nem tudták az egyik árut a másikra cserélni. Nem mindenkinek kellett az adott csereterméke, mert nem lehetett a cserét értékegyeztetéssel végrehajtani, vagy mert a cserélendő termékre az igény nem volt egyidejű (az egyik ember téli fél ruhát készített, de nyáron is ennie kellett valamit stb.), megjelent a pénz.

A nemesfémből készült érmékkel megjelent azok „manipulálása" is. A fém érmék szélét levágták, így próbáltak meg csalni vele. A levágott szélekből újra pénzt lehetett verni. Előfordult, hogy maguk a pénz kibocsátói rontották az értékét azzal, hogy a régieket bevonták és alacsonyabb nemesfém tartalmú érméket bocsátottak ki.

A fémpénz megjelenését követően, első írásos emlék i.e. 3000 körüli Mezopotámiában, a váltó a következő nagy lépés [3].

A nemesfémek kínálata, azok előállítása (bányászata) miatt nem tudta követni a gazdaság növekedését. A pénzhiány eredményeképpen megjelentek a váltók. A váltókibocsátója (adós) kötelezettséget vállalt arra, hogy a váltó birtokosának egy jövőben meghatározott dátumra kifizeti a tartozását.

Ezeket a váltókat az elfogadóik egy idő után tovább forgatták, pénzként adták tovább. A váltókkal az eredendő probléma az volt, hogy a sokadik forgatása után az elfogadó már térben és időben messze került az által ismeretlen adósságot garantáló személytől. Ezért nem mindig fogadták el szívesen. Természetesen a magánszemélyek által kibocsátott váltókkal megjelent azok hamisítása is.

A váltóhamisítás, ahogy a pénz szélének körbevágása, már szofisztikáltabb csalás volt. A magánszemélyek által kiadott váltük esetében az aláírások odahamisítása, díszes papírok lemásolása már komolyabb előkészületeket igényelt.

A középkorban megjelenő bankok őrzésre átvették a pénzeszközöket – a pénz kopása, őrzése és szállítása jelentős költséggel járt. Az átvett pénzeszközökről igazolást adtak ki. A bankok által kibocsátott váltókat már mindenki elfogadta – nagyobb biztonságot jelentett a gazdaság szereplőinek. A bank által kibocsátott fizetési ígérvények már közvetlen ősei voltak a bankjegyeknek.

Egyes bankok csődje, a piac szabályozása és az „önös" érdek is azt eredményezte, hogy az államok magukhoz vették a bankjegykibocsátás monopóliumát. Létrejött az állami bank, a jegybank. „Bár az 1668-ban alapított Sveriges Riksbank a legidősebb központi bank, az állambankári feladatokat ellátó intézmények Európa-szerte az 1694-ben, magánbankként felállított Bank of England példáját követték" [3]. Egy idő után már csak az állam által kibocsátott bankjegyekkel lehetett fizetni. [3] [4] [5]

A bankjegyek hamisítása és a bankok kirablása a mai napig virágzó „üzletág". A hamísítás természetesen magával hozta a bankjegyek hamisítás elleni védelmének fejlődését. A bankok kirablása, pedig a biztonsági rendszerek fejlődését.

TELEKOMMUNIKÁCIÓ ÉS A SZÁMÍTÓGÉP MEGJELENÉSE

Az első időszakban még csak fizikai formában létezett a pénz. A követelések lekönyvelése effektíve könyvekben, papíralapon történt. A papírlapú működés koporsójába az első szöget azonban még nem az informatika, hanem a telekommunikáció fejlődése ütötte.

A London és New York között 1858-ban létrejött távírókapcsolat nem titkolt célja a gazdaság két meghatározó piacának összekötése volt. A korabeli beszámolók alapján a banki tranzakciók időtartama a korábbi négy hétről így egy napra csökkent [6].

A XIX. század közepéig kellett várni, hogy a számítástechnika is hasonló áttörést hozzon a bankok működésében, mint amekkorát a távírógépek hoztak. Az első időszakban a számítógépeket a könyvelésben, a back office területeken használták. Azokon a területeken, ahol a számítások pontossága, gyorsasága és a legtöbb adminisztrációs feladat volt.

A számítógépek használatának elterjedésével és azok összekapcsolásával létrejöttek a komplex rendszerek. 1965-re az Egyesült Királyságban és az Egyesült Államokban a legtöbb nagy bank bevezette az elektronikus adatfeldolgozást, ami lehetővé tette, hogy már a nap végén lássák az aznapi teljes számlaforgalmat [6].

Az 1960-as évek végén az adatbáziskezelő rendszerek megjelenése, a digitalizáció mellett a szabványosítás elterjedése kellett azonban ahhoz, hogy a különböző bankok közötti tranzakciókban is ki tudják szorítani az informatikai megoldások a fizikai instrumentumokat.

Az előzőek teremtette meg annak az alapját, hogy az elektronikus banki szolgáltatások beszivárogtak a lakossági szolgáltatásokba is. Az ügyfelek bankszámlát nyitottak, fizetésüket közvetlenül a bankszámlájukra kapták.

1967-ben Londonban, amikor az első ATM elkezdte működését született meg a 0-24-ben működő szolgáltatás intézménye. A New York-i Chemical Bank már azzal hirdette az automatáját: „Szeptember 2-án bankjaink 9 órakor nyitnak, és soha többé nem zárnak be" [7]. A bankkártya megjelenése, a pénzhasználati kultúra megváltozása magával hozta a bankok működésének átalakulását.

A következő nagy lépés az volt, amikor a bankfiókok beköltöztek az emberek otthonába. Az 1982-ben az Egyesült Királyságban bevezetett „Homelink" rendszer, ahol a televízió teletex dekóderével és a telefonvonal segítségével az emberek otthonából elérhetővé vált a bankszámlájuk. Franciaországban ehhez hasonló és nagyon sokáig közkedvelt megoldás volt az úgynevezett Minitel, aminek 1990-ben 6,5 millió felhasználója volt [8].

Magyarországon 1994-ben az OTP Bank vezette az automatikus telefonos szolgáltatását a Telebankot. Az internet használata a Wells Fargo nevéhez köthető, aki 1995-ben indította online banki szolgáltatását [6]. Mára a Statista kutatása alapján az internetet bankolásra használók száma megközelíti a 2 milliárdot, 2024-re várhatóan a 2,5 milliárdot [8].

Az elektronikus eszközök térnyerésével, az informatika fejlődésével a nyilvántartások elektronikusak lettek. Azt gondolnánk, hogy a mai modern korban már minden elektronikusan tárolt, kereshető, de nagyon sok bank küzd még ma is azzal, hogy archív anyagai nincsenek digitalizálva, bizonyos instrumentumok (például régi garanciák) még papíralapon vannak könyvelve.

Az elektronika térnyerésével a támadók is új módszerekre tértek át. Volt olyan ATM berendezés, a technológia megjelenésének hajnalán, ahol mágneses vagy lyukkártyát kellett a gépbe csúsztatni, esetleg fém zsetont kellet a berendezésbe dobni. Ezeket a zsetonokat a bank később postai úton visszaküldte az ügyfeleknek. Ezzel egy újfajta rablási módszer: a zsetonok ellopása és az azokkal való visszaélés is gyorsan megjelent [9].

KIBERBŰNÖZÉS FEJLŐDÉSE

A kiberbűnözés, ahogy korábban már elemeztük, az elektronikus technológiák fejlődésével párhuzamosan fejlődött. Amikor egy találmány forgalomba került, a bűnözők is megtalálták annak módját, hogy valahogy ők is hasznot húzhassanak belőle.

A következő részben az egyes bűnelkövetési módszereket vesszük górcső alá. Időrendi sorrendben haladva megnézzük a kezdetleges módszerektől hogyan jutottunk el a szofisztikált kibertámadásokig. Olyan eseményeket és technikákat fogunk vizsgálni, amelyek az elődjei voltak a bankokat megcélzó támadásoknak.

Korai telefonok feltörése

Ahogy a számítógépet a telefon, úgy a számítógépes bűnözést is megelőzte a telefonos-bűnözés. A korai években a telefonos központokban tinédzser fiúk dolgoztak. Már 1878-ban, két évvel azután, hogy Alexander Graham Bell „felfedezte" a telefont, megtörténtek az első telefonos visszaélések. A fiatalok hívásokat szakítottak meg vagy irányítottak át, később saját hívásokat indítottak. A visszaélések hatterében inkább a saját maguk szórakoztatása, mint a haszonszerzés volt [10].

Távíró feltörése

Természetesen a korai távírórendszereknek is megvoltak a saját hackereik. 1903-ban a Marconi vezetéknélküli távírójának első nyilvános bemutatását zavarta meg Nevil Maskelyne azzal, hogy sértő, trágár üzeneteket küldött a berendezésre. Célja a biztonságosnak mondott találmány hiteltelenítése volt – saját állítása szerint, hogy felhívja a figyelmet a rendszer sérülékenységére [11].

Fénykép: Nevil Maskelyne, a távíró feltörője, forrás: https://listverse.com [12]

Háborús kódfeltörők

A világháborús kódfeltörőkről több film és regény is született. Leghíresebb talán a német Enigma feltörésének története, ami a talán az etikus hackerkedés előfutára lehetett. 1939-ben az Egyesült Királyságbeli Bletchley Parkban Alan Turing és Gordon Welchman kifejlesztette a BOMBE-berendezést a német Enigma berendezés által titkosított üzenetek dekódolásásra [13].

Az azóta eltelt időben többször szóltak a hírek arról, hogy bizonyos támadások mögött már nemcsak magánszemélyek, hanem szervezett csoportok, esetleg idegen kormányok is állhatnak. Ugyanúgy, ahogy a támadók, a védelem vonala sem néhány elszigetelt emberből áll.

2007-ben az észt számítógépes infrastruktúra elleni támadáskor ismerték fel az emberek az államok által támogatott kiberbűnözői csoportok létezését. Bár ez csak a második jelentős mértékű összehangolt támadás volt, a 2003-as Titan Rain után [14]. Mégis az észtországi támadássorozat volt, ami felnyitotta az államok szemét, és például a NATO kibervédelmi központjának (*Cooperative Cyber Defence Centre of Excellence*) megalapításához vezetett.

Napjainkban, a cikk írásának pillanatában, is a folyamatban lévő „fizikai" háború mellett folyik egy információs háború is. Ebben a háborúban az Oroszország által támogatott hacker-sereg áll szemben az ukrán és az őt támogató országok hacker-seregeivel. A hackerek a másik fél katonai rendszereinek feltörésével, a csapatmozgások nyilvánosságra hozásával próbálnak a fizikai hadszintéren is előnyre szert tenni.

Etikus hacker

Az első etikus hacker René Carmille volt, aki megakadályozta, hogy a Franciaországot elfoglaló nácik kinyerjék az országban élő zsidók adatait – „zsidóságukra" vonatkozó információt – a lyukkártyás alapon működő nemzeti demográfiai nyilvántartó rendszerből. Carmille feltörte a nyilvántartó rendszert. Bárhogyan próbálkoztak is a nácik a zsidóságra vonatkozó adatot bevinni vagy kinyerni a nyilvántartóból a rendszer senkinél se hozott fel erre vonatkozó adatot.

Közel két évig meg tudta akadályozni a nácikat a demográfiai nyilvántartó használatában. Amikor végül 1944-ben rájöttek, hogy Carmille manipulálta a gépeket Dachauba szállították, ahol végül meg is halt [15].

Az etikus hackerség azóta legalább annyira elterjedt lett, mint a „sima” hackerség. Több cég nyújt a kiberbiztonsági tanácsadás kertében etikus hacker szolgáltatásokat. Kontrolált körülmények között megpróbálják megkeresni egy adott cég informatikai rendszerének hiányosságait. Több intézményben, például az Óbudai Egyetemen, képeznek etikus hackereket.

Fénykép: René Carmille, az első etikus hacker, forrás: https://listverse.com [12]

Telefonok feltörése („phone phreaks”)

Az ’50-es évek végétől jelentek meg az úgynevezett „phone phreaks”-ek. Ezek az emberek a telefonokat „hackelték meg”. Rájöttek, hogy a telefonkagylóba a megfelelő zene lejátszásával fel tudják törni a telefonhálózatot és szabadon tudnak hívást indítani bárhova. Az eljátszott vagy elfütyült hangsor, amennyiben megegyezett a megfelelő titkos kóddal, egy belső, a távolsági hívásokat kezelő operátorhoz kapcsolta a hackert. Az operátor ezáltal azt hitte, hogy kolléga van a vonal másik végén, így a kért tetszőleges számra kapcsolta őt – természetesen teljesen ingyen.

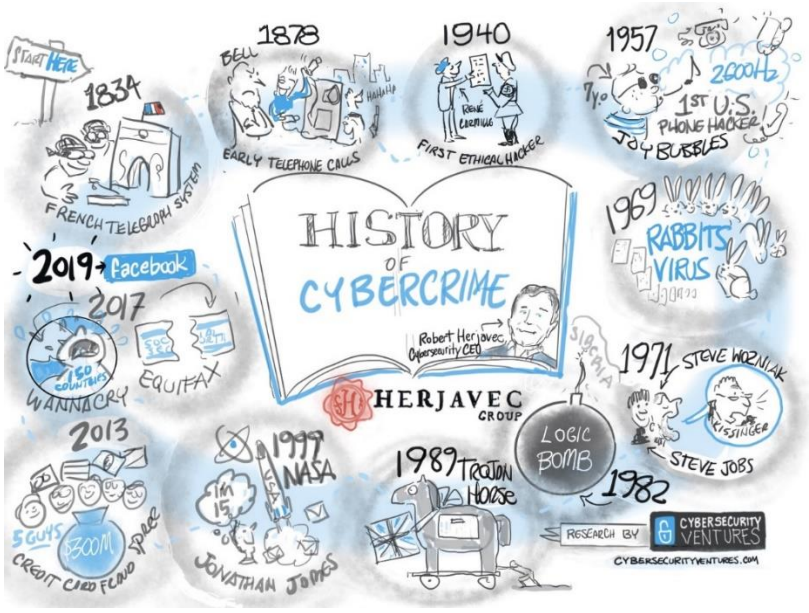
David Condont (1955) tartják az eljárás úttörőjének. Azonban Joe Engressia (Joybubbles), a vak 7 éves tökéletes hallású fiú, lett a leghíresebb „fütyülő hacker” [12].

John Draper, aki egy müzlis dobozban talált síppal törte fel telefonrendszert (innen származik a beceneve Captain Crunch) inspirálta később Steve Jobs-ot és Steve Wozniakot. Az Apple későbbi megalapítói találták ki a telefonvonalak feltörésére alkalmas blue-box berendezést (1971) és kerestek sok pénzt a későbbi „tömeggyártásából” [12].

A telefonok feltörését (phreaking) fejlesztette tovább a Phonemasters csoport. A csoport tagjai először csak lopott, nemzetközi hívásokhoz használható kártyakódokat árultak. Majd kiterjesztették a működésüket és mindenféle személyes adatot árusítottak, amire a „vevőnek” szüksége volt. Legdrágább csomagjuk: 500 dollárért bármelyik híres ember, politikus vagy celebritás, címét vagy telefonszámát meg lehetett vásárolni. Tevékenységükkel közel 1,85 millió dollárt kerestek [16].

Számítógépes jelszó feltörése

Allan Scherr volt az első, aki feltörte egy számítógép belépési jelszavát. Scherr egészen pontosan az első jelszóval védett számítógépet törte fel. Az MIT-n 1962-ben jelszóval védték a számítógépeket. Allan Scherr azonban megelégelte a beállított időkorlátokat, ezért a többi felhasználó feltört jelszavával lépett be, amikor lejárt a saját ideje. Az első számítógépes troll megjelenése is neki köszönhető. Az osztálytársaival az egyik megszerzett jelszóval a tanáruk fiókjába lépett be és tette őt nevetség tárgyává [17].



2. Ábra: Kiberbűnözés története, forrás: https://cybersecurityventures.com [17]

Hackerek megjelenése

Maga a szó, hogy „hacker" is az MIT-ról származik. Carlton Tucker az egy tanár használta az iskola telefonos rendszerét feltörőkre, phone phreak-ekre. A „hack" szót már korábban is használták, de akkor még csak az elektronikával foglalkozókra. Ebben a negatív értelemben először Carlton Tucker használta 1963-ban a „hacker" szót a telefonos rendszert feltörőkre [12].

Számítógépes vírusok és a DDoS

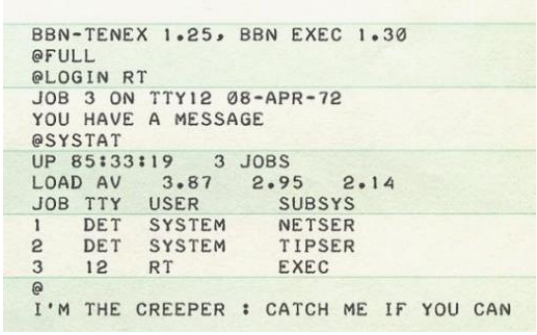
A RABBITS volt 1969-ben az első számítógépes vírus. Programkód eredete nem ismert, de a vírus terheléses támadással térdre kényszerítette a Washingtoni Egyetem számítógép központját. A programot ismeretlenek feltelepítették az egyetem egyik számítógépére és a program elkezdte lemásolni magát. A program két másolatot készített magából, a másolatok tovább szaporodtak – a gyors szaporodási módszerből származik a vírus neve is. Az elszaporodott programocskák egy idő után túlterhelték a számítógépet, ami így leállt [17].

Öt évvel később valaki, aki ismerte a fenti történetet létrehozott egy újabb „nyúlvírust", amit WABBIT-nak hívott. Azért, hogy egy másik számítógépes felhasználót „kiüssön" feltelepítette a programot az APRANET-re, az amerikai tudományos intézetek között kialakított számítógépes hálózatra – az Internet elődjére (Advanced Research Projects Agency Network, „ARPANET"). Ez volt a történelem első számítógép ellen végrehajtott túlterheléses támadása (Distributed Denial-of-Service, „DDoS") [12].

Számítógépes vírus az Interneten

Ray Tomlinson és Bob Thomas volt az első, aki 1971-ben az Interneten keresztül egy levélben juttatott el egy vírust. A Creeper nevezetű féregvírus lemásolta saját magát és

így terjedt az ARPANET-en. Minden egyes másolat egy ablakban felugrott és azt írta ki, hogy „Én vagyok a creeper: kapj el ha tudsz” („I’m the creeper: Catch me if you can”). Később, az Internet felfedezésekor Tomlinson ide is feltöltötte a vírusát [12].



Fénykép: Creeper, az első számítógépes vírus képernyőképe, 1972, forrás: https://listverse.com [12]

Híres hírhedt hackerek

A leghíresebb hacker valószínűleg Kevin Mitnick volt, aki 1970 és 1995 között majdnem a világ összes szigorúan védett számítógépes hálózatát feltörte. Mitnick a „pszichológiai befolyásolás” (social engineering) segítségével törte fel ezeket a rendszereket. A dolgozók megtévesztésével megszerezte azok azonosítóját és jelszavát.

Saját bevallása szerint a különböző rendszerek minél mélyebb szintű megismerése vezérelte a tetteit. Abban az időszakban a leginkább keresett bűnöző volt. Végül kétszer is (1988-ban és 1995-ben) bebörtönözték „áldásos” tevékenységért, először 46 majd 22 hónapra. A büntetéséből 8 hónapot magánzárkában töltött, mert az ügyészek meggyőzték a bírót, hogy telefonba fütyüléssel el tudja indítani a nukleáris rakétákat [18].

„Számítógépes” sikkasztás

Az első sikkasztás, számítógép segítségével, nem sokkal azután történt, hogy a számítógépeket már nem csak a back office-ban alkalmazták elvont számításos műveletek elvégzésére, hanem a normál banki működés része lett. Egy New York-i bank pénztárosa 1973-ban több mint 2 millió dollárt sikkasztott el [17].

Trójai vírusok

Az első trójai vírust John Walker készítette 1975-ben. A vírus két évvel azelőtt született, hogy az első otthoni személyi számítógépek az üzletekbe kerültek volna. A vírus kitalálója, saját bevallása szerint, csupán jóindulatból állította úgy be az általa készített ANIMAL nevű játékot, hogy a háttérben bemásolja magát minden meghajtóra, majd minden a megfertőzött gépbe berakott (akkor még) mágnesszalagra.

Walker állítása szerint így szeretett volna az embereknek segíteni, hogy ne kelljen elkérni a játékot – és nehézkesen átmásolni –, hanem ő már előre „elhelyezte” azt számukra a saját gépükre [12].

Az első kiberbűnöző

Bár Kevin Mitnick sok dologban megelőzte, mégis Ian Murphy volt az első ember, akit 1981-ben el is ítéltek kiberbűnözés miatt. A rajongói által csak Captain Zap-nak hívott

Murphy feltörte az AT&T vállalat hálózatát és átállította a rendszer belső óráját, hogy munkaidőben is csúcsidőn kívüli díjakat számítson fel. Tettéért akkor még csak 1.000 óra közmunka és 2,5 év próbaidő volt a „jutalma". A későbbi a Komputerkémek (Sneakers, 1992) című mozifilm írója a ténykedéséből merítette a film inspirációját [17].

Zsarolóvírus

Az első jelentősebb zsarolóvírus támadást 1989-ra datálják. Ebben az évben egy AIDS adatbázist küldtek több ezer AIDS kutatóknak és egy angol számítógépes magazin előfizetőinek. A program egy trójait tartalmazott, amely 500 dollárt kért a számítógép adatainak „felszabadításáért" [19].

World Wide Web

1994-ben elindul a World Wide Web. A hackerek innentől kezdve határok nélkül „dolgozhattak". A technológia megkönnyítette a számítógépes rendszerek feltörését, de a hackerek egymás közötti kommunikációját is.

A korábbi szűk körű, online fórumokon folyó kommunikáció mindenki számára elérhetővé válik a különböző weboldalakon keresztül. Ezt használja például ebben az évben egy angol diák, aki a web-en talál betárcsázó program segítségével az otthoni Commodore Amiga számítógépéről feltöri Korea nukleáris rendszerét, belép a NASA és több más amerikai hivatal számítógépes rendszerébe [19].

Bankokat ért jelentős kibertámadások

Az egyik első jelentős bankot érintő kibertámadás a 30 éves Vladimir Levin nevéhez köthető. Az orosz kiberbűnöző 1995-ben, az akkor még gyerekcipőben járó világháló segítségével a szentpétervári otthonából törte fel a Citibank New York-i informatikai rendszerét.

A rendszer feltörése után, az ügyfelek belépési azonosítójával és jelszavával csalárd tranzakciókat engedélyezett. A hivatalos becslések szerint közel 12 millió dollárt utalt át különböző számlákra világszerte – Levin ebből „csak" 3,7 millió dollárt ismert el. A tranzakciók egy részét sikerült az FBI-nak lekövetnie. Levint 1998-ban 3 év börtönbüntetésre ítélték, a pénz jelentős részét megtalálták [20]. Az eset, és a jelentős mértékű ellopott, összeg korai figyelmeztető jel volt a banki számítógépes rendszerek sérülékenységére.

Albert Gonzalez, már 14 éves korában felkeltette az FBI figyelmét, amikor feltörte a NASA számítógépes rendszerét. 2003-ban elfogták, amikor a ShadowCrew csapat tagjaként bankkártya adatokat lopott és értékesített online. 2006-tól 2008-as elfogásáig több millió dollárt szerzett hitel- és betétkártya adatok ellopásával – többek között a TJX, Heartland Payment Systems és a Citibank rendszereinek feltörésével. Az ellopott pénzt szállodákban és luxus bulikra költötte el. Tevékenységért a „jutalma" összesen 20 év börtön volt [17].

2005-ben az HSBC több mint 180.000 ügyfélnek küld levelet figyelmeztetve őket, hogy a kártyaadataik az egyik kiskereskedő (Polo by Ralph Lauren) rendszerének feltörésén keresztül kompromittálódhattak [17].

2010-ben egy kelet-európai kiberbűnöző csapat szintet lép. Zeus nevű trójai vírusuk segítségével Egyesült Államokbeli és angol bankok rendszerének feltörésével az ott vezetett bankszámlákról 70 millió dollárt lopnak el. A vírus eredetileg számítógépeket célzott, de upgrade-elve lett mobil telefonokra. A károsultak által megkapott levélben vagy megnyitott oldalon található linkre kattintva feltelepült a program az eszközökre, ami megjegyezte a

károsultak billentyű leütését, amikor azok beírták a belépési azonosítójukat. Az eset arra hívta fel az emberek figyelmét, hogy a XXI. század szervezett bűnözése a kiberbűnözésben is aktívan részt vesz [21].

Zeus rekordja nem tartott sokáig. 2013-tól 2015-ös elfogásukig egy orosz hacker csapat több mint száz pénzintézet számítógépes rendszerét törte fel és lopott el hozzávetőlegesen 800 millió dollárt. Az egész világon átívelő kibertámadás-sorozat keretében egy vírus segítségével beléptek a rendszerekbe, hamis átutalásokat engedélyeztek, sőt sikerült bankjegykiadó automatákat is feltörniük, amikből kártya nélkül készpénzt tudtak felvenni [22].

2013-ban egy másik rekord dőlt meg. Az Egyesült Államok addigi történelmének legnagyobb kiber-bűnesetét és hitelkártya csalását követték el. Az elfogott öt ember több mint 300 millió dollár kárt okozott tettükkel. Elfogásukkor fény derült a Nasdaq, a Visa és egyéb cégek ellen folyamatban lévő támadásokról. Az elkövetők nyomait akkor már évek óta követték. Az öt férfi (négy orosz és egy ukrán) legalább 160 millió hitelkártya adatát lopta el és adta tovább [23].

A hírhedt bangladesi bankrablás nemcsak a rablási érték miatt került a hírekbe: 81 millió dollárt loptak el néhány óra alatt a Bangladesh Banknál vezetett bankszámlákról, de csak egy apró programozási hiba miatt nem tudták a többi közel 1 milliárd dollárnyi összeget ellopni. Ami felkeltette a hatóságok érdeklődését az a technika, ahogy a tolvajok betörtek a bank rendszerébe. A nemzetközi átutalási rendszert, a SWIFT-et használták, hogy feltörjék a bank számítógépeit. A SWIFT egy 1970 óta működő szuper-biztonságos(nak gondolt) zárt pénzügyi rendszer amit világszerte közel 11.000 intézmény használ, közel napi 25 millió tranzakció végrehajtására – a világ pénzügyi átutalásainak jelentős része. Pénzintézetek, kereskedők, pénzügyi szervezetek használják a SWIFT-kódokat az intézmények beazonosítására a tranzakciók ellenőrzésére [24].

ÖSSZEFOGLALÁS

Cikkben bemutattam a pénzügyi rendszer fejlődése mellett hogyan fejlődtek a pénzügyi rendszer elleni támadások is. A pénz megjelenésétől, a pénzintézetek megjelenéséig nagy utat jártunk be. A fejlődés azonban nem állt meg, a papíralapú működéstől a digitalizációig még sok évnek kellett eltelnie. A digitalizáció rohamos fejlődése azonban magával hozta a bankszektort érintő veszély növekedését [25].

A támadásokra adott egyenes válaszként a szakemberek megpróbálták megvédeni az informatikai rendszereket. Először megpróbálták lekövetni, majd később a hackerek előtt járni, csapdába csalni azokat (például a *honey pot* megoldásokkal). Ennek a macska-egér harcnak az közvetlen eredménye a kibervédelem erősödése. A történelmi áttekintés célja az volt, hogy megmutassam milyen utat kellett ahhoz bejárni, hogy a kiberbiztonság mai szintjére érkezzünk meg.

A technika fejlődése azonban természetesen nem állt meg, a Blockchain technológiák vagy a mesterséges intelligencia alkalmazása új lehetőségeket nyithat meg a banki kibervédelemben.

Jelen cikk része egy nagyobb, a banki kiberbiztonságot vizsgáló kutatásnak.

FELHASZNÁLT IRODALOM

[1] Szabó Szilvia, „Maslow motivációs piramisa," [Online]. Available: http://www.azi-rastukreben.hu/maslow-motivacios-piramisa. [Hozzáférés dátuma: 16 05 2022].

[2] Szűcs Endre, „Az "ősember" biztonságtechnikai eszköze," Hadmérnök, 11. évfolyam 4. szám 2016 december, pp. 216-221. (4 oldal).

[3] Kosztopulosz Andreász, „A pénz és a pénzrendszerek fejlődése," Szegedi Tudományegyetem Gazdaságtudományi Kar, SZTE GTK 2017/2018, 2018.

[4] „kiszamolo.hu," 04 03 2013. [Online]. Available: https://kiszamolo.hu/a-penz-rovid-tortenete/. [Hozzáférés dátuma: 05 05 2022].

[5] Divéki Éva, Keszy-Harmath Zoltánné, Helmeczi István, Innovatív fizetési megoldások, Magyar Nemzeti Bank: MNB Tanulmányok 85., ISSN 1787-5293, Budapest, 2010. május.

[6] OTPédia, 22 04 2022. [Online]. Available: https://www.otpedia.hu/melyviz/ugyvitel/hogyan-forradalmasitotta-szamitogep-bankolast_1/. [Hozzáférés dátuma: 11 05 2022].

[7] Múlt-kor, 17 05 2021. [Online]. Available: https://mult-kor.hu/reggel-kilenctol-az-orokkevalosagig-igy-kezdodott-a-bankautomatak-tortenete-20210519. [Hozzáférés dátuma: 11 05 2022].

[8] Statista, 03 2021. [Online]. Available: https://www.statista.com/statistics/1228757/online-banking-users-worldwide/. [Hozzáférés dátuma: 11 05 2022].

[9] Múlt-kor, OTPédia, 28 05 2021. [Online]. Available: https://www.otpedia.hu/digitalis-korunk/fizetes/atm-sztori_2/. [Hozzáférés dátuma: 11 05 2022].

[10] Cyber Crime In The 21st Century, „UKEssays," 27 04 2017. [Online]. Available: https://www.ukessays.com/essays/media/cyber-crime-in-the-21st-century-media-essay.php#citethis. [Hozzáférés dátuma: 11 05 2022].

[11] Jade Fell, „Hacking through the years: a brief history of cyber crime," 13 03 2017. [Online]. Available: https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/. [Hozzáférés dátuma: 11 05 2022].

[12] Mark Oliver, „10 Early Hackers From Before The Invention Of The Home Computer," 14 05 2018. [Online]. Available: https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/. [Hozzáférés dátuma: 11 05 2022].

[13] Crypto Museum, „Bombe, Breaking the Enigma cipher," 23 11 2012. [Online]. Available: https://www.cryptomuseum.com/crypto/bombe/. [Hozzáférés dátuma: 11 05 2022].

[14] „The 7 worst cyberattacks in history," Dvice, 22 09 2010. [Online]. Available: https://web.archive.org/web/20141112155600/http://www.dvice.com/archives/2010/09/7_of_the_most_d.php. [Hozzáférés dátuma: 19 05 2022].

[15] Matthew Wills, WWII and the First Ethical Hacker, Technology and Culture, Vol. 45, No. 1 (Jan., 2004), pp. 80-101: The Johns Hopkins University Press and the Society for the History of Technology, 2017.

[16] John Simons, „Unplugged! The biggest hack in history, ZDNet," 01 10 1999. [Online]. Available: https://www.zdnet.com/article/unplugged-the-biggest-hack-in-history/. [Hozzáférés dátuma: 16 05 2022].

[17] Robert Herjavec, „Cybercrime Magazine," 17 07 2019. [Online]. Available: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/. [Hozzáférés dátuma: 11 05 2022].
[18] Anthony, Technology means business, „5 Examples of Cyber Crime and the Cyber Criminals Who Got Caught," 09 04 2018. [Online]. Available: https://blog.tmb.co.uk/cyber-criminals. [Hozzáférés dátuma: 16 05 2022].
[19] Vuk Mujovic, „Where does cybercrime come from? The origin & evolution of cybercrime, Le VPN," 18 10 2018. [Online]. Available: https://www.le-vpn.com/history-cyber-crime-origin-evolution/. [Hozzáférés dátuma: 16 05 2022].
[20] The Wall Street Journal, „Russian Hacker Is Sentenced To 3 Years in Citibank Heist," 24 02 1998. [Online]. Available: https://www.wsj.com/articles/SB888360434859498000. [Hozzáférés dátuma: 16 05 2022].
[21] Richard Esposito, Jason Ryan, „ABC News, FBI: Crime Ring Stole $70 Million Using Computer Virus," 16 07 2010. [Online]. Available: https://abcnews.go.com/Blotter/fbi-crime-ring-stole-70-million-computer-virus/story?id=11777873. [Hozzáférés dátuma: 16 05 2022].
[22] Dan Elsom, „The Sun," 11 10 2017. [Online]. Available: https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/. [Hozzáférés dátuma: 16 05 2022].
[23] David Jones, Jim Finkle, „U.S. indicts hackers in biggest cyber fraud case in history, Reuters," 26 07 2013. [Online]. Available: https://www.reuters.com/article/us-usa-hackers-creditcards/u-s-indicts-hackers-in-biggest-cyber-fraud-case-in-history-idUSBRE96O0RI20130726. [Hozzáférés dátuma: 16 05 2022].
[24] Kim Zetter, „That Insane, $81M Bangladesh Bank Heist, WIRED," 17 05 2016. [Online]. Available: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/. [Hozzáférés dátuma: 16 05 2022].
[25] Gulyás Olivér, Kiss Gábor, „Kiberbiztonság 2021-ben a bankszektorban és a pénzügyi szervezeteknél," Biztonságtudományi szemle, pp. 83-90, 2022. IV. évf. 1. szám.

TRUST THROUGH THE STUDY OF GAME THEORIES

A BIZALOM A JÁTÉKELMÉLETEK VIZSGÁLATÁN KERESZTÜL

VALOCIKOVÁ, Cyntia[1]

Abstract

Why do we choose trust, even if it makes us vulnerable to the other party? Advanced trust can lead to success or failure, depending on the behavior of the trustee. Because the trustee cannot control the trustee, the result is uncertain. Complex researches on trust examines various aspects that directly or indirectly affect an individual's trust decisions. In my study, I examine trust through game theory, which analyzes the relationships and decisions of participants through a disciplinary approach to mathematics. Different experiments in game theory place trust in a light that finds connections between trust, altruism, and cooperation through practical circumstances and decision-making situations. The study is a collection of existing game theory experiments and their results. A review of the literature and theory provides a basis for subsequent primary research, which also examines trust in the form of an experiment, based on the results presented in the study.

Keywords

trust, game theory, trustgame, prisoner's dilemma, reciprocity

Absztrakt

Miért választjuk a bizalmat, még akkor is, ha ezáltal sebezhetővé vállunk a másik féllel szemben? A megelőlegezett bizalom sikeres vagy sikertelen eredményt hozhat, mely függ a megbízott személy viselkedésétől. Mivel a bizalmat adó nem irányíthatja, vagy ellenőrizheti a megbízottat, a végkifejlet bizonytalan. A bizalom összetett kutatása különböző aspektusokat vizsgál, mely közvetlen vagy közvetett módon hatással van az egyén bizalmi döntéseire. Tanulmányomban a bizalmat a játékelmélet szemüvegén keresztül vizsgálom, mely a matematika egy diszciplináris megközelítésével elemzi a résztvevők kapcsolatát és döntéseit. A különböző játékelméleti kísérletek olyan megvilágításba helyezik a bizalmat, mely gyakorlati körülmények és döntési helyzetek által talál rá a bizalom, az altruizmus és az együttműködés közötti összefüggésekre. A tanulmány meglévő játékelméleti kísérletek és azok eredményeinek gyűjteménye. A szakirodalmi és elméleti áttekintés alapot nyújt egy későbbi primer kutatáshoz, mely ugyancsak kísérlet formájában vizsgálja a bizalmat a tanulmányban bemutatott eredményekre alapozva.

Kulcsszavak

bizalom, játékelmélet, bizalomjáték, fogolydilemma, reciprocitás

[1] valocikova.cyntia@uni-obuda.hu | ORCID: 0000-0003-3541-4222 | PhD student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztoságtudományi Doktori Iskola

BEVEZETÉS

A bizalom fogalmi keretei nem tekinthetőek egyértelműnek, vagy egységesnek, hiszen számos megközelítés létezik a bizalom definiálására. Das & Tang (2004) a kockázat oldaláról közelítették meg a bizalmat, mely szerint a bizalom pozitív vélekedés a másik fél magatartásáról akképpen, hogy a körülmények bármiféle változása esetén az nem cselekszik opportunista módon. A bizalom tehát azt jelenti, hogy önkéntesen kockázatot vállalunk abból fakadóan, hogy sebezhetővé válunk a másik fél által [1]. A bizalom interdiszciplináris megközelítésben, a tudomány számos ágában jelen van, gazdaság-, társadalom- akár a biztonságtudományban egyaránt. Egy korábbi tanulmányban [2] szemügyre vettük az altruizmus, a bizalom és a biztonság kapcsolatát, melyben a bizalmi döntésekben rejlő kockázat és sebezhetőség útján az egyén biztonsága (fizikai és lelki) veszélybe kerülhet. Ahogyan a bizalom definíciói, a bizalom alapú kutatások sokrétűsége is korlátot szabhat a konzisztens elemzésnek. A játékelmélet egy máig széles körben alkalmazott, interdiszciplináris megközelítés, melyről elmondható, hogy olyan stratégiai problémák elmélete, amely két vagy több szereplős döntés irányoz elő [3]. A játékelméleti modellek felépítésében fontos szerepet kap az együttműködés, hiszen a kooperatív viselkedés teljesülése esetén a kölcsönösen előnyös megoldás a játékosnak nagyobb hasznot biztosíthat, ezáltal pedig feltételezhető egyfajta személyközi bizalom kialakulása. Az ilyen típusú megelőlegezett bizalom a nem feltétlenül önérdekkövető, mind inkább altruista magatartás sajátossága [4] [5]. A tanulmányban főképp szakirodalmi elemzésre szorítkozom, meglévő játékelméleti kutatások vizsgálatán keresztül vizsgálom az egyének bizalomhoz és reciprok viselkedéséhez fűződő magatartását.

A FOGOLYDILEMMA STRATÉGIÁJA

A játékelmélet úgy definiálható, mint annak a dinamikának a vizsgálata, amelyen keresztül a játékosok közötti együttműködés kialakulhat és fennmaradhat. A központi kérdés mindig a társadalmi dilemmák megoldására tett kísérlet a következő kérdésekre alapozva:

- Mi akadályozza meg az egyén önérdekű magatartását abban, hogy a csoport érdekeit megsértse?
- Mi tévesztheti meg a szereplőket az optimálistól eltérő döntések meghozatalában?

E társadalmi dilemmák megoldásával foglalkozó irodalom egy narratívájára összpontosítok első lépésben, a fogolydilemmára. Sokszereplős fogolydilemmaként említhető a közlegelők tragédiája, melynek problémái a túlzott használatból eredő negatív externáliákhoz kapcsolódnak, vagy a „szabadlovas" problémához, amelyben a jószágért nem fizető emberek azokhoz továbbra is hozzáférhetnek. Ez egyben elvezet ahhoz a társadalmi dilemmához, amit a közlegelők tragédiájaként vált köztudottá. Garrett Hardin (1968) ismertette ezt a modellt tanulmányában, amelyben felvetette, hogy ha az egyén saját érdekeit szem előtt tartva, a csoport szereplőitől függetlenül meríti ki a megosztott erőforrásokat, az ellentétes a csoport hosszú távú érdekeivel. Azzal érvelt, hogy a közös erőforrást használók önzésének szabadsága az erőforrások gyors kimerítéséhez vezet. Az önzés mohó viselkedésformája hosszútávon katasztrófába sodorja a társadalmat, ám az önzetlen viselkedés evolúciós előnyökkel jár [6].

Robert Axelrod (1984) főként a fogolydilemma elméletével foglalkozott, és bírálta az önérdekű döntéshozatalt támogató elméleteket. Legfőbb munkája egy a „*The Evolution*

of Cooperation", amelyet William D. Hamiltonnal közösen írt 1981-ben, azzal a céllal, hogy továbbfejlessze a darwini individualista evolúcióelméletet. Bemutatják, hogyan világíthatja meg a játékelmélet és a számítógépes modellezés az erkölcsi filozófia bizonyos aspektusait, különösen az egyének szerepét a csoportokban, az önzés és altruizmus biológiáját, valamint az evolúciós szempontból előnyös együttműködés megvalósítását. A társadalmi és biológiai környezetben ugyanazok az egyének többször találkozhatnak, mely lehetővé teszi számukra a visszaemlékezést a korábbi interakció néhány aspektusára. Ez azonban nem jelenti azt, hogy a több egyénnel való interakció során, mindenkivel egyformán kell bánni. A diszkrimináció gyakori viselkedési minta, mely által az egyén megkülönböztető bánásmódban részesíti a másik egyént vagy csoportot, az együttműködő magatartást jutalmazással, míg a dezertáló magatartást büntetéssel sújtja. Axelrod modellje egy iterált Fogolydilemma, mely a lehetséges stratégiák sokkal gazdagabb halmazával dolgozik [4].

Leghatékonyabb stratégiája az ún. „*TIT FOR TAT*" (TFT), amely egy kölcsönösségen alapuló utánzó stratégia. A stratégia első lépése minden esetben a kooperáció, majd minden ezt követő lépés a másik résztvevő előző döntésének lemásolását jelenti. A stratégia megköveteli azonban, hogy az együttműködés fejlődéséhez szükség van a folyamatos és hosszú távú interakcióra a résztvevők között. Hamilton evolúciós elméletei között a kölcsönösség elmélete szerint, együttműködés alakulhat ki egymással nem biológiai kapcsolatban lévő egyének között is. Állítása azon a tényen alapszik, hogy számos biológiai környezetben ugyanaz a két egyed többször is találkozhat. A játékelméleti megközelítés azonban igen széles skálája alkalmazható a valóságban. Kezdve egy igen egyszerű organizmussal, mely rendkívül egyszerű stratégiát követ. A baktériumok nem tudnak „emlékezni" vagy „értelmezni" a változások összetett múltbeli sorozatát, és valószínűleg nem tudják megkülönböztetni a kedvezőtlen vagy előnyös változások alternatív eredetét, így a viselkedésük az együttműködés szintjén pusztán biológiai. Ahogy haladunk felfelé az evolúciós létrán, a játékelméleti magatartás viszont egyre gazdagabbá vállik. Azokban az esetekben, amikor egy szervezet nem képes felismerni azt az egyént, akivel korábban interakciót folytatott, egy helyettesítő mechanizmus gondoskodik arról, hogy minden interakciója ugyanazzal a játékossal történjen, mely megtehető úgy, hogy folyamatos kapcsolatot tart fenn a másikkal. Egy más megközelítésben, az egyének egymás közötti kapcsolata úgy is biztosítható, ha a találkozás helyszíne rögzített. Ez a módszer olyan feltételeket teremt, amelyek mellett a kölcsönösségen alapuló együttműködés a biológiai rendszerekben a résztvevők előrelátása nélkül is kialakulhat [7].

A TFT kooperatív és dezertáló magatartást is feltételező stratégia azonban, annál fogva, hogy a játékos döntése a másik játékos előző döntésétől függ, reciprocitáson is alapul. Ha a játékos kooperál, akkor a kooperáció pozitív válaszát kapja jutalmul, ha dezertál, akkor a dezertálás negatív válaszát kapja büntetésül. Habár a játékelméletben a TFT stratégiája egyértelmű, a társadalomban bekövetkezhet egy váratlan akadályozó körülmény félrekommunikáció vagy félreértés által, amikor a játékos "botlása" nem követi a betervezett elméleti lépéseket. Ekkor a játék stratégiáját követve, a játékosok egy megtorlási spirálba kerülnek, amely folyamatos dezertálást eredményez. A TFT nagylelkű viszonzó stratégiája viszont teret enged a dezertálás kooperációval való válaszára. Vannak azonban további, lehetséges stratégiái a TFT modellnek, mint:

- az aszinkron (ekkor a játékosok egymás után hozzák meg a döntéseket, nem pedig egyszerre);

- a bűnbánó (kooperatív stratégia, a játékosok a kölcsönös dezertálást megbánják, így kooperálnak);
- a számító (a lehető legtöbb pontszámot akarja elérni a játékos, így mindaddig megismétli az előző forduló lépéseit, míg nyerésre áll, amint viszont veszít a cselekvését az ellenkezőjére változtatja);
- a haragtartó stratégia (kooperál mindaddig, míg nem tapasztalja a dezertálást, miután engesztelhetetlenül dezertáló magatartással sosem tér vissza a kooperáláshoz) [8].

A négy alapstratégia azonban, amely a leggyakrabban felmerülő cselekvési alternatívákat kínálja az utánzó, a bűnbánó, a számító és a haragtartó. Az alapvető kooperációs minta, mindig a kooperáció másolását írja elő, dezertálásnál azonban a négyféle választási lehetőség, esetünkben a négy alapstratégia, mely leírja a játékelmélet kooperációs potenciálját. Axelrod játékelméleti modellje a bizalom egyfajta evolúciójának is tekinthető, hiszen a játékosok döntéseit nagymértékben befolyásolja a másik játékos iránt érzett bizalma, melyet nem csupán az ismeretség szintje, hanem például a tapasztalat, értékek és készségek, szociális kapcsolat, és sok egyéb aspektus is meghatározza. A TFT stratégia során kialakul a kölcsönösen előnyös kapcsolatok hálója, ahol az együttműködés terjedésével lassan kialakul a bizalom. Az ilyen típusú együttműködésben megfigyelhető a reciprok altruizmus megjelenése. A kooperálás támogatása növeli a mások jóléte iránti törődést, mely szoros kapcsolatban áll az altruista viselkedéssel. Az altruizmus a leghatékonyabban a rokoni kapcsolatokon keresztül tartható fenn, a szocializáció által fenntartott altruizmus nem rokoni kapcsolatok esetén kockázatosabb. Axelrod szerint, az altruizmus költsége csökkenthető, ha az első körben az egyén mindenki irányába altruistán viselkedik, majd csupán azokkal, akik hasonló viselkedést mutatnak, mint a pozitív reciprocitás biztosításaként [9].

Az evolúciós játékelmélet, amelyben az együttműködést hűséggel jutalmazzák, a természetes kiválasztódással látszólag összeegyeztethetetlen altruista viselkedési stratégiákat mutat. Evolúciós értelemben az altruizmus akkor fordul elő, amikor az egyén önként csökkenti saját fitneszét (alkalmasságát, vagyis annak valószínűségét, hogy rövidtávon szaporodjon), hogy javítsa egy másikét. Az altruizmus leggyakrabban olyan állatoknál fordul elő, amelyek szociális viselkedést mutatnak, például figyelmeztető hívást adnak le veszély esetén, ételt osztanak ínséges időben, vagy kolóniaképző viselkedést követnek. A figyelmeztető hívások és az ételosztás előnyei a reciprok altruizmuson alapulnak, pontosabban remélve, hogy a másoknak nyújtott előnyöket a jövőben jutalomként visszakapják. Az a madár, amely figyelmeztető jelzést ad, átmenetileg észlelhetővé vállik a ragadozók számára, így csökken az azonnali fitnesze, azonban ugyanazon madárnak a jövőben előnyös lehet más madarak hasonló figyelmeztető hívása. A kölcsönös altruizmus az élőlények többszöri kölcsönhatásán alapul, a játékelmélet pedig keretet ad a reciprok altruizmus evolúciójához. Az iterált fogolydilemma jellemzően kis létszámú játékosok közötti ismétlődő interakciókat foglal magában; az altruizmus azonban a közvetett és közvetlen kölcsönösség kombinációja révén még nagy csoportokban is fejlődik. Közvetlen kölcsönösségről akkor beszélünk, ha ugyanaz a két személy ismételten interakcióba lép egymással, míg közvetett kölcsönösségről akkor beszélünk, ha a későbbi interakciók különböző egyének között jönnek létre. Míg az altruista viselkedés átmenetileg csökkentheti az egyén fitneszét, a reciprok altruizmus növeli azt az egyén egész élete során [10] [11].

A BIZALOMJÁTÉK, AVAGY A BIZALOMKUTATÁS MEGHATÁROZÓ ESZKÖZE

A kooperatív interakcióban a bizalom nagyobb valószínűséggel jelenik meg. Számos kutatás foglalkozott már a bizalom és a reciprocitás közötti összefüggésekkel a játékelméleti modellek alkalmazásán keresztül, ezek közül a bizalomjáték, amely a viselkedés tudományok kiemelkedő kísérleti paradigmájává vált. A bizalomjátéknak számos interpretációja van, alapesetben a játék két egymásnak idegen résztvevő között folyik, ahol az első játékos dönt, a második játékos pedig ehhez mérten reagál. A játék kifizetése abban az esetben nem nulla, ha az első játékos bizalmat szavaz a másodiknak, és felajánl egy bizonyos összeget. A második játékos pedig ehhez mérten dönthet, hogy dezertál, vagy a reciprocitást választja [12] [13].

Evans et al. (2008) személyközi bizalmat vizsgáló kísérletükben arra az eredményre jutottak, hogy a magas bizalmi szinttel rendelkező egyének könnyebben mutattak altruista viselkedést [14]. Glaeser et al. (2000) hasonló eredményeket értek el, kutatásukban arra az eredményre jutottak, hogy a magas bizalmi szinttel rendelkező egyének kölcsönös csereként tekintenek a kooperatív interakcióra [15]. Burnham et al. (2000) felismerték, hogy a bizalomra és a reciprocitásra is egyaránt hatással van a társadalmi keretek kialakítása. A reciprocitás mértéke megváltozott, amikor a játék során, az egyik játékos felé intézett utasítások a másik játékost partnernek, nem pedig ellenfélnek nevezték. Amikor a játék kooperatív interakciót feltételezett, a bizalom és a reciprocitás egyaránt valószínűbb volt [16]. Brülhart és Usunier (2012) megvizsgálták, hogy az altruizmus milyen hatással van a bizalomjáték során alkalmazott kifizetésekre. A módosított bizalomjátékban csoportosították a második lépés játékosait "szegényekre" és "gazdagokra", mely során a kezdő játékosok egyidejűleg játszottak mindkét csoport tagjaival. A vizsgálat során megfigyelték a kifizetések módosulását a két csoport irányába. Feltételezték, hogy a magasabb kifizetések a szegények irányába fog mozdulni, mely bizonyítaná az altruista viselkedést és a bizalom felülemelkedését önérdekkövető döntéssel szemben. A kutatás során az is bizonyosságot nyert, hogy a játékosok a döntéseik során nem feltétlenül a tökéletes Nash-egyensúly szerint cselekednek, és hogy a kifizetések mértéke mögött nem az önzés a domináns motiváció [17]

A bizalmat vizsgáló játékelméleti modellek alkalmazásakor, az első játékos pénzküldési hajlamát a bizalom mértékeként értelmezik a kutatók, mivel ez magában foglalja a bizonytalan végkifejlet elfogadását a másik játékos viselkedésével kapcsolatos elvárások alapján. A második játékos válaszát pedig a megbízhatóság mércéjének tekintik, hiszen ez nem jár sebezhetőséggel vagy bizonytalansággal; ehelyett a játékos arról dönthet, hogy betartja-e a kölcsönösség normáját. Összhangban azzal az elképzeléssel, hogy a bizalom erkölcsi szempontból elengedhetetlen magatartás, a bizalommal foglalkozó kutatások is alátámasztják, hogy az emberek társadalmi kötelességüknek érzik bizalmat szavazni idegeneknek. Az általános bizalomnak reputációs következményei vannak, ezáltal az idegenekbe vetett bizalom erkölcsi "*kötelesség*" [5].

A magas bizalmi szinttel rendelkező egyéneket társaik erkölcsösebbnek tekintik, erősítve azt az elképzelést, hogy az emberek azért bízhatnak másokban, mert úgy érzik, ez a helyes magatartás. A magas bizalmi szinttel rendelkező egyének jobb szociális készségekkel rendelkeznek, és ezeket a készségeket önző vagy önzetlen célok elérésére egyaránt felhasználhatják. Ebben a megközelítésben a bizalom erkölcsi, azonban nem pusztán önfeláldozó magatartás. Az egyén úgy tekinthet a bizalomra, mint egy társadalmilag racionális

meggyőződésre, amely mindkét fél számára előnyös. Az egyensúlyelméletet követve pedig azok az egyének, akik az erkölcstelen csoportokat megbízhatónak tartják, maguk is erkölcstelennek tekinthetők. A megbízható és megbízhatatlan csoportok megkülönböztetésének képessége hatással van a reputációra. Hasonló azonban a megítélése a feltétlen és feltételes bizalmat szavazó egyéneknek is, a feltétlen bizalmat szavazó egyének megítélése negatívabb azoknál, akik képesek felmérni a csoportok megbízhatóságát [18] [19]. Az általános bizalom és a megkülönböztető képesség független hatással van a személy észlelésére, azonban az egyén intelligenciájával szoros kapcsolatban áll. Az intelligens egyének hatékonyabban mérik fel, mikor lehet bízni másokban, ezekkel a tapasztalatokkal pedig több pozitív szociális tapasztalatot is szereznek, melyek magasabb általános bizalomhoz vezetnek. Az általános bizalom az erkölcs és a szocializáltság jelenségével is összefüggnek. Azok az egyének, akik bíznak másokban, nagyobb valószínűséggel tekinthetőek erkölcsösnek és társaságkedvelőnek, egyúttal pedig szakértőknek. Az erkölcsös egyéneknek pozitívak a szándékaik, becsületesek és jóindulatúak; a szociális egyének magas interperszonális készségekkel rendelkeznek, barátságosak és extravertáltak; és a szakértő egyének pedig intelligensek és hatékonyak. Az erkölcs tehát az egyén azon szándékára utal, hogy segítsen, vagy éppen ártson másoknak, a szocializáltság és a szakértelem pedig az egyén azon képességeire utalnak, hogy az erkölcsös szándékokat érvényesítse [20] [18] [21].

Evans és Krueger (2011) megvizsgálták, hogy a kockázat és a perspektíva figyelembe vétele hogyan hat a bizalomra és a reciprocitásra. A bizalomjátékban az első játékos választ a status quo és a bizalom lépései között. A status quo esetén a játék véget ér, és mindkét játékos a P kifizetést kapja. A bizalom választása esetén a játék a következő szakaszba lép, amelyben a második játékos választ a reciprocitás és az árulás között. Reciprocitás esetén mindkét játékos megkapja az R kifizetést; árulással az első játékos S, a második játékos pedig T kifizetést kap. A játékban ezek a kifizetések a következőképpen épülnek fel: $T>R>P>S$. Az első játékos tisztában van azzal, hogy a bizalom jobb eredményt hoz, mint a status quo ($R>P$), de nincs garancia arra, hogy a reciprocitás megvalósul. Az árulás azonban olyan eredményhez vezet, amely az első játékost rosszabb helyzetbe hozza, mint a status quo ($S<P$), az első játékosnak tehát el kell döntenie, hogy érdemes-e vállalnia ezt a kockázatot. A bizalomjátékban hozott döntéseknél a kifizetés három összetevőből épül fel. A bizalom első két összetevője a költség és a haszon, amelyek együttesen kapcsolódnak a sebezhetőség és a kockázat fogalmához. Az első játékos potenciális költsége a status quo és az árulás közötti különbség ($P–S$), a potenciális haszna pedig a kölcsönösség és a status quo közötti különbség ($R–P$). A bizalom harmadik összetevője a kísértés, amely az árulás és a reciprocitás közötti különbség a második játékos kifizetésénél ($T–R$). Ez a különbség jelzi annak valószínűségét, hogy a második játékos viszonozza-e a bizalmat, elmondható tehát, hogy a kísértés mértéke előrejelzi a reciprocitást. A bizalom összetevőinek azonosítása elősegíti a döntéshozatal folyamatának elemzését. A klasszikus játékelméleti megközelítés feltételezi, hogy mindkét játékos szigorúan önérdekkövető. Feltételezve, hogy a döntés csupán a kifizetés értékétől függ, egyértelmű, hogy a második játékos az árulást választja, ha az első játékos megbízik benne ($T>R$). Ebből kiindulva azonban az első játékos a status quot választja, hiszen $P>S$. A bizalomjátékban ebből az következik, hogy az egocentrikus költségek és hasznok nagyobb hatást gyakorolnak a döntésre, mint a második játékos kísértése az árulásra. A kísérlet során az első játékos hasznának bármilyen növelése ugyancsak nö-

velte a második játékos árulásra irányuló kísértését is, ezáltal csökkentve a reciprocitás valószínűségét, azonban a haszon növelése ennek ellenére növelte a bizalomra eső választás esélyét. Ha a játékos magasnak ítéli a személyes kockázatát a bizalom választása esetén, gyors döntést hozva nagyobb valószínűséggel választja a status quot. A bizalomra eső választás mértékét azonban ezesetben nem befolyásolja a második játékos árulásra irányuló kísértésében történt változás, így a játékosok bizalmatlanok maradnak még akkor is, ha csekély a kísértés. Ezzel szemben, ha a személyes kockázat alacsony, a játékos figyelembe veszi a másik játékos árulásra irányuló kísértését, ami miatt nagyobb valószínűséggel fontolják meg, hogy bizalmat szavaznak. Két lehetséges beavatkozás csökkentheti ezt az ellentétet. Az első az, hogy hangsúlyosabbá váltható a második játékos nézőpontja. Az első játékos automatikusan elutasítja a második játékos perspektíva-szemlélését, ha a bizalomra eső választásnak magas a kockázata, azonban a perspektíva-szemlélet elősegítheti a bizalmat. Magas kockázat esetén az egocentrikus döntés eredménye a kooperáció elutasítása a másik résztvevő szempontjának figyelembe vétele nélkül. Az interakció átstrukturálható a kockázat csökkentése esetén is a költségek csökkentésével vagy a haszon növelésével [22].

A bizalomjáték során a játékelméletben alkalmazott racionalitás írja elő a bizalom alapú döntéseket, melyek függnek a lehetséges kockázattól (egocentrikus költségek és hasznok) és a reciprocitás valószínűségétől (a megbízott kísértése a dezertálásra). Ahogyan Axelrod módszerében is kiderült, a haszon növelése növeli a bizalmat, még akkor is, ha ez egyben a másik egyén kísértését is fokozza a dezertálásra. Ez a feltevés arra utal, hogy a játékosok nem veszik teljes mértékben figyelembe a másik fél szempontját. A bizalom kanonikus definíciója — a sebezhetőség és az elvárás szempontjából — magában foglalja a várható értékek becslését, tehát hogy a racionális döntéshozó egyenlő arányban foglalkozik a következménnyel (sebezhetőség) és a valószínűséggel (elvárás). Az internetes kereskedelem példáján keresztül megfigyelhető, hogy a vevők és az eladók korlátozott kommunikációval és látszólagos anonimitással lépnek egymással kapcsolatba. A fizikai formájában még nem látott áru megvásárlására való hajlandóság megköveteli a vevőtől, hogy hallgatólagosan bízzon az eladóban. A vevő számára azonban nem az eladó látszólagos megbízhatósága a legfontosabb szempont, hanem a vásárlás vélt költsége és haszna. Ezért olyan feltételek biztosítása, amelyek korlátozzák a bizalom látszólagos kockázatát, mint a garancia, hatékony módszer az ismeretlen felek közötti bizalom megteremtésében. Az egocentrikus döntés kockázata csökkenthető oly módon is, ha az eladó hangsúlyozza az árulás képtelensége iránti álláspontját. Az a megállapítás nem újkeletű, hogy a stratégiai döntéseket egocentrikus érdekek motiválják, azonban új megvilágításba helyezhető, amint a személyközi bizalom kontextusában is értékeljük. Így, a példára szorítkozva elmondható, hogy az eladó kísértése a megbízható viselkedés legfontosabb előrejelzője. A másik fél nézőpontjának figyelembevétele stratégiai önérdek, mivel a bizalmat elsősorban az egocentrikus kockázatvállalás motiválja, azonban a nézőpont figyelembe vétele akkor számít, ha a döntéshozó a kockázatot kellően alacsonynak találja. A racionális bizalom azonban megköveteli a sebezhetőség és az elvárás értékelését [23] [22] [24]. A személyközi bizalom mindkét féltől függ, így az két szempont alapján vizsgálható: mások általános megbízhatósága és az egyén saját általános hajlandósága a másokra irányuló bizalomra. A bizalom egy másik formája, az „egyéb-központú bizalom", mely arra vonatkozik, hogy mások mennyire tekinthetők megbízhatónak. Azonban általános jelenség, hogy az egyén múltbeli tapasztalatai alapján — ahol a bizalom megerősítést nyert, vagy inkább megtört — különbözteti meg a bizalomra

méltó és a bizalmatlannak tekinthető egyéneket. Eszerint, az ilyen típusú bizalom kevésbé függ a másik személy egzisztenciájától, mint inkább az egyén saját biztonságérzetének és megbecsülésének észlelésétől. Ha a bizalomra való hajlandóság magas, akkor az tükrözi a világról alkotott optimista felfogást és a másokkal szembeni általános pozitív elvárásokat [25]. Az egyén bizalom szintjének vizsgálatához a múltbeli bizalmi magatartások konkrét esetei is iránymutatást adnak, míg a megbízhatóságot a másokba vetett általános bizalom mutatja. A családi állapothoz, a szociális készségekhez és a karizmához kapcsolódó egyéni tulajdonságok nagyban befolyásolják a bizalmi döntéseket, hiszen ez „egyéni társadalmi tőke", amely tükrözi a társadalmi helyzetekből származó megtérülést.

Egy későbbi kutatásban Evans és Beest (2017) a bizalmat és a reciprocitást a nyereség-veszteség kontextusában vizsgálták hasonló játékelméleti modell alkalmazásával, mint az előző vizsgálatokban. A két körös bizalomjátékban a kifizetések módosításával vizsgálták a nyereség-veszteség, a bizalom és a reciprocitás kapcsolatát. Az első körben minden döntéssel csak nyerhettek a játékosok 0 induló ponttal, azonban a döntéseik befolyásoltak a nyeremény mértékét, míg a második körben csak veszíthettek a játékosok, ugyancsak a döntéseikhez mérten. A játékosok viselkedése arra mutatott, hogy növekedett a bizalom, ellenben a reciprocitással, ha a döntés következménye veszteség volt. A veszteségek keretében hozott bizalmi döntések kevésbé voltak érzékenyek a várható érték változásaira. A reciprocitást eredményező döntések esetében pedig kevésbé voltak érzékenyek a pénzügyi kísértés mértékére. A nyereség-veszteség keretezés nem befolyásolta a reciprocitás valószínűségét, de befolyásolta a reciprocitást eredményező döntések meghozatalának módját. A bizalomra és a reciprocitásra vonatkozó döntések attól függnek, hogy az emberek az eredményeket a nyereség vagy a veszteség szemszögéből érzékelik-e. A veszteségek kellemetlenek, de a megnövekedett bizalom váratlan hasznát is hordozhatják, továbbá veszteséggel járó bizalmi és reciprok döntések kevésbé kiszámíthatóak, mint a nyereséggel járó döntések. Az eredményeik együttesen azt sugallják, hogy a nyereség-veszteség keretezésnek egyedi interperszonális következményei vannak, melyek gazdasági és társadalmi folyamatokhoz kapcsolódnak [26].

ÖSSZEFOGLALÁS

Az együttműködés az egyének között kölcsönösen előnyös helyzetet teremt, mely támogatja a bizalom növekedését. A kooperáció azonban nem csupán a bizalmat segíti elő, hanem támogatja az altruista viselkedést. A magas bizalmi szinttel rendelkező egyének könnyebben mutatnak törődést mások iránt, és az együttműködésre pozitív csereként tekintenek és a másik felet partnernek tekintik. Az ilyen típusú bizalmat nem feltétlenül az önzés, vagy a magasabb jutalom igérete mozgatja, mind inkább a társadalmi kötelességük teljesítése. Ezáltal növekszik a társadalmi reputációjuk, azonban egy-egy rossz megítélés a megbízhatatlan csoportok felé önmagukat is rossz színben tüntetik fel. Az intelligencia szoros kapcsolatban áll az egyén bizalmi megítélésével, a helyes ítélőképességgel pedig több pozitív szociális tapasztalatot jelent. Mindez hozzájárul, hogy az egyént erkölcsösnek, szociálisnak és egyúttal hozzáértőek tekintsenek. Racionális bizalom esetén a sebezhetőség és az elvárás is előzetesen értékelésre kerül, azonban az általános bizalom egocentrikus kockázatvállaláson alapul, mely nem minden esetben értékeli ezeket a tényezőket, tehát nem veszi figyelembe a másik fél szempontjait. Az egyének múltbéli tapasztalatai is erősen hatással vannak a bizalmi döntéseikre, azonban a személyes kockázat mérlegelése is nagymértékben

befolyásolja a döntést. Magas kockázat esetén az egyén nem szavaz bizalmat, ha viszont a kockázatát alacsonynak ítéli, akkor nagyobb esély van a bizalomra. Ebben az esetben figyelembe veszi a másik egyén szempontját, és mérlegeli a sebezhetőséget, a lehetséges végkifejletet és az elvárást. Önmagában, a másik fél perspektíva-szemlélése növelné a bizalmat, azonban ha az egyén a személyes kockázatát túlzónak érzi, elveti ennek lehetőségét. A kooperációt a nyereség-veszteség kontextusába helyezve világossá vált, hogy a bizalom könnyebben kialakul a veszteség kontextusában, hiszen az egyén nagyobb hasznot remélt a kooperációból a kockázat ellenére, mintha meghátrált volna. A bizalom számos formája létezik — csupán néhány, mely a tanulmányban szerepel a személyközi, racionális vagy egyéb központú bizalom — melyeket különböző attribútumok befolyásolnak. A tanulmányban a bizalmi döntések vizsgálata a játékelméleti kísérleteken keresztül rávilágított olyan fontos attribútumokra, melyek hasznos segítséget nyújtanak a jövőben elvégzendő primer kutatásomhoz.

FELHASZNÁLT IRODALOM

[1] T. Das and B. Teng, "The risk-based view of trust: a conceptual framework," *Journal of Business and Psychology,* vol. 19, no. 1, pp. 85-119, 2004.

[2] C. Valociková és J. Velencei, „TRANSDISCIPLINARY APPROACH TO FIND CONNECTIONS BETWEEN ALTRUISM AND SAFETY," *Safety and Security Sciences Review ,* %1. kötet2, %1. szám1, pp. 87-97, 2020.

[3] J. Neumann és O. Morgenstern, Theory of games and economic behavior, Princeton, New Jersey: Princeton University Press, 1944.

[4] R. Axelrod, The Evolution of Cooperation, New York: Penguin Books, 1984.

[5] A. M. Evans és P. P. Van de Calseyde, „The Reputational Consequences of Generalized Trust," *Personality and Social Psychology Bulletin,* %1. kötet44, %1. szám4, pp. 492-507, 2018.

[6] G. Hardin, „The Tragedy of the Commons," *Science New Series,* %1. kötet162, %1. szám3859, pp. 1243-1248, 1968.

[7] R. Axelrod és W. D. Hamilton, „The evolution of Cooperation," *Science,* %1. kötet211, %1. szám4489, pp. 1390-1396, 1981.

[8] R. Axelrod, „On Six Advances in Cooperation Theory," *Analyse & Kritik,* %1. kötet22, pp. 130-151, 2000.

[9] A. Rapoport, D. A. Seale és A. M. Colman, „Is Tit-for-Tat the Answer? On the Conclusions Drawn from Axelrod's Tournaments," *PLoS ONE,* %1. kötet10, %1. szám7, p. 11, 2015.

[10] C. C. Cowden, „Game Theory, Evolutionary Stable Strategies and the Evolution of Biological Interactions," *Nature Education Knowledge,* %1. kötet10, %1. szám6, p. 6, 2012.

[11] G. Marosán, „Tit-for-tat – az egyéni és a közösségi siker alapja," in *Együttműködés – versengés*, V. Rab, Szerk., Budapest, Gondolat Kiadó, 2010, pp. 105-116.

[12] S. Karajz, „Az altruista viselkedés modellezési lehetőségei," *Észak-magyarországi Stratégiai Füzetek XV.,* pp. 82-91, 2018.

[13] J. Engle-Warnick és R. L. Slonim, „The evolution of strategies in a repeated trust game," *Journal of Economic Behavior & Organization,* %1. kötet55, %1. szám4, pp. 553-573, 2004.

[14] A. M. Evans és W. Revelle, „Survey and behavioral measurements of interpersonal trust," *Journal of Research in Personality,* %1. kötet42, p. 1585–1593, 2008.

[15] E. L. Glaeser, D. I. Laibson, J. A. Scheinkman és C. L. Soutter, „Measuring trust," *Quarterly Journal of Economics,* %1. kötet115, %1. szám3, pp. 811-846, 2000.

[16] T. Burnham, K. McCabe és V. L. Smith, „Friend-or-foe intentionality priming in an extensive form trust game," *Journal of Economic Behavior and Organization,* %1. kötet43, pp. 57-73, 2000.

[17] M. Brülhart és J.-C. Usunier, „Does the trust game measure trust?," *Economics Letters,* %1. kötet115, pp. 20-23, 2012.

[18] A. M. Evans és J. I. Krueger, „Bounded Prospection in Dilemmas of Trust and Reciprocity," *Review of General Psychology,* %1. kötet20, %1. szám1, pp. 17-28, 2016.

[19] J. F. Landy, J. Piazza és G. P. Goodwin, „When It's Bad to Be Friendly and Smart: The Desirability of Sociability and Competence Depends on Morality," *Personality and Social Psychology Bulletin,* %1. kötet42, %1. szám9, pp. 1272-1290, 2016.

[20] P. Sturgis és P. Smith, „Assessing the Validity of Generalized Trust Questions: What Kind of Trust are we Measuring?," *International Journal of Public Opinion Research,* %1. kötet22, %1. szám1, pp. 74-92, 2010.

[21] A. Ben-Ner és F. Halldorsson, „Trusting and trustworthiness: What are they, how to measure them, and what affects them," *Journal of Economic Psychology,* %1. kötet31, pp. 64-79, 2010.

[22] A. M. Evans és J. I. Krueger, „Elements of trust: Risk and perspective-taking," *Journal of Experimental Social Psychology,* %1. kötet47, pp. 171-177, 2011.

[23] A. Ben-Ner és L. Putterman, „Trust, communication and contracts: An experiment," *Journal of Economic Behavior & Organization,* %1. kötet70, %1. szám1-2, pp. 106-121, 2009.

[24] C. Snijders és G. Keren, „Determinants of trust," in *Games and human behavior,* D. V. Budescu, I. Erev és R. Zwick, szerk., Mahwah, NJ, Lawrence Erlbaum, 1999, pp. 355-385.

[25] M. Zhang, „Assessing Two Dimensions of Interpersonal Trust: Other-Focused Trust and Propensity to Trust," *Frontiers in Psychology,* %1. kötet12, pp. 1-11, 2021.

[26] A. M. Evans és I. v. Beest, „Gain-loss framing effects in dilemmas of trust and reciprocity," *Journal of Experimental Social Psychology,* %1. kötet73, pp. 151-163, 2017.

[27] L. Berek, T. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.

DEVELOPMENT OF SECTORAL REGULATION OF ACCESS AND SURVEILLANCE SYSTEMS IN THE SHADOW OF THE GDPR

A BELÉPTETŐRENDSZEREK ÉS A MEGFIGYELŐRENDSZEREK ÁGAZATI SZABÁLYOZÁSÁNAK FEJLŐDÉSE A GDPR ÁRNYÉKÁBAN

FÁBIÁN Péter[1]

Abstract

Nowadays, property protection is already unthinkable without electronic security devices and systems. We no longer have to think about complex, industrial systems, but simple security solutions with purposeful functionality have also appeared in the smallest flats and condominiums. Whatever the complexity of the solution used, they are used for detection and signaling in terms of their primary function, and increasingly for the evaluation, storage and management of data generated during the performance of previous tasks. Nowadays, simple plug & play cameras and other "gadgets" that can be ordered from the internet have become part of it. With the development of information technology, these tools have not only communicated with other IT tools and systems, but have become such tools themselves. They also process and store data while performing their function. In my study, I review and evaluate the development and current issues of regulation of the application and use of the two key security tools in the light of the provisions of the GDPR.

Keywords

Access control system, surveillance system GDPR

Absztrakt

Napjainkban a vagyonvédelem már elképzelhetetlen elektronikus biztonságtechnikai eszközök és rendszerek nélkül. Már nem csak komplex, ipari rendszerekre kell gondolnunk, hanem a legkisebb lakásokban, társasházakban is megjelentek az egyszerű, célirányos funkcionalitással rendelkező biztonságtechnikai megoldások. Bármilyen komplexitású legyen az alkalmazott megoldás, elsődleges funkciójukat tekintve érzékelésre és jelzésre szolgálnak, és egyre jellemzőbben az előző feladatok teljesítése során felmerült adatok értékelésére, tárolására és kezelésére. Napjaink részév lettek az internetről rendelhető egyszerű plug & play kamerák, egyéb „kütyük". Az informatika fejlődésével már az ezen eszközök nem csak kommunikálnak egyéb IT eszközökkel és rendszerekkel, hanem maguk is ilyen eszközökké váltak. Funkciójuk betöltése során adatot dolgoznak fel és tárolnak is. Tanulmányomban a két meghatározó biztonságtechnikai eszköz alkalmazására és használatára vonatkozó szabályozás kialakulását és aktuális kérdéseit tekintem át és értékelem a GDPR rendelkezések tükrében.

Kulcsszavak

Beléptetőrendszer, megfigyelőrendszer GDPR

[1] fabianpeter@topcopgroup.com | ORCID: 0000-0003-0640-6557 | Founder, Top Cop Group | Alapító, Top Cop Group

BEVEZETÉS

Munkám során alapvetően a magánbiztonság terén felmerülő kérdések kerülnek a fókuszba, a rendőrség, a közterület-felügyelet, egyéb hatóságok, a közösségi közlekedés szervezői stb. által alkalmazott biztonságtechnikai eszközökkel kapcsolatos szabályokra nem térek ki. Az értekezés elején nagyon fontosnak érzek 2 kardinális tényt rögzíteni: Az egyik lényeges körülmény, hogy az informatikai, technológiai fejlődés gyakorlatilag korlátlan lehetőségeket biztosít az elektronikai jelzőrendszerek fejlesztésével, gyártásával foglalkozók számára. A másik – az előbbivel valamelyest összefüggő – sajátosság pedig, hogy nem létezik egységes, a vizsgálandó terület valamennyi szegmensét lefedő, vagy akár csak keretjelleggel bíró szabályozás: az, aki naprakész kíván lenni, annak a legváltozatosabb jogágak területére eső, nemritkán eltérő mélységű jogszabályokkal kell megismerkednie.

ALKOTMÁNYJOGI ALAPOK

A biztonság optimális szintjének elérése és tartós biztosítása egyszerre feladata a közösségnek és az egyénnek [1]. A magánbiztonság fogalma a rendszerváltást megelőző időszakban értelmezhetetlen volt, szocialista viszonyok között a gazdasági rend alapját „a termelési eszközök társadalmi tulajdona" jelentette [2]. Az 1989. évi XXXI. törvénnyel bevezetett alkotmánymódosítás nyomán nyert csak elismerést az elv, mely szerint *„a köztulajdon és a magántulajdon egyenjogú és egyenlő védelemben részesül"* [3]. A 2012. január 1-jén hatályba lépett Alaptörvény a Nemzeti Hitvallás című részében ugyanakkor már azt is leszögezi, hogy *„a polgárnak és az államnak közös célja […] a biztonság, a rend […] kiteljesítése"* [4].

A köztulajdon és a magántulajdon védelme, a közbiztonság és a magánbiztonság ilyenformán szorosan összefonódik, és ez további kötelezettségeket keletkeztet a jogalkotó számára: olyan módon kell szabályozni a magánbiztonság körébe eső tevékenységeket, hogy egyfelől biztosítva legyen az egyén számára a jog arra, hogy indokolt esetben megvédhesse saját magát és javait, másfelől kizárja annak lehetőségét, hogy e jog gyakorlása mások jogainak és szabadságának sérelmével járjon. Ebből következően a magánbiztonság kérdése elválaszthatatlan az emberi jogok és szabadságok témakörétől, különösképpen azért, mert a magánbiztonság körében (is) alkalmazásra kerülő eszközök között akadnak olyanok, melyek használata adott esetben érinti a polgárok személyiségi jogait [5]. Márpedig, miként azt az Alaptörvény deklarálja, mindenkit megillet a személyes adatok védelméhez való jog [6].

A VAGYONVÉDELEM JOGI KERETEI

Magyarországon a szocialista időszakban a vagyonvédelem egyet jelentett a társadalmi tulajdon védelmével, ennek egy sajátos eszközét jelentette az üzemrendészeti tevékenység, az ezt szabályozó 6/1988. (II. 12.) MT rendelet [7] egészen 2000. január 31-ig maradt hatályban [8]. Időközben elfogadták a vagyonvédelmi tevékenységet engedélyező – ugyanakkor a magánnyomozást kifejezetten tiltó – 24/1987. (VII.22) MT. számú rendeletet, mely a vagyonvédelem terén folytatható tevékenységek sorában kifejezetten nevesítette a biztonsági berendezések és rendszerek tervezését, készítését, felszerelését, karbantartását, javítását, és a mindezekkel összefüggő tanácsadás [9]. A magánbiztonság szervezeti, intéz-

ményi kereteit a személy-, vagyonvédelmi és magánnyomozói tevékenység szabályait meghatározó 1998. évi IV. törvény (a továbbiakban: VSzVMt.) teremtette meg [10]. Mind az 1988-as minisztertanácsi rendelet, mind az 1998-as törvény esetében igaz, hogy bár (viszonylagos részletességgel) meghatározta a hatálya alá tartozó foglalkoztatottak feladat- és jogkörét, ám megfigyelő-, jelző- és más hasonló berendezések telepítésére, alkalmazására vonatkozó szabályokat nem tartalmazott.

Ilyen szabályozási előzményeket követően fogadta el az Országgyűlés a többször módosított, jelenleg is hatályban lévő, a személy-, a vagyonvédelmi, valamint a magánnyomozási tevékenység szabályait meghatározó 2005. évi CXXXIII. törvényt (a továbbiakban: SzvMt.) [11].

A továbbiakban külön-külön megvizsgálom, miként alakult az elmúlt három évtizedben az elektronikus megfigyelő rendszerek, a beléptető rendszerek alkalmazására vonatkozó és kiterjedő szabályozása.

BELÉPTETŐ RENDSZEREK

A beléptető rendszerek jelentik az egyik legmeghatározóbb szegmensét az elektronikai védelemnek, azt hivatottak biztosítani, hogy a védendő területre csak az arra feljogosított személyek léphessenek be. Ennek megfelelően három+ egy fő funkciójuk van: a belépni kívánó személy azonosítása; annak megállapítása, hogy az illető rendelkezik-e belépési jogosultsággal; végül az áthaladás szabályozása, és azzal kapcsolatos adatok rögzítése. A beléptető rendszer további funkciókkal is bővíthető, így – többek között – rendszámfelismerésre, munkaidő nyilvántartásra is szolgálhat [12].

Az Szvtv. rendelkezett az elektronikus beléptető rendszerek alkalmazásának feltételeiről, a törvény szerint ilyen rendszert csak azon esetekben lehet működtetni, ha a védett területre nem léphet be mindenki, csak az, akit a belépésre, ott-tartózkodásra jogszabály vagy a terület felett rendelkező erre feljogosított. A törvény meghatározta az elektronikus beléptető rendszer működésével kapcsolatban keletkezett adatok (a belépésre jogosultak személyes adatai, a belépés időpontja stb.) kezelésére, illetve törlésére vonatkozó szabályokat [13].

A GDPR rendelettel összefüggésben módosított SzVMt. igen lakonikusan rendelkezik az elektronikus beléptetőrendszereket illetően, pusztán csak annyit rögzít, hogy ilyen rendszer kizárólag a megbízóval kötött szerződés alapján és csakis akkor alkalmazható, ha a védett területre jogszabályi rendelkezés vagy a terület felett diszponáló személy döntése folytán az arra feljogosítottakon kívül más nem léphet be [14]. Az adatkezelésre, adatfeldolgozásra vonatkozó szabályokat – a kamerás megfigyelésnél tárgyaltakkal megegyezően – a megbízási szerződés, valamint a GDPR rendelet és az Info.tv. vonatkozó szakaszai tartalmazzák.

A beléptető rendszerek alkalmazása kiemelt jelentőséggel bír a sportrendezvények esetében. A sportról szóló 2004. évi I. törvény taxatíve meghatározza azokat a kritériumokat, melyeket a rendezvényre belépni kívánó személynek teljesítenie kell, így például rendelkeznie kell az illetőnek érvényes belépőjeggyel, nem állhat sem alkoholos befolyásoltság, sem sportrendezvények látogatásától eltiltás hatálya alatt [15].

Ugyancsak feltétele a belépésnek, hogy az érintett tudomásul vegye: a rendezvény során kép- és hangfelvételt készíthetnek róla [16]. Ez utóbbi szabályt – egy sor más, szigorú rendelkezéssel egyetemben – a sporthuliganizmus elleni fellépés jegyében iktatták be a

sporttörvénybe 2011-ben [17]. A 2011. évi CIV. törvénnyel bevezetett módosítás 2013 júliusától kötelezővé tette a szervezők számára a fokozott- és a kiemelt biztonsági kockázatú mérkőzéseken az egyedi azonosításra alkalmas beléptetési, illetve ellenőrző rendszerek alkalmazását, valamint a névre szóló belépőjegyek és bérletek értékesítésének kötelezettségét [18]. A 2014 júliusától hatályos törvénymódosítás pedig felhatalmazta a beléptetési rendszert alkalmazó szervezőt arra, hogy személyazonosításra alkalmas klubkártyát (úgynevezett szurkolói kártyát) vezessen be, és annak kiváltását kötelezővé tegye a rendezvényre belépni szándékozók számára [19]. A kártya biometrikus adatokból (például ujjlenyomat, vénalenyomat) generált kódok révén látja el a személyazonosító funkciót, és miután a rendszer össze van kötve a rendőrség által vezetett sportrendészeti nyilvántartással, így az azonosítás során egyértelműen kiderül, ha a belépés megtagadására okot adó körülmény áll fenn [20].

ELEKTRONIKUS MEGFIGYELŐ RENDSZEREK

Az elektronikus (praktikusan kamerával felszerelt) megfigyelő rendszerek olyan zártláncú televízió rendszerek, melyek képsorait kizárólag a hálózatba bekapcsolt tagok láthatják. A megfigyelő eszközök lehetnek beltéri vagy kültéri, fix telepítésű vagy vezérelhető kamerák, maga a megfigyelés lehet jelen idejű, melynek során az operátor a monitorokat figyeli, de megtörténhet egyidejűleg a felvétel rögzítése is, adathordozón vagy merevlemezen [21].

Az elektronikus vagyonvédelem körében a kamerás megfigyelő rendszerek jogi szabályozása a legkiterjedtebb és kétségkívül ez az a téma, amely leginkább a közvélemény érdeklődésének homlokterébe esik: az, hogy egy tűzjelző rendszer felszerelésekor milyen jogszabályokat kell figyelembe venni, aligha foglalkoztatja az átlagembereket, ám az, hogy megfigyelhet-e valakit a munkáltatója munkavégzés közben vagy egy áruházi kamera rögzítheti-e a próbafülkében tartózkodókat, sokak számára érdekes lehet.

Az SzVMt. feljogosította a vagyonőrt vagyonvédelmi biztonságtechnikai rendszerek,[22]. azon belül is elektronikus megfigyelőrendszerek alkalmazására (térkamerás megfigyelésre), azzal a kitétellel, hogy ez utóbbira kizárólag magánterületen, valamint magánterületnek a közönség számára nyilvános részén van mód, és csakis abban az esetben, ha ehhez a megfigyelt személy – kifejezetten, illetve ráutaló magatartással – hozzájárult [23]. Az SzvMt. ugyanakkor tételesen meghatározta azt is, milyen adatkezelési célok érdekében lehet kép- és/vagy hangrögzítéssel járó elektronikus megfigyelőrendszert alkalmazni, e körbe tartozott az emberi élet, a testi épség, személyi szabadság védelme, a vagyonvédelem, a veszélyes anyagok őrzése, valamint a fizetési, üzleti, bank- és értékpapírtitok védelme [24]. Mindezek mellett az SzvMt. azt is kimondta, hogy a vagyonőr az elektronikus megfigyelőrendszerek alkalmazása során köteles az adatvédelmi törvény [25] előírásait betartani, és a megfigyelés tényéről, valamint az ezzel összefüggő, törvényben felsorolt körülményekről (a felvétel készítésének, tárolásának céljáról, jogalapjáról stb.) a közönséget megfelelő módon tájékoztatni [26]. A SzvMt. szigorú határidőket határozott meg a felvételek törlésére vonatkozóan: a felhasználásra nem kerülő felvételeket főszabály szerint a rögzítés utáni három munkanap elteltével kellett törölni, megsemmisíteni, speciális esetekben ez a határidő harminc napra, illetve hatvan napra emelkedett (például hatvan napig lehetett tárolni a felvételt, ha a rögzítés pénzügyi szolgáltatás védelmét célozta) [27].

2016. május 24-én lépett hatályba az Európai Unió általános adatvédelmi rendelete (GDPR), alkalmazását kétéves türelmi időszakot követően kellett megkezdeni [28]. Ezzel összefüggésben módosították az SzvMt. vonatkozó rendelkezéseit is. Így – 2019. április 26-i hatállyal – kikerült a törvényből az adatkezelési célokat tartalmazó taxáció és az adatkezelés időtartamát érintő időkorlát, e kérdéseket érintően a továbbiakban az adatkezelő jogosult dönteni, értelemszerűen a GDPR rendelet és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info.tv.) [29]. alapelveinek és szabályainak a figyelembevételével. Ilyen elv különösen az adattakarékosság, a célhoz kötöttség, a korlátozott tárolhatóság elve [30].

Elektronikus megfigyelőrendszer immár kizárólag magánterületen telepíthető és működtethető, a magánterület közönség előtt is megnyitott részén nem [31]. Éppen ezért a módosítás hatályba lépését követően azokat a kamerákat, melyek a közterület magánterületként használt részére voltak irányítva, le kellett szerelni, ez volt a helyzet például a közterületre kinyúló éttermi teraszokat, autóparkolókat megfigyelő kamerák esetében. Nem változott ugyanakkor az a rendelkezés, mely szerint nem alkalmazható kamerás megfigyelés olyan helyen, ahol az az emberi méltóság sérelmével járhat, a törvény által adott példálózó jellegű felsorolás szerint kiterjed a tilalom a mosdókra, öltözőkre, próbafülkékre, illemhelyekre, kórházi szobákra [32].

Ugyancsak kikerültek a törvényből a megfigyelés által érintett személyek jogaival összefüggő garanciális rendelkezések (mint amilyen például a megfigyelés tényére, az adatok kezelésének módjára vonatkozó tájékoztatási kötelezettség), az érintettek a továbbiakban az Info.tv. alapján érvényesíthetik az adatkezeléssel kapcsolatos jogaikat (előzetes tájékozódáshoz való jog, hozzáféréshez való jog stb.) [33].

Ugyancsak az Info.tv.-ből következnek az adatkezelő kötelezettségei. Így – többek között – az adatkezelő köteles érdekmérlegelési tesztet lefolytatni, és a teszt eredményétől függően dönteni arról, üzemelteti-e a kamerát, illetve milyen időkorlát mellett kezeli a megfigyelés során keletkezett adatokat, köteles továbbá adatvédelmi hatásvizsgálatot lefolytatni, melynek során beazonosításra kerülnek az érintettek alapvető jogainak érvényesülését befolyásoló kockázatok [34]. Azt, hogy a vagyonőr adatkezelőnek vagy adatfeldolgozónak tekintendő, a megbízási szerződésben határozzák meg a felek a GDPR, illetve az Info.tv. vonatkozó rendelkezései alapján. A gyakorlatban ez utóbbi megoldás a tipikus, a vagyonőrök jellemzően adatfeldolgozóként látják el az elektronikus megfigyelőrendszerrel kapcsolatos teendőket [35].

Speciális szabályok vonatkoznak a munkahelyeken, a társasházak közösen tulajdonolt részein, valamint a sportrendezvényeken folytatott kamerás megfigyelésekre.

Kamerás megfigyelés társasházban

A társasházakról szóló 2003. évi CXXXIII. törvény releváns rendelkezései ugyancsak a GDPR rendelet átültetése során módosultak [36]. Változatlanul érvényes az a szabály, mely a közgyűlésnek az összes tulajdonos kétharmados beleegyező szavazatával meghozott határozatához köti a kamerás megfigyelés lehetőségét. Az adatkezelési célra, valamint a felvételek tárolására vonatkozó időkorlátok – hasonlóan az SzVMt.-hez – kikerültek a törvényből, az ezen kérdésekkel kapcsolatos döntések az adatkezelő kompetenciájába tartoznak, akit szintén terhel az érdekmérlegelési teszt, adatvédelmi hatásvizsgálat lefolytatá-

sának kötelezettsége. A kamera elhelyezésével kapcsolatos tilalmakat is tartalmaz a törvény. Így a kamerát nem lehet külön tulajdonban álló ingatlan ajtajára, ablakára irányítani, még akkor sem, ha az a közös tulajdonú, közös használatú részen van elhelyezve, továbbá nem folytatható kamerás megfigyelés a közös tulajdonú helyiségekben sem, ha a megfigyelés az emberi méltóság sérelmével járhat (ez a helyzet mosdó, illemhely stb. esetében) [37].

Kamerás megfigyelés munkahelyen

A munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) felhatalmazása alapján a munkáltató korlátozhatja a munkavállaló személyiségi jogait, így például a munkavállalót is értintő kamerás megfigyelést alkalmazhat, erre azonban kizárólag akkor kerülhet sor, ha ez a korlátozás „a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos" [38]. A 2019 áprilisa előtt is létező szabályt a GDPR rendelet hazai jogba történő átültetésekor kiegészítették, az új rendelkezések tájékoztatási kötelezettséget írnak elő a munkáltató számára (például a megfigyelt területekkel, a szükségesség-arányosság teszt eredményével, az adatkezeléssel kapcsolatos munkavállalói jogokkal kapcsolatosan) [39]. Lényeges, hogy a munkavállaló kizárólag a munkatevékenységével összefüggésben ellenőrizhető, privát szférája a munkahelyen sem figyelhető meg. Ebből következően a „munkahelyi magánélet" szokásos helyszínein, így az ebédlőben, az öltözőben, a pihenésre szolgáló helyiségben kamera nem helyezhető el, a jogosulatlan kamerás megfigyelés, illetve e körülmény elhallgatása pedig adott esetben a munkavállaló rendkívüli felmondását megalapozó indokként szolgálhat [40].

Kamerás megfigyelés sportrendezvényen

A sportrendezvények során történő kamerás megfigyelés lehetőségét a 2011-ben, a futballhuliganizmus elleni fellépés jegyében tették lehetővé, ekkor még csak a sportrendezvény szervezőjét, illetve rendezőjét, a 2019 januárjától hatályos újabb módosítással pedig már az utazó sportszervezet képviselőjét is feljogosították arra, hogy a rendezvény helyszínén, továbbá szurkolói parkolókban és a közterületnek a beléptetésre várakozó nézők által elfoglalt részén ilyen jellegű megfigyelést folytasson. E megfigyelés specialitását jelenti egyfelől az, hogy a kamerák rögzíthetők a szervező, illetve a rendező testén is, a másik sajátosság pedig, hogy a kiemelt biztonsági kockázatú sportrendezvények, valamint a fokozott biztonsági kockázatú labdarúgó rendezvények esetében a rendőrség határozza meg a kötelezően telepítendő kamerák számát, illetve a kamerák felszerelésének helyét [41]. Lényeges, hogy a kamerás megfigyelés tényéről és az adatkezelésről a nézőt többszörösen is tájékoztatni kell: a klubkártyán piktogram használatával, egyébként pedig szöveges formában kell az erről szóló hirdetményt elhelyezni a belépőjegyen, a bérleten, a sportlétesítményen kívül, valamint annak területén, a magyar nyelv mellett angolul is [42].

Láthatjuk tehát, hogy míg az SzVMt. alapján folytatott kamerás megfigyelések a jelenleg hatályos szabályok szerint közterületet még csak részben sem érinthetnek, addig a sportrendezvényeknél – ha azt a vagyonbiztonság és a résztvevők személyi biztonsága indokolttá teszi – az ilyen típusú megfigyelés kötelező jelleggel kiterjednek a közterület meghatározott részeire. Van egy másik lényeges különbség is az SzVMt. és az Stv. szerinti szabályozás között: az SzVMt.-ből a GDPR rendelet adaptálásával összefüggésben kikerültek a rögzített adat tárolására vonatkozó időkorlátok, nem úgy azonban az Stv. esetében. A sporttörvény értelmében ugyanis a szervező (rendező, utazó sportszervezet) köteles a rendőrség felhívásában közölt időtartamig, de legfeljebb hatvan napig megőrizni a felvételeket;

a rendőrség ilyen tartalmú felszólítást a rendezvény befejezését követő százhúsz órán belül intézhet a kötelezetthez, feltéve, hogy az adatok tárolását büntető- vagy szabálysértési eljárás lefolytatása teszi szükségessé [43].

ÖSSZEGZÉS

A munkámban az elektronikus megfigyelő rendszerek, a beléptető rendszerek alkalmazásának és használatának szabályozását, e szabályozás időbeli alakulását tekintettem át a rendszerváltozást megelőző évektől kezdődően napjainkig. Vizsgálódásaim középpontjában az adatkezeléssel kapcsolatos jogszabályok álltak. A dolgozat témaköre több önálló, folyamatos átalakulásban lévő folyamat és kérdéskör érintettségével is rendelkezik. Fontos itt említeni, hogy az informatikai fejlődés révén nem csak korábban „vágy és álom" szinten megfogalmazott funkciókkal rendelkező „okos eszközök" széles palettájával bővült a biztonságtechnikai eszközök tárháza, hanem ezek ára mára olyan szintre lépett, hogy bárki számára elérhetőek, használatuk pedig annyira egyszerűsödött, hogy a hétköznapi emberek számára elterjedté váltak. Nem különben új lehetőségeket nyitva a magánbiztonság, a bűnüldözés és vagyonvédelem szegmenseiben.

Ezen folyamatokkal synergikus viszonyban a technikai fejlődés azon tényszerűsége, hogy az információ adat szintű tárolása az informatikai eszközök révén egyre egyszerűbb és olcsóbb. Egyre több adatot használunk napi életünkben és tároljuk információ formájában valamilyen informatikai eszközön, kiváltképen igaz ez a vizsgált biztonságtechnikai eszközök esetében. Ezzel párhuzamosan a társadalmi fejlődés révén az egyén és a társadalom egésze tekintetében- pontos az információ alapú társadalmiasodás miatt is- nagyon szenzitív és kényes kérdés lett az adatok kezelése, tárolása, használata és megismerése.

Ezen jelenség indikálta az a folyamatot, amelynek eredménye az ezzel kapcsolatos közösségi szabályozás az adatok védelmére, amely minden tagországra nézve egységesen kötelező érvényű, s amelyet GDPR néven ismerhettünk meg.

A kamerák által rögzített felvételekkel összefüggő adatvédelmi kérdéseket korábban az SzVMt. szabályozta, ám a GDPR 2018-as alkalmazásba lépésével a jogalapokat illetően számottevő változások következtek be, melyekre a magyar jogalkotó a személy- és vagyonvédelmi törvény deregulációjával reagált.

A szabályozás valós társadalmi igény látens szintű kielégítését szolgálta, a legmagasabb jogforrási szinten. Mint a minden reguláció, amely folyamatokat szabályoz, feladatokat ró a jogalkalmazóra és mindenkire, akire kiterjed. A vagyonvédelem tekintetében úgy érzem számos olyan korlátozó és szűkítő rendelkezést tartalmaz, amely az nem szolgálja a rendelkezés létrehozásának alapját jelentő társadalmi igényt, illetve más társadalmi értékek eredményes megvédését szolgálni hivatott módszerek eszköztárát, indokolatlanul korlátozza. Több esetben pedig csak érdemtelen, felesleges adminisztrációs terhet ró ránk.

Nem vitatható, hogy az információ alapú világunkban szükséges volt az adatok védelmének egységes szabályozása, azonban az elmúlt közel 5 év tapasztalati szerint, lassan időszerű lenne a rendelkezése áttekintése és aktualizálása.

FELHASZNÁLT FORRÁSOK

[1] Berek Lajos (2014): Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Budapest. 15.o
[2] Takács Albert (2019): „Valljuk, hogy a polgárnak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése.” In: Patyi András (szerk.): Rendhagyó kommentár egy rendhagyó preambulumról. Dialóg Campus, Budapest. 340. o.
[3] 1949. évi XX. törvény a Magyar Népköztársaság Alkotmányáról. 1989.10.22-ig hatályban volt szöveg. 6. § (1) bek.
[4] 1949. évi XX. törvény a Magyar Népköztársaság Alkotmányáról. Az 1989. évi XXXI. évi törvénnyel megállapított, 1989.10.23-án hatályba lépett szöveg. 9. § (1) bek.
[5] Magyarország Alaptörvénye (2011. április 25.) Nemzeti Hitvallás.
[6] Takács (2019) i.m. 339–340. o.
[7] Magyarország Alaptörvénye (2011. április 25.) VI. cikk.
[8] 6/1988. (II. 12.) MT rendelet a közületi szervek rendészeti tevékenységéről.
[9] Kántás Péter (2007): A közrend elleni jogsértések természetéről. Doktori értekezés. Eötvös Lóránd Tudományegyetem Állam- és Jogtudományi Kar, Budapest.
[10] 24/1987. (VII.22) MT. számú rendelet a vagyonvédelmi tevékenységről és a magánnyomozás tilalmáról 2. § (1) bek. a) pont.
[11] 1998. évi IV. törvény a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról.
[12] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.
[13] Berek (2014) i.m. 19.
[14] Szvtv. 32. § Hatálytalan 2019.04.26-tól.
[15] Szvtv. 32. § Megállapította: 2019. évi XXXIV. tv. Hatályos: 2019.04.26-tól.
[16] 2004. évi I. törvény a sportról (a továbbiakban: Stv.) 71. § (1) bek.
[17] Stv. 71. § (1) bek. g) pont. Beiktatta: 2011. évi CIV. tv., hatályos: 2011.09.01-től.
[18] 2011. évi CIV. törvény a sporthuliganizmus jelensége elleni fellépés érdekében szükséges egyes törvények módosításáról.
[19] Stv. 72. § Megállapította: 2011. évi CIV. tv., hatályos: 2013.07.01-től.
[20] Stv. 72/A. § Megállapította: 2014. évi XXVII. tv., hatályos: 2014.07.04-től.
[21] Stv. 72/A. § (8) bek. Megállapította: 2019. évi CXXXV. tv., hatályos: 2019.01.07-től.
[22] Takács (2014) i.m. 6. o.
[23] SzVMt. 26. § (1) bek. e) pont.
[24] SzVMt. 30. § (2) bek.
[25] SzVMt. 31. §
[26] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (a továbbiakban: Avtv.).
[27] SzvMt. 28. § (2) bek. Hatálytalan 2019.04.26-tól.
[28] SzvMt. 31. § Hatálytalan 2019.04.26-tól.
[29] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről

és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) OJ L 119, 4.5.2016, 1–88. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679
[30] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
[31] EU) 2016/679 rendelet 5. cikk.
[32] SzvMt. 30. § (2) bek. Megállapította: 2019. évi XXXIV. tv. Hatályos: 2019.04.26-tól.
[33] SzvMt. 30. § (3) bek.
[34] Info.tv. 14. §
[35] Info.tv. 25. §
[36] Adatvedelmirendelet.hu: A GDPR-salátatörvény elfogadásával kapcsolatos főbb változások. 2019.04.12. Elérhető: https://www.adatvedelmirendelet.hu/adatvedelmi-rendelet/a-gdpr-salatatorveny-elfogadasaval-kapcsolatos-fobb-valtozasok/
[37] Hasonlóképpen változtak a lakásszövetkezetek esetében is a kamerás megfigyelésre vonatkozó előírások. 2004. évi CXV. törvény a lakásszövetkezetekről.
[38] 2003. évi CXXXIII. törvény a társasházakról 25. §
[39] 2012. évi I. törvény a munka törvénykönyvéről (a továbbiakban: Mt.) 10. § 2019. évi XXXIV. törvénnyel megállapított szöveg, hatályos 2019.04.26-tól.
[40] Mt. 11/A. § 2019. évi XXXIV. törvénnyel megállapított szöveg, hatályos 2019.04.26-tól.
[41] BH2014. 89.; Bankó Zoltán – Berke Gyula – Kiss György – Szőke Gergely László (2019): Nagykommentár a munka törvénykönyvéről szóló 2012. évi I. törvényhez. Elérhető: Complex Jogtár
[42] Stv. 74. § (1) bek. Megállapította: 2018. évi CXXXV. tv., hatályos: 2019.01.01-től.
[43] Stv. 74. § (2) bek. Megállapította: 2018. évi CXXXV. tv., hatályos: 2019.01.01-től.

DISPOSABLE LOCKS, SEALS AND THEIR POSITION IN PROPERTY PROTECTION (PART 2)

EGYSZER HASZNÁLATOS ZÁRAK (PLOMBÁK) ÉS HELYZETÜK A VAGYONVÉDELEMBEN (2. RÉSZ)[1]

SZABÓ László András[2]

Abstract

I have been developing, manufacturing, and marketing disposable locks for almost twenty years. Suddenly this became the main profile of the business and I grew into it pretty slowly and realized that as almost always the products and activities underestimated by the public are the most difficult to dig into. There is always more and there is always someone who needs it. It must be protected, preserved, and made identifiable. In my study, I process legislation, standards and my own experience in both domestic and international scientific literature. Thus, this is a two-part expert study. In the second part, I review and place domestic and international regulations and standards in the complex system of property protection

Keywords

for one use locks, property protection, mechanical protection, standards, regulation

Absztrakt

Közel húsz éve foglalkozom egyszer használatos zárak (plombák) fejlesztésével, gyártásával és forgalmazásával. Hirtelen ez lett a fő profilja a vállalkozásnak én meg szép lassan belenőttem és rájöttem, hogy mint szinte mindig a közvélemény által alábecsült termékek és tevékenységek a legbonyolultabbak, ha beleássuk magunkat. Mindig van több és mindig van, akinek az kell. Védeni, őrizni és beazonosíthatóvá kell tenni. A témában nincsen se hazai, se nemzetközi tudományos szakirodalom a tanulmányomban jogszabályokat, szabványokat és saját tapasztalatot dolgozom fel. Igy ez egy két részből álló szakértői tanulmány. A második részben a hazai és nemzetközi szabályozást és szabványokat tekintem át és helyezem el a vagyonvédelem komplex rendszerében.

Kulcsszavak

egyszer használatos zárak, vagyonvédelem, mechanikai védelem, szabványok, szabályozás

[1] A tanulmány első része a Biztonságtudományi Szemle 2022. évi IV. évf. 1. számában jelent meg: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/206/176

[2] szabolandras.kmo@gmail.com | OROCID: 0000-0001-7957-0724 | doctoral candidate, Óbuda University Doctoral School for Safety and Security Sciences | doktorjelölt, Óbudai Egyetem Biztoságtudományi Doktori Iskola

BEVEZETÉS

Mint a Biztonságtudományi Szemle 2022. IV. évf. 1. szám Egyszer használatos zárak (plombák) és helyzetük a vagyonvédelemben (1. RÉSZ) című szaktanulmányban megismertük nincs olyan szabályozás, amely az egyszer használatos zárak működésére, annak megoldásaira, illetve a külső megjelenésre vonatkozna.

A tevékenysége végzése az egyszer használatos zárak fejlesztése, gyártása és forgalmazása nem engedélyköteles. Ezt a tevékenységet hivatalból nem ellenőrzi senki. Létezik ennél egy ennél nagyobb szabályozó és ellenőrző feladattal bíró egység ez pedig a piac. A felhasználók és megrendelők nagy egység, mely igényével és elvárásaival képes és tudja is szabályozni a zárakat. A gyártástól a felhasználáson keresztül a megsemmisítésig. Mellékletben ott található a piac legfontosabb és legnagyobb szegmensének a MÁV-nak egy 1986-os és egy 1997-es szabályozása. A 2003-as vasút liberalizáció után ezen szabályozásokat sokan átvették mivel a MÁV-nak már nem volt kötelessége minden vagon zárása. A MÁV szabályozást példának szeretném hozni hiszen minden szállítással foglalkozó cégnek Magyar Posta, TEFU, MASPED, MAHART, HUNGAROKAMION, mind rendelkezett valamilyen saját belső szabályozással. Ezek alapvetően nem tétek a példaként hozott MÁV-étól. Az ISO 17712/ 2003 Árufuvarozási konténerek- Mechanikus záró elemek szabvány, mely nem túl régi és a MABISZ egy Termék - Megfelelőségi Ajánlása. Ezen dokumentumokat nem fogom idézni. Megpróbálok egy általános áttekintést adni a rendszerváltás előtti időktől a jelenlegi helyzetig. Nem célom, hogy a szabályok, és szabványok puszta begépelése. A saját szakmai észrevételeimet és értelmezésemet szeretném leírni.

1986-os évtől kezdődött a változás, érződött, hogy történni fog valami. Akkor még ég nem beszélhetünk magántulajdonról csak köztulajdonról. Míg a Posta a pénzállítást végezte, a MÁV volt az egyetlen vasúti árufuvarozó cég mely nagy mennyiségben használ egyszer használatos zárakat. A MÁV-nál a megnevezés, Kocsizár Jelképes zár ás Biztonsági zár. A MÁV nagyon hamar felismerte, hogy mint minden a vasúton történő eseményt ezt is szabályozni kell. Nekem nagyon tetszik főképp a régi MÁV esetében az a katonai felfogás és precizitás a szabályozásban, ami jellemezte és jellemzi valamennyire ma is. Tehát leszabályozták a Kocsizárak a Jelképes és Biztonsági zárak raktározását, őrzését, dokumentálását, kiadását levételét és az 1997.es dokumentumban a megsemmisítését. Megjegyzendő, hogy a MÁV is csak műszaki paramétereket adott meg, hossz, átmérő, szakító szilárdság, feliratozás, jelzések elhelyezése és a manipuláció lehetőségének minél inkább csökkentése, és megnehezítése.

MAGYAR ÁLLAMVASUTAK ÁRUFUVAROZÁSI UTASÍTÁS C.1. SZÁMÚ UTASÍTÁS (ÁRUK, ÉLŐÁLLATOK ÉS HULLÁK FUVAROZÁSÁRA)

Érvényes: 1986 július hó 1. [1] Kivonat a Kocsizárakra vonatkozóan :

Mint a dokumentumban szerepel itt még a Kocsizár nevet használták és nem volt Biztonsági zár használatban ezért nem is kellett a két zárat megkülönböztetni. Itt még a sorszám mellett az állomásnév szerepel a Kocsizárak szalagján. (1990 után már az állomások külön számot kaptak és az lett beleütve a szalagba.) A kivitel az előző fejezetben említett úgynevezett patentzár. Igazából az a fontos, ahogy a zárakat a szolgálati helyekre való beérkezéstől egészen a felhasználás végén a levételig leszabályozza. Idegenkezűséget minél inkább megnehezítve, személyre és névre szóló felelőséggel a dokumentációval. Látszik,

hogy már akkor is benne volt az egyszer használatos zár a vagyonvédelem komplex rendszerében hiszen a kocsikisérőt kiegészítve és a két védelmi elem egymást váltva igyekezett az árufuvarozás rendszerén belül minél magasabb szinten az elvárásoknak megfelelni. Vasúti rendészet is volt hiszen szinte csak köztulajdon volt, melyet az állami vállalatok rendészeti szervezetei védtek és szervezték a védelmüket.

Sokszor még a mai napig is azzal próbálnak védekezni a rajtakapott fosztogatók, hogy már sérült volt a zár. Ezért fontos, mint a dokumentumban is szerepel a zárak feltétel előtti megvizsgálása a helyes és szakszerű feltétele. Hiszen, ha a feltétel közben megsérül, akkor rendkívüli esemény esetén már nem bizonyító erejű.

- Menet közbeni vizsgálat szemrevételezés, a zárak megléte és sérülésmentessége.
- Kocsizár levétele ugyanúgy szakszerűen, elvágva a szalagot egy tiszta vágással nem okozva sérülést a záron. Hiszen letépve, roncsolva el lehet leplezni azon sérüléseket, melyek az esetleges manipuláció közben keletkeztek.
- Kocsizár hiány sérülés, rendkívüli esemény. Jegyzőkönyvezni, megtenni a szükséges intézkedéseket.

A VÁM zárat már akkor is használták, de megjelentek a magánzárak is." A Vasút engedélyével magánlakattal lezárva" engedély birtokában tehették meg. A MÁV akkor még minden szállítmányt felülzárt.

Szerintem, aki ma egyszer használatos zárakat használ legyen az vasúti, közúti, banki, vízi vagy légi úti szállítmányozó vagy speditőr a fenti szabályozást alkalmazza még ha nem is tud róla mert azóta ez terjedt el a legjobban, illetve alapja a későbbi szabályozásoknak.

KOCSILEZÁRÁSOK

(Utasítás az Árufuvarozási Üzletszabályzat 11.§. (2) bek. és 48.§. (3) bek. végrehajtására) 1997. november 15.-től hatályos. Nagyon fontos három új elem jelenik meg ebben a szabályozásban.

A Kocsizáraknál megjelenik a csoportosítása. Jelképes zár, Biztonsági zár, speciális lezárási eszköz. Mint láttuk eddig csak, mint kocsizárakról beszéltünk. A MÁV igényelte egy újfajta műanyag zár és egy drótköteles biztonsági zár bevezetését és használatát. Már tudjuk a jelképes zár csak az illetéktelen felnyitás jelzésére szolgál a biztonsági zár pedig bizonyos mértékű védelmet is ad. Alapvetően a használat köre a lezárandó kocsi vagy konténer tartalmának az értéke. Felmerülhet, hogy a fosztogatók számára nem e figyelemfelhívó, ha egy biztonsági zárat látnak a konténeren. Sajnos az, de az élőerős őrzéssel együtt jól leszabályozva van rá esély, hogy megelőzzük a fosztogatást, a rendkívüli eseményt.

Továbbá az, hogy belekerült a dokumentumban a vasúton a MÁV-nál használatos zárak képe és megnevezése, illetve az egyéb engedélyezett zárak megnevezése márkaneve. Itt már a magántulajdon, a magánfeladások és a magáncégek jelen vannak a piacon azt befolyásolják és ők adják a megrendelési állomány nagy részét. Nem lehet elvárni egy magáncégtől sem, hogy lezárja a szállítmányát ez megmarad a MÁV kezében. Felelősség biztosítást, vagyon biztosítást is csak a zárak alkalmazásával együtt kötnek a MÁV-val a biztosítók. De megtiltani sem lehet a magáncégeknek, hogy lezárják a szállítmányaikat. Marad a párhuzamos zárás, felülzárás. Voltak törekvések a zárás MÁV részére való előírásának az eltörléséről, de végül nem jártak sikerrel.

Kocsizárakat nem kell használni, ha a szállítmányt, vagont kocsi kisérővel látják el. A MÁV-nak mindig volt rendészete és a Vasútőr, Mávőr vállalkozások is megjelennek. Az egész piacon minden szegmensében jelen vannak és egyre inkább teret nyernek a vagyonvédelmi vállalkozások.

A kocsizárak felhelyezése, menet közbeni ellenőrzése, levétele, sérülés vagy hiány esetében az intézkedések megtétele nem mutat különbséget az előző szabályozással. Megtalálható benne a VÁM-ra vonatkozó rész ugyanúgy, mint a magánzárakra. A magánzárak használatához hoz nem kell külön engedély a felülzárás miatt ugyanis a MÁV szempontjából nem lényeges a meglétük. Fosztogatásnál, illetéktelen hozzáférésnél alapvetően a kocsizár meglétét, hiányát, sérülését vizsgálják. A kártérítési eljárást a biztosítók szintén a kocsizáraktól teszik függővé. Mindazonáltal a magánzárakkal történő minden vasúti eseményt is dokumentálni kell és a feladó felé jelezni.

Kocsizárak levétele: Még a lehetőségét is ki kell zárni, hogy a felhasznált zárak illetéktelen kezekbe kerüljenek, hiszen több zárból kisipari módszerrel össze lehet állítani egy látszatra ép, sértetlen zárat. A számot átütve, a levágott zár helyére a szállítmány kifosztása után fel lehet helyezni. A végállomáson a levételnél veszik észre mi történt. Komoly anyagi és erkölcsi kárt jelent. Milyen intézkedéseket lehet tenni? A zárat be kell vizsgáltatni független laboratóriumban. De a megelőzés nagyon fontos. A felhasznált zárakat fajta szerint gyűjteni az állomásokon egy központi raktárba beszállítani és dokumentálva megsemmisíteni. Másik ok amiért fontos a felhasznált, de nem manipulált zárakat egy ideig őrizni, ha esetleg felbukkan egy ugyanolyan sorszámú zár vagy ha kiderül a szállítmányt mégis fosztogatták a zár bizonyítani, vagy cáfolni tudja ezen esemény megtörténtét. Sajnos találkoztam felelőtlen levétellel egyszerűen kidobták a szemétbe nem jegyzőkönyvezetek.

Kocsizárak selejtezése. A fel nem használt zárakat egyedi azonosítójuk miatt nem szabad simán kiselejtezni vagy kidobni. Jelzés és sorszám szerint kell gyűjteni és dokumentálva megsemmisíteni. Hivatkozva az előzőekre itt is a zárakkal való visszaélés manipuláció fennállhat. Nagyon egyszerű mert itt nem kell kisipari módszerrel felhasznált zárakból újat összerakni, hanem elég az ellenőrző számot átütni, ha még ilyen típus van használatban. A típus megjelölése a leselejtezési jegyzőkönyvben és közreadása meg előzheti ezt a fajta visszaélést.

A fenti szabályozás kisebb módisításokkal mai napig hatályban van. A vasút liberalizáció miatt 2003.-tól a MÁV, és utódcége a MÁV Cargo Zrt, valamint a Rail Cargo Hungária Zrt nem kötelessége a felülzárás, ahol feladói magánzár van. A magánvasutak ugyanezen fenti szabályozásokat használják természetesen figyelembe véve az egyedi cégükre jellemző sajátosságokat.

Felvetődik jogosan, az a kérdés, hogy mi alapján választotta, választja ki a MÁV és egyéb a piacon egyszer használatos zárat használó megrendelő, feladó a számára megfelelő zárat. Azt már tisztáztuk, hogy a zárás módja és a külső megjelenés minden gyártónál, fogalmazónál más és más. A MÁV saját Műszaki Dokumentációval rendelkezik a zárak laboratóriumi bevizsgálására és a műszaki követelményekre, mint a Jelképes zár, mint a Biztonsági zár esetében. Ezt a dokumentumot nem hivatkozom be és nem is csatolom mivel a mai napig a MÁV utódai előbb a MÁV Cargo most meg a Rail Cargo Hungaria Zrt használja, pályázatainál csak pénzért adja ki és úgy gondolom etikátlan és jogsértő is lenne a nyilvánosságra hozatala.

Viszont a MÁV már 2001-óta ragaszkodik a MABISZ általi Biztosítói Minősítési Tanúsítványhoz. Lassan az egész magánpiacnál elfogadott lett ezen Tanúsítvány használata. Legfőbb erre irányuló erőt a biztosítók fejtették ki a cégek felé, másképpen nem voltak hajlandóak biztosítást kötni a szállítmányokra, védendő objektumokra. A MABISZ hasonlóan a MÁV-hoz bizonyos műszaki bevizsgálások alapján Műszaki Szakértői Véleménnyel adja meg a Tanúsítványt. A Tanúsítvány publikus de a Műszaki Szakértői Tanúsítvány nem az. Mindazonáltal a MÁV és a MABISZ általi bevizsgálások jegyzőkönyvét egyedi kérésre a vevőnek, a zár felhasználójának át lehet adni. Tapasztalatom szerint ilyen igény még nem volt csak a Tanúsítványt szokták kérni.

Fontos, hogy a következőben ismertetendő szabvány 90%-ban azonos a MÁV Műszaki Dokumentációjában és a MABISZ Műszaki Szakértői Tanúsítványában szereplő vizsgálatok leírásával. Felvetődik itt egy nagyon fontos kérdés mi alapján lettek a következő vizsgálatok és az azokhoz hozzárendelt méréshatárok, műszaki paraméterek megállapítva. A válasz szokás alapján.

Ahogy már írtam összegyűjtötték a piacon lévő egyszer használatos zárakat, fuvarozási zárakat és a felhasználói igényeket, meg a meglévő műszaki előírásokat és konszenzus alapján állították össze a szabványt. Főképp a legnagyobb cégek igényeit és gyártmányait vették figyelembe.

Szóval kellett egy általános előírás, mely a zárakat valamilyen formában sorolja és elhelyezi a vagyonvédelem palettáján nos ez lett az ISO/PAS 177712:2003 Árufuvarozási konténerek-mechanikus záró elemek szabvány.

Mellékletben megtalálható egy MABISZ Biztosítói Minősítő Tanúsítvány 2001-ből és összehasonlításul egy MABISZ Termék - Megfelelőségi Ajánlás 2007.-ből. Érdekes a névben történt változás, de még érdekesebb, hogy a 2007-es dokumentumban a Vizsgálati eljárás alapja pontba bekerült az ISO/PAS 17712:2003 Szabvány is mint vizsgálati előírás. Az egyszer használatos zárak plombák gyártásával és forgalmazásával foglalkozó cégeknek újra be kellett vizsgáltatniuk a záraikat már e szabvány követelményei szerint.

ISO/PAS 177712:2003 ÁRUFUVAROZÁSI KONTÉNEREK MECHANIKUS ZÁRÓ ELEMEK SZABVÁNY

Nézzük át miről is van szó. Sajnos a fordító nem volt „szakmabeli" a manipulációt mindenhol megbabrálásnak fordította. [2] A Szabványt a Szabó és Fia Szolgáltató Kft vevői igényre szerezte be az Magyar Szabványügyi Testület-től és saját költségén fordíttatta le. 2006.-ban, és haladéktalanul be is vizsgáltat a zárai független laboratóriumban már e szabvány szerint tudtommal elsőként a piacon Magyarországon. A mellékletben szereplő MABISZ Termék - Megfelelőségi Ajánlás dokumentumba azért került, mert a Szabó és Fia Szolgáltató Kft díjmentesen a MABISZ részére bocsátotta a fordítást.

Tehát mint látjuk három kategóriába sorolja be a zárakat

- Biztonsági zár → Megfelel gyengébb Biztonsági zárnak, vagy erősebb Jelképes zárnak
- Megerősített biztonsági zár → Megfelel a Biztonsági zárnak
- Jelzésértékű zár → Megfelel a Jelképes zárnak

2002.-től a Magyar piacon is megjelent az igény egy a két felhasználási körű zár a Biztonsági zár és a Jelképes zár között. Erősebb műszakilag, mint a Jelképes zár, de árban kedvezőbb, mint a Biztonsági zár kifejlesztésére, ami sok cég esetében meg is történt.

A szabvány nagyon jól áttekinti a zárak fajtáit:

- Szálhuzalos zárak
- - Lakatos zárak (újra felhasználható kivitel, konténerekre kifejlesztve) Érdekes, hogy egy klasszikusan nem egyszer használatos zár is belekerült a szabályozásba. de a szabvány az Árufuvarozási konténerekről is szól.
- Lemezcsíkos zárak
- Fémsodrony-zárak
- Csapszeges zárak (ezek a klasszikus tengeri zárak)
- Ráhúzó szalagos (hevederes) zárak
- Sodrott lezárások
- Rovátkolt szalagos zárak
- Címkezárak

A felsorolás célja rámutatni arra, hogy nagyon jól látszik a szabványból, hogy alapvetően tengeri szállítással foglalkozó cégek szabályozásai kerültek bele.

Az alapkövetelmények a jelek, jelzések elhelyezése és a feliratok sorszámok megoldása sokféle lehet erről nem szól a szabvány ezért kiegészítem.

- Benyomással (présgép által)
- Beleégetéssel. Például a műanyag záraknál
- Megfestéssel felületi festés
- Bevonó anyag rávitelével, melyre jelet lehet elhelyezni fémzárnál műanyag bevonat
- Öntéssel már a fém vagy műanyagba beleöntve lehetőleg kidomborodóan.
- Az eljárások célja és lényege az, hogy az egyedi beazonosító jeleket nyom nélkül ne lehessen eltávolítani, sem mechanikai sem vegyi sem kémiai úton Az egyedi beazonosíthatóság vagyonvédelmi elvárás. Az Általános követelmények megegyeznek az előbbiekben kifejtett MÁV és MABISZ előírásoknak.

Itt is nem arról van szó, hogy ne lehessen megbabrálni, manipulálni, hanem ez a lehető legnehezebb legyen. Amit el akarnak lopni azt el is lopják! De az egész vagyonvédelem célja ennek megnehezítése és a többi vagyonvédelmi komplex elemmel együtt –élőerős őrség-a tettenérés. Magyarországon az egyszer használatos zárak (plombák) gyártásához, forgalmazásához nincs és nem is volt szükség VÁM általi jóváhagyásra. Kivéve a jövedéki termékekre kerülős zárak esetében, ebben az esetben nagyon komoly ellenőrzésen és helyszíni bejáráson kell átesnie a gyártónak, forgalmazónak. Shengeni csatlakozás és az EU belső határainak megszüntetése mára a piac teljes liberalizációját hozta. Később a Tapasztalatoknál fogom kifejteni miért fontos mégis a gyártás és forgalmazás ellenőrzése, leszabályozása a gyártó részéről.

A Szabvány négy különböző vizsgálati, minősítési leírást tartalmaz.

- Szakító próba
- Nyírási próba
- Hajlítási próba

- Ütési próba

A hozzájuk rendelt erőket, terheléseket Kg-ban újabb szabályozásoknak megfelelően KN-ban és Nm-ben adja meg. Nem szándékom egyenként a vizsgálati eljárásokat elemezni. Jól érthető és egzakt előírások. Független akkreditációval rendelkező laborban kell a vizsgálatokat elvégeztetni a szabvány előírásait követve. A vizsgálati eljárás végén az eredményeket jegyzőkönyvbe foglalva a zárak típusonkénti megjelölésével és besorolásával a minősítésnek meg lehet felelni. A vizsgálatokat a besoroláshoz csak egyszer kell elvégeztetni a Szabvány nem követeli meg a felülvizsgálati, vagy újbóli vizsgálatokat. Érdemes mégis a gyártónak ellenőrzés képen a zárai időközönként vizsgálat alá vetni még ha ISO minőségbiztosítási rendszerrel is rendelkezik.

Az vizsgálatok elvégetetése, a szabvány bevezetése vagy az ISO rendszer és folyamati működtetése, fenntartása nem kötelező, csak és kizárólag a piac a vevők, felhasználók igényei kikényszerítették a megbízhatóság miatt. Az egyszer használatos zárak olyanok, mint a gyufák a használat közben derül ki, hogy működnek e. Ezért fontos a szabályozás. Természetesen, mint minden termék esetében a nem rendeltetésszerű használat esetén nem lehet garanciát vállalni, hogy a zár megfelelően ellássa feladatát. Még, mikor az első egyszer használatos zárakkal kezdtem foglalkozni, gyártani és forgalmazni észrevettem, hogy főképp azon cégeknél, felhasználóknál, ahol megelőzően nem használtak zárat plombát nem igazán tudták, hogyan is kell a zárakat kezelni. A megszűnt vállalati állami rendészeteket a magánbiztonság még nem tudta teljesen pótolni. Részben a szabályozás részben a magáncégek anyagi megfontolása miatt. Összeállítottam a MÁV-os előírásokból egy általános Ajánlást, és részt vettem több cégnél a plombák használatának bevezetésénél. Ott tapasztaltam, hogy hiába volt, van meg a tudásom többször a fejemhez vágták, hogy csak gyártó vagyok ne szóljak bele a cégük dolgaiba. Ez vezetett oda, hogy először a Biztonságszervezői I felsőfokú tanfolyamot elvégeztem majd jelentkeztem és felvételt nyertem a Rendőrtiszti Főiskolára a Nemzeti Közszolgálati Egyetem jogelődjére.

GYÁRTÓI, FORGALMAZÓI AJÁNLÁS [3]

Megrendelés:

Az írásban, faxon, vagy elektronikus levélben (e-mail) elküldött megrendelésben hivatkozni kell az igényelt magánzár (én a magánzár nevet használom) típusára (fém vagy műanyag)

A megrendelésben szerepeljen a magánzár színe és a felirat szövege, vagy a logo mintája, ha egyik sincs az egyedi azonosító megjelölése.

A megrendelésben szerepeljen még a folytatólagos sorszám, az utolsó megrendelésénél befejezett sorszám lesz a kezdő. Új megrendelésénél a sorszám 000001-től indul folyamatosan, emelkedően.

A megrendelő bekerül egy számítógépes és manuális nyilvántartásba így a jövőben a megrendelések megkönnyítése miatt elég, ha a kapcsolattartó ügyintéző telefonon adja le azt.

Magánzárak tárolása és nyilvántartása:

A megrendelés után beszállított magánzárakat érkeztetés után „Magánzár nyilvántartásba” kell venni. A nyilvántartást a következő rendészeti szempontrendszer szerint kell elkészíteni:

- Megrendelés időpontja és száma, kapcsolattartó neve beosztása.
- A magánzárak beérkezésének időpontja, az átvétel átszámolás eredménye. Ha van hiány
    - annak a jegyzőkönyvezése és jelentése.
- A Magánzár sorszáma és darabszáma
    - A felhasználásra kiadott magánzárak darab és sorszáma az átvétel ideje, az átvevő neve
    - Időszak végéig (heti, havi) beérkezett és felhasználásra kiadott magánzárak összesítése.
    - A rendelkezésre álló darabszám, mennyiség megállapítása.
- A magánzárakat egy erre rendszeresített ha ilyen nincs megfelelően zárható helyen kell tárolni, hogy ahhoz illetéktelen személyek ne férjenek hozzá.
- Rendészetileg fontos, a magánzárak tárolásával egyetlen személyt felelőssé tenni
- A felhasználásra kiadott magánzárakról felhasználó helyenként - amennyiben több felhasználó hely van – úgy nevezett „Helyi felhasználói nyilvántartást kell vezetni”.
- A felhasználói helyekre általában csak az egy napi vagy az adott zárásmennyiség szükségletének megfelelő magánzár mennyiséget célszerű kiadni, a visszaélések megelőzése érdekében.
- A „ Helyi felhasználói nyilvántartásban” szerepelnie szükséges:
    - A zár felhasználás, felhelyezés időpontjának.
    - A már felhasználásra került magánzárak darabszámának
    - A már felhasználásra került magánzárak sorszámának
    - A lezárt objektum, vagon, gépjármű, konténer egyedi azonosítójának (rendszám, kocsiszám, konténer száma)
- A felhelyezésnél roncsolódott magánzár sorszámát és a felhelyezés dátumát.
- Felelős személy rendész, vagyonőr, biztonsági őr nevét.

Magánzárak használata:

Magánzárral el kell látni a lezárandó objektum, közúti gépjármű vasúti kocsi vagy konténer olyan zárható nyílását, ahol az áruhoz hozzá lehet férni.

A magánzár szárát a zár házába olyan módon kell felfűzni, hogy annak megsérülése nélkül a lezárt nyílást még résnyire sem legyen megnyitható. Szorosra kell húzni. Ellenőrizni, hogy ténylegesen zár a magánzár, ellentétesen óvatosan meghúzni.

A lezárandó objektumba, közúti kocsiba vasúti kocsiba vagy konténerbe történő berakodás után a magánzárakat azonnal fel kell helyezni.

A felhasznált magánzárak darabszámát és sorszámát a kísérő dokumentumokon, okmányokon fel kell tüntetni.

A telephelyről való kilépés alkalmával a kapuszolgálatnak a felhelyezett magánzárak sorszámazonosságát ellenőrizni és szignálni kell.

Amennyiben a telephelyről való kilépés alkalmából a rendészeti előírások miatt a közúti gépjármű, illetve a vasúti kocsi rakományát ellenőrizni, felnyitni szükséges, az eredeti magánzár roncsolásmentes eltávolítás (egyszerű tiszta levágás) után az újonnan felhelyezett magánzár számát a kísérő dokumentumokra fel kell jegyezni. Ezzel egyidejűleg arra vonatkozóan is fel jegyzést kell tenni, hogy melyik eredetileg felhelyezett magánzár- sorszám megjelölésével- lett eltávolítva

A magánzárak azonosságát és épségét a portán való belépés és kilépés alkalmával minden esetben ellenőriztetni szükséges. Amennyiben a portaszolgálat, vagy más ezzel megbízott személy megállapítja a magánzár sérülését a sérülés tényét a gépjármű vezetőjével el kell ismertetni.

A magánzár hiánya, vagy sérülése esetén a fentieken túl, ha erre lehetőség van tételes árú ellenőrzést is célszerű végezni. Amennyiben a kísérő dokumentum adataihoz képest a közúti vagy vasúti jármű rakománya eltérő, az eltérés tényét, okát, ha megállapítható és időpontját jegyzőkönyvben rögzíteni kell. A jegyzőkönyvet lehetőleg az áru kísérőjével is alá kell íratni, amennyiben ezt megtagadja az előírt intézkedéseket haladéktalanul meg kell tenni.

Mint a fejezet elején említettem a gyártók maguk döntik el milyen kivitelű zárási megoldású és formájú zárta gyártanak, forgalmaznak. Mint láttuk a szabályozás és a szabvány nem más, mint ajánlások sorozata. A Gyártói Ajánlásban megpróbáltam egy általános elvárát megfogalmazni és így minden cég, felhasználó a saját rendszeréhez, vagy a biztonsági szolgálatához tudja illeszteni. Természetesen nem várható el mindenhol minden elem működtetése. A számomra legideálisabb állapot, ha a felhasználó bevezeti és működteti az ISO szabvány szerinti minőségbiztosítási rendszerét, és rendszerelemmé teszi a zárak használatának szabályozását.

A MÁV előírások de a Gyártói Szabályozás is a Vagyonvédelem Komplex Rendszerének a tagja pontosabban a Rezsim Intézkedések közé tartozik. Fontosnak tartom mégis külön kiemelni. Ezzel elérkeztünk a következő fejezethez, melyben a zárakat elhelyezzük a Vagyonvédelemben.

HELYZETÜK A VAGYONVÉDELEMBEN

Először a vagyonvédelem fogalmát tisztázzuk. Vagyonvédelem: az ingatlan és ingóság őrzése, a pénzérték-szállítás és szállítmánykísérés, a rendezvények biztosítása, valamint a felsorolt tevékenységek tervezése, szervezés és irányítása. A ~ ellátása gyakran kapcsolódik → *személyi védelem*hez, amely az adott természetes személy életének és testi épségének védelmére irányul. Ebben az utóbbi esetben már személyi és vagyonvédelmi tevékenységről van szó. [4]

Nem szeretem, azt a hasonlatot miszerint minden lánc annyira erős, mint a leggyengébb láncszeme.

Szeretem úgy felfogni a szervezetek, szolgálatok működését, mint egy gépét. Összetett organikus és mechanikus elemekből, alkatrészekből álló komplex rendszer. Minden elemet méretezni kell és a saját helyén kezelni. Lehet sőt biztos, hogy egymáshoz képest eltérnek erő, szakítószilárdság és más mutatóikban, de együtt megteremtik a tökéletes működést, a tökéletes rendszer. Például egy gépjármű gyújtógyertya ugyanolyan paraméterekkel kell rendelkezzen, mint az ablaktörlő, vagy az indítómotor? Természetesen nem, az együttműködés a kooperáció az elemek együtt dolgozása, és a szinergiája a lényeg. Az ember nem gép, elfárad, sérül, rossz napja van vagy elromlik. Sőt még a gép is elromlik. Ebben a szellemiségben tekintek a Vagyonvédelem rendszerére, mint az emberek az eszközök és intézkedések komplex rendszerére. Hasonlóan, mint a szervezetek közötti együttműködés, kooperáció a vagyon ellenes bűncselekmények, és a bűnmegelőzés mint a magánbiztonság,

mint a rendvédelmi szervek között. De említhetném a Polgárőrségeket és a helyi önkormányzatok bűnmegelőzési bizottságai és a végén, de nem utolsósorban a polgárok jogkövető magatartását. A törvényeket.

Tekintsük át, ezzel a logikai módszerrel az egyszer használatos zárak (plombák) helyzetét.

A Vagyonvédelem Komplex Rendszere:

- Mechanikus védelem
- Elektronikus védelem
- Élőerős védelem
- Rezsim intézkedések

MECHANIKUS VÉDELEM

Ide tartoznak maguk az egyszer használatos zárak. Két oldalról lehet megközelíteni.

Először azon cégek felhasználók, ahol nem használnak egyszer használatos zárakat és nem is zárnak. Rendészeti szempontból nagyon rossz nem lehet sem védeni sem bizonyítani száz százalékosan, ha valami történik. Hiába van élőerős őrség, biztonsági szolgálat hisz az alkalom szüli a tolvajt, mint tudjuk. Az elektronikus védelem sem mindig célszerű. Az egyszer használatos zár az utolsó védelmi vonal. Ha az elkövető átjutott a héjvédelmen ez a magvédelem vége. Itt már csak az áruk vannak, a védendő javak. Ezért minden előzetes védelmi intézkedést meg kell tenni.

Másodsorban, ahol használnak egyszer használatos zárat de semmilyen dokumentációt nem vezetnek róla. A Rezsim intézkedések teljes hiánya olyan mintha lenne egy drága lakásunk minden földi jóval berendezve hozzá egy hiper modern biztonsági ajtónk csak éppen a kulcsot egyfolytában elhagynánk másoltatnánk belőle rengeteget és agyba főbe osztogatnánk mindenkinek, aki éppen arra jár.

Természetesen én csak az egyszer használatos zárakról beszélek, de nagyon sok vagyonvédelmi, rendészeti rendkívüli eseményre, és azok megelőzésére alkalmas a hasonlat.

ELEKTRONIKUS VÉDELEM

Ide soroljuk a megfigyelő kamerákat a kültéri és beltéri behatolás jelzőket, a tűz és füstjelzőket. A zárak egyik fejlesztési iránya a GPS vagy GPRS globális helymeghatározó rendszerrel ellátott szállítmányok védelme, mégpedig oly módon, hogy maga az egyszer használatos zár zárja az áramkört. Amennyiben illetéktelen módon megnyitják bekapcsol a biztonsági jelző és a központban megtörténik a riasztás. Természetesen a megfigyelő kamerák is nagyon fontosak például cargo terminál, logisztikai központ vagy rendező pályaudvaron a megfigyelés és a rendkívüli esemény felderítésében, bizonyításában. Megtörtént eset, hogy egy fosztogató banda feltörte a konténert, és kezdte kipakolni, a megfigyelőközpont észlelte és jelezte a biztonsági őrök felé. A helyszínre kiérkező biztonsági őrség elől a fosztogató banda szétfutott. Az egyik tagját a kiérkező rendőrség tartóztatta fel egy mellékutcában és a bizonyíték arra, hogy ott volt a biztonsági zár volt, amit a levágás után zsebre tett. A biztonsági zár sorszáma megegyezett a konténerre felhelyezettével és a megfigyelő kamera által rögzített felvételen is felismerhető volt az elkövető.

ÉLŐERŐS VÉDELEM

A munkatársak kiválasztása az alapja a sikeres működésnek. Amennyiben a Biztonsági szolgálat helyezi fel az egyszer használatos zárat ki kell oktatni annak megfelelő és szakszerű használatáról és a vonatkozó dokumentumok kitöltéséről, vezetéséről. Fontos a Biztonsági szolgálat részéről az időszakai vagy járőrhöz kötött ellenőrzése a zárak sértetlenségének. Ez történhet szemrevételezéssel, vagy egyszerű kézzel történő megmozgatással. Legtöbb esetben a Biztonsági szolgálat vagy a Fegyveres Biztonsági őrség már lezárt állapotban találkozik a zárakkal. Sajnos volt rá példa, hogy a pénzszállító Fegyveres Biztonsági őre manipulálta a pénzeszsák lezáró zárját. Megtörtént eset, hosszabb vidéki úti pénzszállításnál a szállítójárműben hátul tartózkodó Biztonsági őrnek volt ideje „játszani" és manipulálni az egyszer használatos zárat. Pénz vett ki belőle, majd visszazárta. A zár már nem zárt rendesen, de úgy tűnt „mintha" zárt állapotban lenne. A bank munkatársai vették észre a hiányt. Az egyszer használatos zár bevizsgálásra került, ahol a független vizsgáló laboratórium megállapította, hogy a zárnál idegenkezűség áll fenn. Hamar kiderült, hogy kinek volt alkalma és ideje a manipulációra. A Biztonsági őrrel szemben a szükséges eljárásokat megindították. Itt is látszik az egyszer használatos zár azon kritériuma, hogy nyom nélkül kinyitni és visszazárni ne lehessen. Ha az élőerős őrség észleli a sérülést a záron, haladéktalanul meg kell tennie a számára előírt védelmi tervekben szereplő intézkedéseket.

REZSIM INTÉZKEDÉSEK

Mint a fentiekben többször hivatkoztam a Vagyonvédelem Komplex Rendszerének elemeinél illetve az előző fejezet szabályozásánál a dokumentálás és előírások fontosságára. Az egyszer használatos zárak az egyik oldala a biztonságos használatnak, a másik nagyon fontos oldal a dokumentáció. Ki, mikor, milyen sorszámú zárat helyezett fel. Hogyan történt a dokumentálása, szállító levél, fuvarlevél, Szignálta-e, menet közben keletkezett e bármilyen sérülés a záron. Ki ellenőrizte, mikor, hol és az ellenőrzést hogyan dokumentálta. Levétel során tapasztaltak-e a záron sérülést. Volt e manipulációra illetve fosztogatásra utaló elváltozás, nyom.

Nagyon fontos a Védelmi Tervek elkészítése, napra készen tartása és lehetőség szerint begyakorlása. Munkatársak kiválasztása, oktatás és a képzés folyamatos végzése, szinten tartása. Tűzvédelmi és Menekülési Tervek elkészítése. Kapcsolat a Rendőrséggel, a Mentőkkel és a Tűzoltókkal. A Rendőrséggel a Védelmi Tervek pontosítása, riasztás rendjének kialakítása.

RENDKÍVÜLI ESEMÉNY

A rendkívüli esemény fogalma [5] :A rendkívüli esemény a szokásos folyamatoktól, eseményektől eltérő, olyan nem várt állapot, helyzet, amely esetenként dominóhatást kiváltva, – a rendeltetésszerű, szokásos működést akadályozza, – veszélyezteti vagy károsítja – az élet- és vagyonbiztonságot, – az alapvető életfeltételeket, a lakossági ellátást, – a természetes és mesterséges környezetet, a természeti értékeket, ezért megelőzése, enyhítése vagy felszámolása, az eredeti állapot helyreállítása tervszerű intézkedéseket, beavatkozást tesz szükségessé. Dominóhatás alatt azt értjük, hogy ha a bekövetkezett esemény eszkalálódik, azaz további, más területre, tevékenységre is kiterjed, ott újabb, kapcsolódó rendkí-

vüli eseményt, súlyosabb következményeket vált vagy válthat ki, illetve azok bekövetkezésének lehetőségét megnöveli. Vagyis minden, ami az általános napi rutintól eltérő esemény. Nagyon széles a spektrum mégis fel kell rá készülni. Terveket készíteni összehangolni a Vagyonvédelem Komplex rendszerének elemeit minél jobban összeszervezni, az ellenőrzési pontokat kijelölni a visszacsatolás a felelős személyek az intézkedéseket kielemezik pontosítanak és módosítanak, ha kell. Példának szeretnék hozni egy megtörtént esetet, melynek kivizsgálásában a gyártó cég részéről jelen voltam.

Egy nagy múlti cég főképp vasúti és tengeri szállítással, fuvarozással foglalkozik. A nevet nem óhajtom megosztani a lényeg ma is a piacon van a cég. Konténerben történik a szállítás Budapesten a vasútállomáson a cég saját munkatársai felhelyezték a saját feliratú és sorszámú fém Biztonsági Magánzárat. (ISO/PAS 17712:2003 besorolása szerint Megerősített Biztonsági Zár).

Majd vasúton elszállításra került a többi konténerrel együtt a Hamburgi tengeri kikötőben, ahol szintén a fenti cég munkatársai leellenőrizték majd hajóra berakodták. Itt még nem történt semmi A rakományt Doverben egy másik nagy tengerjáró hajóra rakták át, hogy megindítsák az USA irányába, Ekkor fedezték fel a fenti cég ottani munkatársai, hogy a fém Biztonsági zár sérült. A rakomány átvizsgálása után, kiderült, hogy a rakomány hiánytalan. De látszottak a próbálkozás nyomai. A hajón dolgozók azzal védekeztek, hogy a konténeren a zár már sérülten került fel a hajóra. Ezt a cég munkatársai és biztonsági szolgálata cáfolta. Mivel nemcsak a vonatkozó fuvarleveleket vezették, de fényképet is készítettek minden egyes konténerről lezárás után. A fényképeken beazonosítható volt a konténer száma és a sértetlen zár. Az amerikai anyavállalat felé kértek tőlem egy vizsgálatot, hogy a zár a rakodás és szállítás közben megsérülhetett-e ily módon. Kértem adják ide a zárat, hogy független laboratóriumban bevizsgáltathassam azt. Ezt megtagadták, de átküldték s fényképeket a zárról. Ebben az esetben nagyon óvatosan jártam el csak a képen látottakra szorítkozva következtetéseimben adtam egy Gyártói Nyilatkozatot. (Mivel nem volt másra jogosultságom). Egyértelműen látszott a képen, hogy kalapáccsal próbálták leverni a zárat, majd a drótkötelet próbálták ugyancsak kalapáccsal elvágni. Nagyon erősen roncsolódott a drótkötél teljesen ellapult de a zár nem nyílt ki. (Kalapáccsal a csapszeges zárat ki lehet nyitni egy ütéssel és úgy visszazárni, hogy egyszerű szemrevételezéssel ne lehessen észrevenni a roncsolódását). Tehát a fém Biztonsági Zár jól vizsgázott. A cég munkatársai, biztonsági emberei felkészültek voltak, szakszerűen jártak el. A legfontosabb a történtekben, hogy akkor nem történt fosztogatás nem volt kár. Nagyon ritka az ilyen eset. Szerencsére a zárt szállítási láncnak nagyon hamar meglettek az elkövetők és kiderült, hogy más konténereket már jó ideje fosztogatnak. A hatóságok felderítették és lezárták az ügyet. Tehát meghiúsult a bűnismétlés. Általában eldobálják a levágott zárakat, hogy nehezebb legyen a beazonosítás.

Még egy érdekessége van az esetnek, fuvarozásánál, szállításnál amíg mozgásban van a vonat vagy a hajó nagyon nehéz fosztogatni, vagy kirabolni. A teherautó más eset, vannak bandák, akik kifejezetten menetközben rabolják ki a kocsikat, vagy kényszerrel megállítják azt. Főképp olyan országokban, ahol a közúti fuvarozás a jellemző. például USA, Németország, Ausztrália.

Tökéletesen kitűnik, hogy csakis a Vagyonvédelem Komplex Eleminek együttműködése, az információk és adatok cseréje, a Védelmi Tervek kidolgozása jelentheti a vagyonvédelem százszázalékos hatékonyságra – ami elképzelt, ideális nem elérhető számváló törekvését.

TAPASZTALATOK

Ebben a fejezetben megpróbálom az évek során szerzett tapasztalataimat oly módon megosztani, hogy azon oldalt is be tudjam mutatni, amelyikkel napi kapcsolatban vagyokfelhasználói oldal- hisz az ő igényeik mutatnak utat az egyszer használatos zárak fejlesztéséhez, A gyártói oldalt és a gyártás szervezését a problémás pontokat a folyamatok ellenőrzését, mire egy vevői igényből, ötletből konkrét gyártmány lesz. És végül de nem utolsó sorban a fosztogatók és azon elkövetők szemszögéből – az ő „ötleteik" is beemelésre kerülnek a zárak fejlesztésénél- akik sikeresen manipulálták a zárakat, még ha nem is találkoztam velük személyesen a „munkájukkal" találkoztam és az azokból levont következtetésekből sokat tanultam és profitáltam.

Konkrét példa: Általában, az emberek azt hiszik, hogy termékeket csak és tisztán tervező asztalnál álmodják meg. A fejlesztés lehet egy jó ötlet terméke, de lehet tisztán a piac elvárása. Ilyen volt mikor 1995-ben a már folyó EU csatlakozások miatt és a joghармonizáció miatt az EU vasúti szállítási piacán kizárólag műanyag zárat lehetett használni. Minden más zárat a határon azonnal levágtak és saját zárat helyeztek fel helyettük. Ez anyagilag is rosszul érintette a Magyar vasúti szállítókat. Kényszerhelyzet volt. Tehát a felhasználó kijelentette vagy műanyag anyagú egyszer használatos zár vagy semmi. Így indult a kifejlesztése az első műanyag zárnak, amelyben részt vetem. Piacra kerülése után jöttek az újabb észrevételek. túl széles nem lehet mindenhol átfűzni. Nincs rajta felfűző furat, nehezebb a kezelhetősége. Hidegben ridegedig, és könnyen törik. Az Osztrák vasútnál az úgy nevezett „termoszos „kinyitást manipulációt használták a fosztogatók. Ami azt jelenti, hogy az ember egy nagy termosz forró teával odasétál a vagonokhoz a termosz tetejét lecsavarja és a műanyag zár alá helyezi úgy, hogy minél jobban érje a forró gőz. Körülbelül tíz másodperc után vagy ha már gyakorlott az illető ez pillanatok alatt lezajlik a zárat egy erős húzással ki lehet nyitni. Mi történik? A műanyag zár rácsszerkezete átalakul fellazul és rugalmassá válik így lehetséges a kinyitás a szalagtest visszahúzása a fejből. A rakomány kipakolása vagy megdézsmálása után a zárat újra le lehet zárni. A lezárt műanyag zár az ép zár látszatát kelti. Tehát nem működik megfelelően nem valósul meg a sérülésmentes nyitás és visszazárás. Hiába voltak fémbetétesek a zárak vagy úgynevezett bebetétezettek a forró gőz hatására mind ki lehetett nyitni. Nehéz feladat, de a megoldást a gyártás adta meg. Vannak vevői igények, amelyeknek nem lehet megfelelni mert egyszerűen műszakilag megoldhatatlan az elvárás. Ilyenkor a tervező és a szerszámos együtt kap szívrohamot. Ez a fenti elvárás majdnem, de csak majdnem ilyen volt. A megoldás különleges műanyag alapanyag mely bírja a -30 C foktól a +100 C fokos hőmérséklet ingadozást. Adalékolás – mesterkeverék bekeverése-az alapanyagba és a műanyag fröccsöntő szerszám különleges kivitele továbbá a műanyag fröccsöntő gép nagyon pontos beállítása a paraméterek folyamatos figyelése és a kieső darabok azonnali minőségi ellenőrzése. Valahogy úgy vagyunk ezzel a hőmérséklet problémával az egyszer használatos záraknál plombáknál, mint a közúti burkolóanyagok esetében. Magyarországon a hőingadozás a téli és a nyári legkisebb és legnagyobb hőmérséklet között nagyon nagy. Kevés anyag bírja ki ezt az eltérést. A Fém Biztonsági zár esetében inkább az egyéni igények, kézsérülés történt a drótkötél vagy a házon maradt öntvény sorja miatt. Koszolt a fém a kézen. Cérnakesztyű bevezetése. Kezelhetőségi igények. A biztonság oldaláról csak két komoly igény érkezett, mégpedig a MÁV Biztonsági osztályától. Meg kellett nehezíteni, hogy tűvel benyúljanak a fémzár házába és, hogy

elvágás után a sordonykötél ugorjon szét elemi szálaira, nehogy ragasztószalaggal való összetekerés után újra lezárhatóvá váljon. Nagyon sok hibás használat miatt voltam kint oktatást tartani, segítettem a belső ellenőrzési rendszer kiépítésében. Jó kapcsolatba kerültem sok vagyonvédelmi vezetővel, munkatárssal. Ez is ösztönzött, hogy jobban elmélyüljek a vagyonvédelmi, biztonsági szakmában. De sokat tanultam a fosztogatók hátra hagyott „munkáiból" is. Kielemezve a manipuláció módszerét azt beépítve a zár működésébe, vagy külső megjelenésébe folyamatos fejlesztéssel lehet csak lépést tartani az egyre rafináltabb és korszerűbb módszerekkel „dolgozó" fosztogatók ellen. Biztonsági szempontból a gyártás leszabályozása a folyamatok ellenőrzése nagyon fontos, amelyet a gyártók vagy a képviseletek sokszor nem tartanak szem előtt. A biztonsági kör eleme a gyártás és dokumentálása, az értékesítés és dokumentálása, a felhasználás és dokumentálása. Igyekeztem a gyártás különböző folyamatait egymástól határozottan elkülöníteni fizikailag és földrajzilag is. Az egyes gyártási és beszerzései folyamatok külön kezelése, az összes lépés és összefüggés egy kézben legyen, mindenki csak a maga feladatát értse és végezze magas szinten. Nem szabad megengedni, hogy akár egy darab zár is úgy kikerüljön, hogy nincs dokumentálva. Azt is ki kell zárni, hogy két különböző megrendelőhöz, felhasználóhoz azonos kivitelű, színű, feliratú és sorszámú zár kikerüljön. Ugyanígy a sorszámismétlést is meg kell akadályozni. Sajnos próbálkoztak fosztogatók, oly módon, hogy az adott cég nevében utánrendelni akartak. Ezért is fontos a regisztráció. Ezt a felhasználó felé azonnal jelezni kell, hogy a hatóságok felé s szükséges bejelentéseket meg lehessen tenni. A cégnél, ahol dolgozom 1995.-től indítva minden egyes zárral el tudunk számolni, még a mintának kiadottakkal is. Egyedi azonosító nélküli zárat nem szabad még mintának sem kiadni. A fent említett kör, gyártás, értékesítés, felhasználás és az egyszer használatos zár műszaki paraméterei együtt adják a biztonság magas szintjét.

ÖSSZEGZÉS

Szaktanulmányomban az egyszer használatok zárak (plombák) fejlődését, történetét történelmi és társadalmi jelentőségét, továbbá műszaki fejlődését és szabályozását jártam körbe. Be kell látnom egy-egy téma önmagában is megfelel egy szakdolgozat anyagául. Nem célom leállva egy fejezetnél azt boncolgatva a másik fejezet téma hátrányára írni. Szakdolgozatommal alapvetően a célom az összefüggések és szinergiák kiemelése, rájuk való mutatás és mindenhol a középpontban az emberrel. Nekem vesszőparipám, hogy minden a munkatársak kiválasztásával kezdődik. Lehet az a műszakilag legmagasabban fejlettebb kivitelű zár, ha a gyártása és annak megszervezése rossz. Silány kivitelű zárral pedig a legjobban működő biztonsági szolgálat, vagyonvédelmi cég sem ér semmit munkája megnehezedik. Ugyanúgy, ha az egyszer használatos zárral műszakilag felhasználhatóság szempontjából minden megfelelő rossz, hanyag kezeléssel, hiányos dokumentációval és a legfontosabb szakképzetlen biztonsági őrökkel biztos, hogy nagyon komoly problémák fognak felmerülni. A dokumentáció a vonatkozó iratok vezetése, jegyzőkönyvezés, utasítások betartása, védelmi tervek elkészítése és ezek begyakorlása az alfája és ómegája minden vagyonvédelemmel vagy kiemelt tevékenységgel foglalkozó vállalkozásnak és szakembernek. Az oktatás és a képzés. Fejleszteni és fejlődni szükséges napra késznek kell lenni. Ahogy a Szakdolgozatomból is látszik ahány gyártó, annyi zárási megoldási és kiviteli mód, formagazdagság. Nem látszik, hogy a szabványosítás a külső formára különösebben hatással lenne. Csak a sorozatgyártás gépesítése. ami teret ad a gyártó cégek zárainak valamilyen

egységesítésére vagy a cégarculat. Ha végigtekintünk a pecsétek fejlődésén már ott is megjelent egy adott uralkodó család vagy dinasztia egységesítési szándéka a jelképrendszerében, így azokon is, amelyek a pecséteken is megjelentek. A hatalom és a magántulajdon kiterjesztésének és érvényesítésének egyik eszköze volt és a hagyományos pecsétek a mai napig ezt a vonulatot képviselik. Az országok és városok is átvették ezt a szokást, a jelképek használatát. A polgárság kialakulásával a kereskedelem fellendülésével a szerződéseket hitelesíteni kellet, és olvasni még mindig kevesen tudtak. Kereskedődinasztiák használták lobogóikon és pecsétjeiken a jelképeiket. Nem tértem ki külön a Szakdolgozatomban a pecsétgyűrűkre, amit most is szokás viselni, monogrammal ellátva vagy valamilyen jellel. A történelem folyamán az uralkodók is használták hitelesítésre a hatalom megnyilatkozásaként. Ma már inkább dísz vagy a vagyon jelképe., esetleg egy iskolához, klubhoz való tartozás szimbóluma. De például az USA rögbi vagy kosárlabda bajnokainak is jár a bajnoki gyűrű. Ezt a kitérőt csak érdekességként tettem. Az újkori, modernkori ember mindent próbál egyszerűsíteni. Sajnos a történelemben a lopás a tulajdon jogtalan megszerzésére való hajlam végigkíséri az emberiség történelmét. Védeni óvni továbbra is kell a vagyontárgyakat és a tulajdont. Sajnos nálunk huszonkét év után sem alakult ki teljesen a magántulajdon tisztelete. Sokszor azt sem tiszteljük, amink van. Nehéz és hosszú lesz még a folyamat, mire eljutunk odáig, hogy ténylegesen nyitva merjük hagyni azt a képletes ajtót. Addig viszont az egyszer használatos zárakra (plombákra) és a vagyonvédelemre is szükség lesz. A Vagyonvédelem Komplex Rendszere és hozzá a megfelelő tudással rendelkező szakemberek képzése, a meglévők oktatása jelenti egyedül a maximális biztonságra való törekvést. Immár túl kell lépni a szükséges minimum színtű biztonsági rendszereken és a feketén foglalkoztatott alulképzett motiválatlan biztonsági őrökön. A cégeknek el kell fogadni, ha ők nem tesznek meg mindent, és ezzel együtt a vagyonvédelmi vállalkozások is akár az ablakon is kiszórhatják a pénzüket. Ide is érvényes az a mondás, hogy az olcsó a drága. A tevékenység jellege határozza meg a védelmi feladatokat. Előre gondolkodni és gondolkodni terveket készíteni, gyakorolni és akkor megnyílik a lehetőség egy optimális a költségeket és a szakmai elvárásokat egyaránt figyelembe vevő rendszer működtetésére és tartós és biztonságos fenntartására. A munkatársak biztonsági tudatosságának növelése nagyon fontos. Ne csak azért tegyen valamit a munkatárs mert elvárják tőle vagy előírják azt neki. Érdektelen, hogy az egyszer használatos zárakról vagy fegyveres biztonsági őrségről van szó, a vagyonvédelmi szempontok megértése, átvétele és azok folyamatos fenntartása napról-napra, a záloga a sikernek.

FELHASZNÁLT FORRÁSOK

[1] Magyar Államvasutak Árufuvarozási Utasítás C.1. Számú Utasítás (Áruk, Élőállatok és Hullák Fuvarozására) https://www.mavcsoport.hu/sites/default/files/mav_utasitasok_gyujtemenye_2015_01_19.p
(letöltve:2022.05.25.)
[2] ISO/PAS 177712:2003 Árufuvarozási Konténerek - Mechanikus Záró Elemek Szabvány
[3] Gyártói, Forgalmazói Ajánlás A Szabó és Fia Szolgáltató Kft archív anyagai között.
[4] Rendészettudományi Szaklexikon Budapest, Magyarország: Ludovika Egyetemi Kiadó, 690 p. 2019

[5] L. Christián, *Személy- és vagyonvédelem*. Budapest: Nemzeti Közszolgálati Egyetem (NKE), 141.p. 2014. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/100420/611.pdf?sequence=1 (letöltve:2022.06.01.)

QUANTUM CRYPTOGRAPHY: QUANTUM KEY DISTRIBUTION, A NON-TECHNICAL APPROACH

KVANTUMKRIPTOGRÁFIA: KVANTUMKULCS-ELOSZTÁS, EGY NEM-TECHNIKAI MEGKÖZELÍTÉS[1]

FRIGYIK András[2]

Abstract

With the rapid development of quantum computers the currently secure cryptographic protocols may not stay that way. Quantum mechanics provides means to create an inherently secure communication channel that is protected by the laws of physics and not by the computational hardness of certain mathematical problems. This paper is a non-technical overview of quantum key distribution, one of the most well-known application of quantum cryptography, a type of cryptography poised to exploit the laws of quantum mechanics.

Keywords

secure communication, quantum cryptography, quantum key distribution, BB84, entanglement

Absztrakt

A kvantumszámítógépek gyors fejlődésének köszönhetően a jelenleg biztonságos kriptográfiai rendszerek nem feltétlenül maradnak azok. A kvantummechanika lehetőséget ad arra, hogy egy olyan kommunikációs csatornát hozzunk létre, amely biztonságát a fizika törvényei garantálják, és nem azon alapul, hogy bizonyos matematikai számításokat klasszikusan nagyon nehéz kiszámolni. A cikk egy nem-technikai áttekintése a kvantumkulcs-elosztásnak, amely talán a legismertebb alkalmazása a kvantumkriptográfiának, egy olyan fajta kriptográfiának, amelyik közvetlenül a kvantummechanika törvényeire építkezik.

Kulcsszavak

biztonságos kommunikáció, kvantumkriptográfia, kvantumkulcs-elosztás, BB84, összefonódottság

[1] A tanulmány angol nyelvű változata a Proceedings of the Engineering Symposium at Bánki, ESB21, 2021 jelent meg.

[2] frigyik.andras@uni-obuda.hu | ORCID: 0000-0002-4220-4680 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem

BEVEZETÉS

Közeleg a Q-Nap! A közelmúltban megjelent egy *Feature* cikk [1] a *Nature* című lapban, amelyben a szerző igyekszik felmérni milyen veszélyt jelentenek a kvantumszámítógépek a jelenleg használatban lévő kriptográfiai rendszerekre. A fent említett Q-Nap arra a napra utal, amikor a kvantumszámítógépek (*Quantum computers*) képessé válnak a jelenleg alkalmazott biztonsági védelmek feltörésére.

A kommunikációs rendszereink biztonsága ma azon az elven alapul, hogy bizonyos matematikai problémák nehezek: Még ha hozzá is férnénk egy szuperszámítógéphez akkor sem tudnánk kiszámolni az eredményt ésszerű időn belül. Számok prímekre bontása vagy a diszkrét logaritmus problémája (számelméleti változata a jól ismert logaritmus keresési kérdésnek) nehéz mert nem ismerünk olyan algoritmust amelyik minden esetben hatékonyan meg tudná oldani a problémát. Viszont, ha valaki azt állítja, hogy tudja a megoldását egy ilyen jellegű matematikai problémának, akkor azt könnyű leellenőrizni.

Ha azoknak van igazuk akik a kvantumszámítógépek eljövetelét hirdetik akkor a helyzet egyik napról a másikra megváltozhat. Ezek a számítógépek elviekben képesek lesznek arra, hogy a jelenleg gyakorlatilag megoldhatatlan problémákat nagyon hatékonyan megoldják. Annak érdekében, hogy a titkos adatainkat megvédjük több dolgot is tehetünk. Az egyik ilyen lehetőség a postkvantum vagy kvantum utáni kriptográfia. Egy másik lehetőség az, hogy a titkosításhoz használt kulcsot extrém biztonsággal juttassuk el a felhasználóhoz: A kvantummechanika segítséget nyújt ahhoz, hogy lehallgatásbiztos kommunikációs csatornát hozzunk létre. Ha a lehallgató személynek nincs mit feltörnie akkor teljesen mindegy milyen számítógéphez van hozzáférése. Ez a cikk igyekszik egy nem-technikai bevezetőt adni egy most is fejlesztés alatt álló módszerhez, amit kvantumkulcs-elosztásnak hívnak. Világossá szeretném tenni milyen szerepet játszik a kvantummechanika ebben a folyamatban.

A cikk további része a következő módon alakul: A 2. fejezet az első olyan rendszerről szól amelyik közvetlenül használta a kvantummechanikát titkosításra. A rendszer kizárólag a Heisenberg-féle határozatlansági elven alapul. A 3. fejezetben egy olyan rendszert írunk le amelyik a kvantummechanika egy másik sajátos jelenségén, az összefonódottságon alapul és ennek segítségével teszi a csatornát biztonságossá. Nem könnyű egy kvantum rendszert létrehozni és vezérelni. Általánosságban, egy komplex rendszer jobban ki van szolgáltatva minden fajta támadásnak, mint egy egyszerű. Az eszközfüggetlen megvalósítása a titkosító rendszereknek éppen ezt a hátrányt próbálja kiküszöbölni: A protokoll bármilyen eszközzel megvalósítható mindaddig amíg az az eszköz az előírásoknak megfelelően működik. Vannak olyan megoldások is, amelyek még akkor is lehallgatás biztosak ha az eszközt egy ellenséges fél hozta létre. A 4. fejezet ezt a témát járja körbe.

A cikk a kriptográfia kvantumos oldalára kíván koncentrálni. A klasszikus kriptográfia fogalmait megtalálhatja az olvasó bármelyik ezzel foglalkozó tankönyvben, például lásd [4] vagy [24]. Nagyon sok cikk foglalkozik a kvantumkulcs elosztás technikai leírásával, pl. lásd [5] és [6], csak hogy egy párat említsünk.

Ennek a cikknek az ötlete akkor született meg amikor kezembe akadt Mordechai Rorvig cikke [22] a *Quanta magazine*-ben valamint Nyári Norberté [23] a *Biztonságtudományi Szemle* folyóiratban.

ALAPÖTLET: BB84

A kriptográfiában a kulcs-elosztás célja az, hogy nagyon-nagy biztonsággal (kerül amibe kerül) megosszunk egy kis mennyiségű információt, ami később egyszer használatos kulcsként szolgál más üzenetek biztonságos kódolására és dekódolására. Feltételezzük, hogy a kommunikáló felek korábban nem osztottak meg titkos információt egymással: Csak az éppen megosztott kulcsot használhatják titkos kommunikációra.

Kvantumkulcs-elosztás esetén a kommunikáló felek a kvantummechanika segítségével teszik biztonságossá a elosztás folyamatát. A kvantumkulcs-elosztásról szóló első cikket [2, 3] 1984-ben publikálta Charles H. Bennett és Gilles Brassard, innen jön a protokoll neve: BB84. A szokásokhoz híven a kommunikáló feleket Aliznak és Bobnak fogjuk hívni és a lehallgató személy neve Éva lesz, az angol Eve-ből, ami a lehallgatásra (*eavesdropping*) utal. Aliz csak és kizárólag Bobbal szeretné megosztani egy titkos kulcsot, hogy aztán titokban tudjon kommunikálni vele. Ennek érdekében egy kvantum és egy klasszikus csatornát nyit Bob felé, de ezt csak akkor használja amikor a protokoll ezt megengedi. A protokollon kívül a két fél nem kommunikál. A kvantum csatorna kvantum biteket használ, olyan biteket, amelyek megfigyelhetően a kvantummechanika szabályai szerint viselkednek. A klasszikus csatorna szokásos klasszikus biteket használ. A kétfajta bit nagyon másképpen viselkedik ha kérdéseket teszünk fel nekik.

Egyik módja, hogy elképzeljünk egy bitet a következő: Képzeljünk el egy kör alapú kijelzőt (egy tárcsát) rajta egy mutatóval. Ha ábrázolni szeretnénk az 1-es és a 0-s értéket azt nagyon sokféleképpen megtehetjük. Például a mutató irányulhat északra (fel) vagy délre (le) és ekkor azt mondhatjuk, hogy a bit, amit ábrázol 1-es értékű. Vagy mutathat keletre, illetve nyugatra, ami a 0-s értéknek felelhet meg. Egy másik lehetőség az, hogy az 1-es értéket a mutató északkeleti vagy délnyugati állásához rendeljük és északnyugati vagy délkeleti pozíció a 0-s értéknek felel meg.

Tegyük fel Aliz előkészít egy klasszikus bitet a tárcsa és mutató segítségével és elküldi azt Bobnak. Bob rendelkezésére két különböző maszk áll. Az egyiket egyenes vonalúnak (*rectilinear*, R) nevezzük és a bevágások a maszkon észak-déli, illetve kelet-nyugati irányúak. A másikat diagonálisnak (*diagonal*, D) és ennek a maszknak a bevágásai északkelet-délnyugati, illetve északnyugat-délkeleti irányúak. Ha Aliz egy olyan tárcsát küldött Bobnak, ahol a mutató északra néz és Bob az R maszkot használja akkor ki tudja olvasni a bit értékét, ami 1 lesz. Ha Bob a D maszkot használja, akkor semmit nem kap eredményül, de mégis hozzájut bizonyos információhoz, mégpedig ahhoz, hogy nem a megfelelő maszkot használta.

Ezek után tegyük fel, hogy Aliz egy kvantum bitet készít elő egy kvantum tárcsát és mutatót használva, de ugyanazt az ábrázolást használva, mint korábban. Az előkészített bitet, ismét, elküldi Bobnak. Bob ugyanazokkal a maszkokkal rendelkezik, mint eddig. Ha az Aliz által küldött tárcsán a mutató északra néz és Bob az R maszkot használja akkor a helyes értéket, az 1-est, kapja. Azaz, ha Aliz állandóan olyan tárcsákat küld, amelyen a mutató északra néz és Bob állandóan az R maszkot használja akkor folyton a jó eredményt fogja kapni. De ha Bob úgy dönt, hogy a D maszkot használja inkább, akkor azt fogja tapasztalni, hogy minden esetben kap valamilyen értéket, de az esetek felében 1-est kap, míg a többi esetben 0-s értéket fog megfigyelni. Ebben a viselkedésben nyilvánul meg a kvantumos jellege a bitnek. Ha Aliz csak egyetlen bitet küld Bobnak és Bob szabadon választhat

a maszkok közül, akkor nincs módja arra, hogy eldöntse, helyesen döntött és a jó maszkot használta vagy rosszul döntött és értelmetlen eredményt kapott.

Hogyan használhatjuk fel ezt a jelenséget arra, biztonsággal kommunikáljunk? Egy lehetséges válasz a BB84 protokoll.

A folyamat azzal kezdődik, hogy Aliz létrehoz *n* darab véletlen bitet. A sorozat egy része fogja majd a folyamat végén alkotni a titkos kulcsot. Ezen kívül Aliz létrehoz egy másik véletlen bit sorozatot, amelynek a hossza szintén *n*. Ez a második sorozat fogja megmondani Aliznak, bitről-bitre, hogyan ábrázolja az első sorozat bitjeit. Például, a második sorozat minden egyes 1 értékű bitje jelentheti azt, hogy Aliz ezekben az esetekben R jellegű ábrázolást (azaz olyan ábrázolás, amit Bob R maszkkal helyesen fog tudni kiolvasni) fog használni a megfelelő első sorozatbeli bitek esetén. Hasonlóan, ha a második sorozatban egy bit 0, akkor az annak megfelelő első sorozatbeli bitnél Aliz D jellegű ábrázolást fog választani, amit Bob D maszk használata esetén helyesen fog tudni kiolvasni.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	⤢	↔	↔	⤢	⤡	⤡	↔	↕	⤢	⤢

1. Táblázat: A BB84 protokoll első néhány lépése (saját szerkesztés)

Tegyük fel, hogy Aliz létrehozott egy tizenkét bit hosszú sorozatot első körben és még tizenkettőt a második körben. Az 1. Táblázatban látható a folyamat első néhány lépése. Aliz úgy döntött, hogy észak-déli irányú mutató fogja jelenteni az 1-es értéket az R jellegű ábrázolás esetén és az északkelet-délnyugati irányú mutató fogja jelenteni ugyanezt az értéket a D jellegű ábrázolás esetén.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	⤢	↔	↔	⤢	⤡	⤡	↔	↕	⤢	⤢
Bob random bitjei	1	1	0	1	1	1	0	0	1	0	0	0
Maszk	R	R	D	R	R	R	D	D	R	D	D	D

1. Táblázat: Bob mérései (saját szerkesztés)

A következő lépésben Aliz elküldi az első bitsorozatot Bobnak a megfelelő ábrázolásokat használva a kvantum csatornán keresztül: Például fotonokat küld optikai szálon át. Mivel Bob nem tudja Aliz milyen ábrázolás mellett döntött az egyes bitek esetén, ő is létrehoz tizenkét véletlen bitet (*n* bitet, általános esetben) és a kapott bitek alapján választja ki a maszkokat, amelyet az egyes bitek kiolvasásához használni fog. Például dönthet úgy, hogy minden egyes 1-es bit R maszkot jelent és minden egyes 0-s bit egy D maszkot. A mérésének eredményét a 2. Táblázatban láthatjuk.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	⤢	↔	↔	⤢	⤡	⤡	↔	↕	⤢	⤢
Bob random bitjei	1	1	0	1	1	1	0	0	1	0	0	0
Maszk	R	R	D	R	R	R	D	D	R	D	D	D
Fogadott bitek	1	0	1	0	0	0	0	0	0	0	1	1
Megtartott bitek	ok	ok	ok	ok	ok		ok	ok	ok		ok	ok

2. Táblázat: Megtartandó bitek (saját szerkesztés)

Minden olyan esetben, amikor a bit ábrázolása és a maszk megegyezik Bob a helyes eredményt fogja kiolvasni. Ha a bit ábrázolása és a maszk nem egyezik meg az eredmény véletlenszerű lesz. Az esetek közel felében Bob 1-es értéket fog látni és a másik felében 0-s értéket. Amint Bob elkészült a kapott bitek vizsgálatával, a kommunikáló felek kapcsolatba lépnek egymással a klasszikus csatornán keresztül. Ez a csatorna lehallgatható, de nem zavarható. Ezen a csatornán keresztül összevetik Aliz által választott ábrázolási jelleget Bob maszk választásaival. Csak azokat a biteket fogják megtartani, amelyeknél a választások megegyeztek. A 3. Táblázat mutatja Bob mérési eredményeit és hogy mely biteket fogják a felek megtartani.

Tegyük fel, hogy Éva, a lehallgató, figyeli a kvantum csatornát is és a klasszikusat is. Továbbá, tegyük fel, hogy a rendszer tervezői figyelembe vették Kerckhoff elveinek legalább egyikét, ami azt jelenti, hogy a protokoll is és a fizikai megvalósítás részletei is publikusak. Ebben az esetben Éva tudja, hogy a csak kétféle maszkra van szüksége és azt is tudja, hogy milyen jellegű maszkokra. Ennek ellenére, ha bármilyen kapcsolatot létesít a kvantum bitekkel, amelyeket Aliz küldött Bobnak, akkor fennáll a veszélye annak, hogy módosítja azokat: Ha a rossz maszkot használja akkor nem megsemmisíti a bitet, hanem módosítja azt. Éva számára, a kapott eredménye megkülönböztethetetlen egy valódi eredménytől. Ha Éva le tudná másolni a kvantum biteket, amit Aliz küldött és lehallgatva a klasszikus csatornát megszerezné a megfelelő maszk választásokat akkor el tudná dönteni mely biteket tartották meg a kommunikáló felek. De a kvantummechanika nem-klónozhatósági tétele meggátolja Évát ebben. A tétel, a jelenlegi helyzetre alkalmazva, azt mondja ki, hogy nem lehet pontos másolatot készíteni egy tetszőleges ismeretlen kvantum bitről. Mivel Éva számára az elfogott kvantum bit teljesen ismeretlen, a kvantummechanika szabályai szerint nem fog tudni másolatot készíteni róluk.

Végül, Aliznak és Bobnak meg kell győződnie arról, hogy nem hallgatták le őket. Ezt úgy tehetik meg, ha a megtartandó bitek egy részét publikussá teszik és megvizsgálják hányad részük egyezik meg. Ha egy bizonyos küszöböt meghalad azoknak a biteknek a száma, amelyek különbözőek, akkor a felek tudják, hogy valaki hallgatózott és nem tarthatnak meg egyetlen bitet sem. Minden olyan bit, amivel Éva kapcsolatot létesített torzulhatott és így hozzájárulhatott a hibás bitek számához. A küszöbszámot meg lehet határozni ha feltesszük, hogy Éva optimálisan viselkedik [7].

Bár a protokoll feltétel nélkül biztonságos [8, 9], a fizikai megvalósítása lehetőséget teremt támadásra [10]. Ezért indult meg az a törekvés, hogy ezeket a protokollokat eszközfüggetlen módon valósítsák meg. A cikk utolsó nagyobb fejezete ezzel kapcsolatos eredményekkel foglalkozik.

MÉG INKÁBB KVANTUM: BBM92, E91

A BB84 protokoll a Heisenberg-féle határozatlansági elven (egy rendszer megfigyelése hatással van a rendszerre) alapul, együtt a nem-klónozhatósági tétellel. A kvantummechanikának van egy másik sajátsága, ami segíthet abban, hogy a klasszikus védettségnél biztonságosabbá tegyünk egy kommunikációs csatornát.

A kvantummechanikai összefonódottság fogalma azt takarja, hogy kvantum rendszerek egyes részei kapcsolatban állhatnak egymással, de egy olyan értelemben, ami túlmutat a klasszikus kapcsolat fogalmán. A következő képen lehet ezt elképzelni egy ilyen nemklasszikus kapcsolatot két olyan érme esetén, amelyek ilyen kapcsolatban állnak: Ha feldobom az egyik érmét és a dobás eredménye fej, akkor a másik érmét feldobva, a dobás eredménye szintén fej lesz. Ugyan ez igaz az írásra is: Ha feldobjuk az egyik érmét és a dobás eredménye írás, akkor a másik érme feldobása is írást fog eredményezni. A két érme vagy egyszerre fog fejet vagy egyszerre fog írást mutatni, de soha nem fog az megtörténni, hogy az egyik fejet, míg a másik írást mutat. Ha fogunk két ilyen nem-klasszikus módon összekötött érmét és nagyon messze elvisszük őket egymástól, a hatás ugyan az marad, a távolságtól függetlenül. Ez az ötlet zavarta Albert Einsteint és ezért kollégáival Boris Podolskyval és Nathan Rosen-nel egy gondolatkísérletet javasolt, amivel a kvantummechanika hiányosságára szeretett volna rámutatni. Ami akkor egy gondolatkísérletet volt, ma mindennapos rutin a fizika laborokban. Az olyan jellegű kvantum biteket, amelyek rendelkeznek ezzel a nem-klasszikus kapcsolattal gyakran EPR pároknak nevezzük.

Artur K. Ekert [11] bevezetett egy protokollt, amit ma E91-nek neveznek és ami az összefonódottságon alapul. A módszer Bell tételét használta, amely arra szolgál, hogy az összefonódottság miatt keletkezett nem-klasszikus korrelációt számszerűen jellemezze és ezzel mérhetővé tegye.

A protokoll a következőképpen működik. EPR párok egy megbízható forrása a pár egyik kvantum bitjét elküldi Aliznak, a másikat Bobnak. A forrás minden EPR párt úgy állít elő, hogy az négy kívánatos állapot egyikében legyen, például úgy, hogy a párt alkotó bitek tökéletesen korreláltak legyenek. A fentebb említett tárcsa analógiát használva azt látnánk, hogy ha ránéznénk az egyik bitre a párból és a mutatója észak-dél irányú lenne, akkor megvizsgálva a pár másik bitjét, szintén egy észak-dél irányú mutatót látnánk. De ha ránézve az egyik bitre egy kelet-nyugat irányú mutatót látunk, akkor megvizsgálva a másik bitet, szintén egy kelet-nyugati irányú mutatót látnánk.

Aliznak is és Bobnak is van három-három maszkja. Az egyszerűség kedvéért a maszkokra az iránypárok helyett csak egyetlen iránnyal utalunk. Aliz maszkjai keletre, északkeletre és északra mutatnak, míg Bob maszkjai északkeletre, északra és északnyugatra. Mindketten, egymástól és a korábbi mérési eredményektől függetlenül választanak maszkot, minden egyes megfigyelés előtt. Mindketten megvizsgálják a bitet, amit kaptak és lejegyzik a megfigyelésüket, valamint a használt maszkot. Amint végeztek az összes tervezett méréssel publikussá teszik a mérések során használt maszkok sorozatát egy olyan klasz-

szikus csatornán, ami, ismét, lehallgatható, de meggátolja a közvetített információ megváltoztatását. A kapott információ alapján mindketten két csoportra bontják a méréseiknek az eredményét: Az első csoportba kerülnek azok az eredmények, amelyeknél azonos maszkokat használtak, a másik csoportba azok, ahol a maszkok különbözőek voltak.

Ezek után nyilvánosságra hozzák a második csoportba tartozó mérési eredményeket, azaz amikor különböző maszkokat használtak. Az így beszerzett információ alapján ki tudják számítani a mérések közötti korrelációt. Ha Éva megpróbál beavatkozni a folyamatba úgy, hogy az összefonódott párokat bármilyen módon manipulálja, akkor a kiszámított korrelációs érték el fog térni a kvantummechanika által meghatározottól és ezzel Éva felfedi magát.

Ch. H. Bennett, G. Brassard (akikről a BB84 van elnevezve) és N. David Mermin [12] előálltak egy protokollal (BBM92 a neve ma), amelyik a Bell tétel nélkül is működik: Éva nem nyer információt abból, ha megfigyeli a EPR pár bitjeit miközben azok átkerülnek Alizhoz és Bobhoz, mivel információ mérés előtt nem létezik. Amit tehet az, hogy megváltoztatja, mondjuk, Aliz bitjét saját igényei szerint, de ez kiderül a mért korreláció csökkenéséből és így Éva lebukik.

Egyik járhatónak tűnő út Éva számára az, ha lecseréli az EPR párok forrását egy olyanra, amelyben a legyártott EPR párokat titokban összefonja egy kvantum bittel, amelyik csak az övé. A cikkükben Bennett, Brassard és Mermin megmutatja, hogy még ebben az esetben sem tud Éva információhoz jutni úgy, hogy közben rejtve marad: Az egyetlen módja annak, hogy rejtve maradjon az, ha a saját bitjét függetleníti az EPR pártól. Bármilyen extra összefonódás rá fogja nyomni a bélyegét a mérési eredményekre.

Továbbá, az is megmutatható, hogy a BBM92 protokoll ekvivalens a BB84 protokollal, ha a kommunikáló felek közül legalább az egyikük azonnal elvégzi a mérést a kapott kvantum biten. Ha egy összefonódáson alapuló protokoll esetén a méréseket nem végzik el rögtön, hanem csak akkor, amikor szükség van rá a kulcs generálásához, akkor a beérkezett biteken végrehajtott változtatás továbbra is kimutatható a mérésekben. Például, ha egy betörő bejut abba az irodába ahol a beérkezett kvantum biteket tárolják és módosítja azokat, akkor ez a tette napvilágra kerül a mérés során. Ugyanez nem igaz a BB84-re, mert ebben az esetben Aliz klasszikusan tárolja a saját információját.

ESZKÖZFÜGGETLEN MEGVALÓSÍTÁS

Ahogy említettük korábban, egyes kutatók [10] rámutattak a fizikai megvalósításból származó sebezhetőségre. Az összefonódottságon alapuló protokollok még akkor is biztonságosan működhetnek, ha az eszközt magát egy ellenséges fél szolgáltatja, mindaddig amíg az eszköz megfigyelhetően a kvantummechanika törvényei szerint működik: Az előző fejezetben kiderült, hogy a kvantummechanika törvényei teszik lehetetlenné Éva, a lehallgató, számára a rejtett megfigyelést.

Ha Aliz és Bob egy ilyen eszköz mellett döntenek, akkor meg kell győződniük valamilyen módon, hogy amit kaptak egy valódi kvantum eszköz. Ezt például úgy lehet elérni, hogy az eszköznek két üzemi állapota van: Kulcsgeneráló és teszt üzemmód [13]. Aliz és Bob egymással „körökben” kommunikál. Minden egyes kör lehet kulcsgeneráló kör vagy teszt kör. Az egyik ilyen megvalósítás esetén ([14]), Bob bizonyos valószínűséggel eldönti,

hogy az adott kör vajon egy kulcsgeneráló vagy teszt kör és erről tájékoztatja Alizt. A kulcsgeneráló körben Aliz és Bob egy E91 jellegű vagy ennél egyszerűbb protokollal generál biteket amelyeket később a tényleges kulcs létrehozására használnak.

A teszt körben viszont egy játékot játszanak. A játék neve CHSH vagy Clauser–Horne–Shimony–Holt játék [15]. A játékot két együttműködő játékos játssza egy bíró közreműködésével, akit általában Charlie-nak hívnak és itt is ezt fogjuk használni. A játékosok, Aliz és Bob, a játék során nem kommunikálhatnak egymással, de a játék előtt megbeszélhetik milyen stratégia szerint fognak játszani, valamint megoszthatnak egy EPR párt, mivel ezeken a párokon keresztül nem lehet kommunikálni direkt módon. Charlie választ két számot: Az első számnak 0-t vagy 1-et választ ugyanakkora valószínűséggel és ugyanezt teszi a második szám esetén. Az első számot elküldi Aliznak, a másodikat Bobnak. Amint Aliz megkapja a számot Charlie-től, egy megfelelő stratégiát követve, visszaküld egy 0-st vagy egy 1-est Charlie-nak. Ugyanezt teszi Bob is. Charlie bíráskodik: Végrehajt egy logikai ÉS műveletet azokon a számokon, amelyeket kiküldött Aliznak és Bobnak és egy modulo 2 összeadást a két biten, amit a játékosok küldtek vissza. Ha a számítások eredményei megegyeznek akkor Aliz és Bob nyer.

A játék klasszikus, lokális változatában, azaz amikor EPR pár nem kerül felhasználásra, átlagosan, az esetek legfeljebb 75%-ban nyerhetnek a játékosok. Ha használják az EPR párt úgy, hogy mérést végeznek rajta, akkor a nyerési esély felmegy nagyjából 85%-ra. Ha az EPR pár hamis vagy meg lett bolygatva, akkor a nyerési esély visszább megy.

Lehetséges, hogy Éva hallgatózik, de ez nem gond: A CHSH játék esetén számszerűen meg lehet határozni mennyi információ szivárog ki Éva felé abból, ahogyan csökken a játék nyerési valószínűsége. Ha a kiszivárgott információ mennyiség elfogadható vagy van valami módszerük arra, hogy a problémát megkerüljék (például ilyen megoldás a „titoktartás erősítése", *privacy amplification*, lásd [14, 16, 17]), akkor még mindig kinyerhetnek egy titkos kulcsot az adatokból, amit Éva nem fog ismerni.

Úgy tűnik, hogy a kutatóknak végre sikerült legyőzni a jelenlegi technológia adta akadályokat: A [14, 16, 17] cikkek, amelyek közel egy időben jelentek meg, arról számolnak be, hogy sikerült valódi eszközfüggetlen kulcs-elosztást megvalósítani.

KONKLÚZIÓ

Van egy pár kérdés, amit érdemes feltenni. Mi a helyzet akkor, ha a kvantummechanika nem érvényes minden körülmények között vagy létezik valami olyan postkvantum fizika amely lehetővé teszi egy fejlett civilizációnak, hogy lehallgasson bennünket. A jó hír az [18], hogy Jonathan Barrett, Lucien Hardy és Adrian Kent szerint egyszerűen csak egy fizikára van szükségünk, amely kizárja a fénysebességnél gyorsabb kommunikációt.

Ebben a cikkben és úgy általában az irodalomban (lásd például [19]) gyakran használunk olyan kifejezéseket, hogy „Aliz kiválaszt egy ábrázolást" vagy „Bob kiválaszt egy maszkot". Mi történik abban az esetben, ha a fizika nem engedi meg a szabad vagy független választást? Mi van akkor, ha a szuperdeterminizmus igaz és a jelenlegi döntéseink mind összefüggenek vagy korreláltak? A szuperdeterminizmus [20] a Bell tétel egy kiskapuja és természetesen nem egy új probléma. John Bell elismerte a létezését és foglalkozott a kérdéssel [21]. A vita még nincs lezárva, de úgy tűnik, hogy a válasz nem változtat igazán semmit a mindennapokban használt modellek jellegén.

ÖSSZEFOGLALÓ

Amint a kvantum számítógépek megjelennek a hétköznapokban, veszélyt fognak jelenteni a jelenlegi titkosítási módszerekre. Jó tudni, hogy ugyan ez a technológia válasszal tud szolgálni a problémára és a segítségével, úgy tűnik, meg fogjuk tudni őrizni a számunkra fontos adataink biztonságát.

FELHASZNÁLT IRODALOM

[1] D. Castelvecchi, "The race to save the Internet from quantum hackers", *Nature, vol.* 602, no. 7896, 198–201, 2022.

[2] Ch. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Conf. on Computers, Systems and Signal Processing* (Bangalore, India), pp. 175-179, 1984.

[3] Ch. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science* vol. 560, 7-11, 2014, DOI https://doi.org/10.1016/j.tcs.2014.05.025. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[4] Ch. Paar and J. Pelzl, "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media, 2009.

[5] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey", ACM Computing Surveys (CSUR) vol. 39, no. 2, 1–31, 2007.

[6] A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography", *Archives of Computational Methods in Engineering,* vol. 28, no. 5, 3831–3868, 2021.

[7] Ch. A. Fuchs, N. Gisin, R. B. Griffiths, Ch-Sh. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy", *Physical Review A,* vol. 56, no. 2, 1163, 1997.

[8] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", *Physical review letters,* vol. 85, no. 2, 441, 2000.

[9] H-K. Lo, "A simple proof of the unconditional security of quantum key distribution", *Journal of Physics A: Mathematical and General,* vol. 34, no. 35, 6957, 2001.

[10] V. Scarani and Ch. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems", *Theoretical Computer Science,* vol.560, 27–32, 2014.

[11] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett*. vol. 67, 661-663, 1991.

[12] Ch. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical review letters,* vol. 68, no. 5, 557, 1992.

[13] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and Th. Vidick, "Practical device-independent quantum cryptography via entropy accumulation", *Nature communications,* vol. 9, no. 1, 1–11, 2018.

[14] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J-D. Bancal, "Device-independent quantum key distribution", arXiv preprint arXiv:2109.14600, 2021.

[15] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical review letters,* vol. 23, no. 15, 880, 1969.

[16] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, V. Scarani, Ch. C-W. Lim, and H. Weinfurter, "Experimental device-independent quantum key distribution be-tween distant users", arXiv preprint arXiv:2110.00575, 2021.
[17] W-Zh. Liu, Y-Z. Zhang, Y-Zh. Zhen, M-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J-W. Pan, "High-speed device-independent quantum key distribution against collective attacks", arXiv preprint arXiv:2110.01480, 2021.
[18] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution", *Physical review letters,* vol. 95, no. 1, 010503, 2005.
[19] A. Ekert and R. Renner, "The ultimate physical limits of privacy", *Nature,* vol. 507, no. 7493, 443–447, 2014.
[20] J-A. Larsson, "Loopholes in Bell inequality tests of local realism", *Journal of Physics A: Mathematical and Theoretical,* vol. 47, no. 42, 424003, 2014.
[21] J. S. Bell, "Free variables and local causality", *Quantum mechanics, high energy physics and accelerators. Selected papers of John S. Bell (with commentary),* 1995.
[22] M. Rorvig, "Cryptographers Achieve Perfect Secrecy With Imperfect Devices" (February 25, 2022), https://www.quantamagazine.org/cryptographers-achieve-perfect-secrecy-with-imperfect-devices-20220225/. Accessed March 13, 2022.
[23] N. Nyári, "The Impact of Quantum Computing on IT Security", *Biztonságtudományi Szemle,* vol. 3, no. 4, 25-37, 2021.
[24] Buttyán L. és Vajda I., „Kriptográfia és alkalmazásai", Typotex Kiadó, 2005.

THE CURRENT STATE AND POSSIBILITIES OF eSZEMÉLYI AND ELECTRONIC SIGNATURE TECHNOLOGY IN HUNGARY

AZ eSZEMÉLYI ÉS AZ ELEKTRONIKUS ALÁÍRÁS TECHNOLÓGIA HELYZETE ÉS LEHETŐSÉGEI MAGYARORSZÁGON

NYÁRI Norbert [1]

Abstract

The aim of the present study is to determine the factors influencing the trust in electronic signature technology in Hungary, as well as the factors hindering its spread, and finally to explore new ways to facilitate the spread of the technology. To carry out the primary research, I chose a qualitative research methodology and conducted two focus group interviews. I used the Grounded Theory method to analyze the data generated during the interviews. The study provides an overview of the basic concepts of trust, possible ways to measure trust, and the current state of eSzemélyi and electronic signatures, based on available statistics and data from interviews. The results can make an effective contribution to the widespread use of electronic signature technology in Hungary.

Keywords

digital signature, electronic signature, IT security, infromation security, Grounded Theory

Absztrakt

Jelen tanulmány célja annak megállapítása, hogy milyen tényezők befolyásolják az elektronikus aláírás technológiába vetett bizalmat Magyarországon, továbbá, hogy milyen tényezők gátolják annak elterjedését, végül pedig új utak felderítése a technológia térhódításának elősegítése érdekében. A primer kutatás végrehajtásához kvalitatív kutatási módszertant választottam, két fókuszcsoportos interjút vezettem le. Az interjúk során keletkezett adatok elemzéséhez a Grounded Theory módszert használtam. A tanulmány áttekintést nyújt a bizalommal kapcsolatos alapfogalmakról, a bizalom mérésének lehetséges módjairól, továbbá az eSzemélyi és az elektronikus aláírás jelenlegi helyzetéről az elérhető statisztikai adatok, valamint az interjúkból kinyert adatok alapján. Az eredmények hathatósan hozzájárulhatnak az elektronikus aláírás technológia széleskörű elterjedéséhez Magyarországon.

Kulcsszavak

digitális aláírás, elektronikus aláírás, informatikai biztonság, információbiztonság, Grounded Theory

[1] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | PhD student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az eIDAS rendelet egy egységes modellt definiál az elektronikus aláírások alkalmazására az Európai Unió területére. Az úgynevezett eSzemélyi igazolvány a magyar megfelelője az állampolgárok azonosítására szolgáló igazolványnak, melyet az eIDAS meghatároz. Az eSzemélyi képes személyre szóló digitális tanúsítvány (és még további egyéb adatok) tárolására. Számos használati eset említhető az igazolvány vonatkozásában: dokumentumok (pl. gépjármű, vagy ingatlan adásvételi szerződések) elektronikus aláírása, hitelesítés e-kormányzati szolgáltatások használatához. Az igazolvány előnyeinek kihasználáshoz szükség van egy számítógépre, és egy ahhoz csatlakoztatott kártyaolvasó készülékre (okostelefonnal és az eSzemélyiM applikációval kiváltható). [1]

A tárolóelemmel rendelkező eSzemélyi igazolványok különféle adatok tárolására alkalmasak, például: digitális tanúsítvány elektronikus aláíráshoz, baleset esetén értesítendő személyek telefonszáma, lakcím adatok, azonosítószámok (TAJ szám, személyi szám), ujjnyomat stb. [2]

Az igazolvány főbb felhasználási területei: elektronikus azonosítás, közösségi közlekedés, postai küldemények átvétele, külföldi utazás és úti okmány (EU-n belül) valamint elektronikus aláírás (e-aláírás). Jelen tanulmány szempontjából a legfontosabb használati eset azonban az elektronikus aláírás így a továbbiakban erre fogok összpontosítani. [3]

Az elektronikus aláírás egy jogi kategória, amit világszerte többféleképp szabályoznak. Az Európai Unió területén a kérdést az úgy nevezett eIDAS (“electronic IDentification, Authentication and trust Services”, „elektronikus azonosítás, hitelesítés és bizalmi szolgáltatások”) rendelet szabályozza, amely alapvetően háromféle elektronikus aláírást határoz meg: „elektronikus aláírás”, „fokozott biztonságú elektronikus aláírás” és „minősített elektronikus aláírás”. [1]

A legnagyobb bizonyítóerővel a minősített elektronikus aláírások bírnak. Ehhez az elektronikus aláírásfajtához ugyanis a jogszabály a kézi aláírásokkal megegyező joghatást rendel. Vannak azonban megkötések, melyeknek a minősített aláírások készítése során meg kell felelni: „minősített elektronikus aláírást létrehozó eszközzel” kell előállítani „elektronikus aláírás minősített tanúsítványának” használatával. [1]

A magyar eSzemélyi használatával – feltéve, hogy rendelkezik minősített tanúsítvánnyal – bármely állampolgár létrehozhat minősített elektronikus aláírást, amely köszönhetően az eIDAS következetes nemzetközi és nemzeti alkalmazásának az EU bármely tagállamában a hagyományos, kézi aláírással egyenértékűen elfogadott lesz. Ezzel az elektronikus aláírással teljes bizonyító erejű magánokiratok is létrehozhatók elektronikus ügyintézés során (magánjogi és közigazgatási jogi ügyekben egyaránt). [1] [3]

A „414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól” meghatároz a minősített tanúsítványokkal kapcsolatosan egy ún. tranzakciós limitet, ami a maximális értéke annak a pénzügyi felelősségvállalásnak, amelyet az aláíró az elektronikus aláírásával tehet. Az eSzemélyi igazolványon található tanúsítványokat a NISZ Zrt. állítja ki, a tranzakciós limit pedig az előbbi jogszabály alapján 50.000.000,- Forint. [4]

Fontos, hogy a magyar igazolványon található tanúsítvánnyal kizárólag magáncélú esetekben írhatnak alá az állampolgárok, vagyis cég képviseleti minőségében nem használhatják eSzemélyi igazolványukat dokumentumok aláírásra cégek képviselői. [5]

Elektronikus aláíráshoz természetesen más magyarországi szolgáltatótól is lehetséges tanúsítványt vásárolni, úgymint Netlock Kft., Microsec Zrt. Ezekkel már jogszerűen lehet céges ügyekben elektronikus aláírásokat létrehozni. Jelen kutatásban azonban az állampolgárok számára a legtermészetesebb módon elérhető elektronikus aláírás kérdéskörét szeretném részletesen megvizsgálni, ezért a továbbiakban csak az eSzemélyi igazolványra fogok koncentrálni.

Jelen tanulmány célja, hogy kivizsgálja az emberek elektronikus aláírásokba vetett bizalmának kérdéskörét Magyarországon kvalitatív kutatási módszertan alkalmazásával. Feltevésem szerint ugyanis pszichológiai tényezők hátráltatják Magyarországon az elektronikus aláírások széleskörű elterjedését: az emberek kevésbé bíznak meg a technikai eszközökkel támogatott elektronikus aláírásokban, mint a hagyományos, kézi aláírásokban.

SZAKIRODALMI ÁTTEKINTÉS

A bizalom alapvetően egy szociológiai, pszichológiai fogalom, amely többféle relációban is megfigyelhető. Elsősorban az interperszonális viszonyokban értelmezett, az emberek ugyanis ösztönösen hajlamosak értékelni más emberek, embercsoportok, szervezetek megbízhatóságát. [6, 7] Fukuyama [8] értelmezésében a személyek közötti bizalom kölcsönös morális elkötelezettségen és belsővé tett etikai szokásokon alapul.

Ugyanakkor beszélhetünk gazdasági értelemben vett bizalomról is, amikor személy-szervezet vagy szervezet-szervezet relációban merül fel. Jelen kutatás jellege miatt a továbbiakban a személy-személy illetve a személy-szervezet relációban értelmezett bizalomról lesz szó. [7]

A bizalom definíciója Mayer et al. [7] szerint a következő: a bizalmat adó (trustor) hajandósága arra, hogy sérülékenységét felvállalja egy másik fél, a bizalmat kapó (trustee) felé. Cikkük szerint a bizalom úgy mérhető, ha a kutatásban résztvevő megbízóknak olyan kérdéseket teszünk fel, melyek a megbízott felé tanúsított kockázatvállalási hajlandóságukra vonatkoznak.

A bizalom McKnight és Chervany [9] modellje alapján három alapvető kategóriára osztható:

- feltétlen bizalom vagy ősbizalom: bárki és bármi iránti feltétel nélküli bizalom,
- intézményi bizalom: egyes intézményekkel, szervezetekkel szemben tanúsított bizalom,
- interperszonális bizalom: emberek egymás közötti bizalma. [10]

Jelen téma szempontjából az intézményi bizalom és az interperszonális bizalom érdemel különös figyelmet, hiszen az elektronikus aláírásokat használóknak bizalommal kell lenniük az eIDAS-ban definiált, a tanúsítványokat kibocsátó bizalmi szolgáltatók (intézményi bizalom) továbbá a szerződő partnerek felé is (interperszonális bizalom).

A bizalom többdimenziós mivoltát erősiti meg Paine [11] munkája is, mely szerint a bizalom többszintű (személyek, csapatok, szervezetek közötti), és időben dinamikusan változó (fázisok építés, destabilizáció, felbomlás). A dimenziók többek között a sérülékenységet, őszinteséget, elkötelezettséget és a kölcsönösséget is magukban foglalják. A bizalom különböző dimenzióinak méréséhez módszertani ajánlást is tesz.

Lynn és társai [12] a számítási felhőszolgáltatásról szóló írásukban kitérnek arra, hogy a személyes kapcsolat, jelenlét hiánya negatívban befolyásolja a felek közötti bizalmat. Meglátásuk szerint az online térben az is nehezíti önkiszolgáló, magánszemély és szervezet közötti

szerződéskötést, hogy a felek nem tudják megtárgyalni a szerződéses feltételeket, így a potenciális szerződő választási lehetőségei igen nagy mértékben redukálódnak: lényegében egy eldöntendő kérdés marad, hogy elfogadja-e a feltételeket vagy nem. Meglátásaikra a továbbiakban is érdemes figyelemmel lenni, mivel a szerződő felek közötti személyes kapcsolat az elektronikus aláírás alkalmazásakor akár teljes mértékben is hiányozhat.

Az elektronikus kereskedelem területén megkülönböztethető általános és specifikus bizalom. Az előbbi, az általános bizalom elemei lefedik mindazon elemekbe, mechanizmusokba vetett bizalmat, amely egy elektronikus tranzakció megfelelő és biztonságos lebonyolításához szükségesek, beleértve az általános bizalmat az IT infrastruktúrába is. A specifikus bizalom ezzel szemben közvetlenül a tranzakcióban részt vevő partnerhez kapcsolódik ideértve a jóakaratot, becsületességet, szakszerűséget is. [13, 14]

Gelei-Dobos [6] a bizalmat a Mayer et al szerinti definícióval megegyezően értelmezik, de különbséget tesznek bizalom (trust) és bizalomra méltóság (trustworthy) között. Megállapításaik szerint a bizalomra méltóság mértéke befolyásolja a kockázatvállalási hajlandóságot a felek között. Magas kockázatú ügyletek akkor jöhetnek létre, a bizalomra méltóságot a felek egymásra nézve kölcsönösen magas szinten állapítják meg. [6, 7]

Előbbi megközelítés tovább cizellálható, a szakirodalom ugyanis az elektronikus okiratok esetében két kvalitatív dimenzióra osztja a bizalomra méltóság fogalmát: megbízhatóság (reliability) és hitelesség (authenticity). A megbízhatóság az jelenti, hogy az okirat tartalma megfelelően reprezentálja azt a jelentést, amelyet tanúsítani hivatott. A hitelesség pedig az okirat olyan attribútumait takarja, mint az eredetihez való hűség állapota, valamint a sértetlen és igazolt származás, vagyis az tanúsítja, hogy az okirat valóban az, aminek látszik. [15, 16]

Kiss [17] az internet elterjedtségének hiányával és a lakosság bizalmatlan hozzáállásával és a lehetséges használati esetek alacsony számával indokolja az elektronikus aláírás korlátozott elterjedését. Azóta az internet széleskörben elterjedt ugyan Magyarországon, de a másik két tényező továbbra is fennállhat. Amint az fentebb olvasható, a magyar eSzemélyi elektronikus aláírás használati esetei korlátozottak.

Ez a lakossági bizalmatlanság látszódhat a Belügyminisztérium Informatikai Helyettes Államtitkárság rendszeresen megjelenő statisztikáiból is: az állampolgárok csak igen alacsony százaléka igényel olyan eSzemélyit, amelyen az elektronikus aláíráshoz használható digitális tanúsítvány is telepítve van. [18]

2016 óta lehetséges eSzemélyi igazolványt igényelni. [2] A Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság honlapján (www.nyilvantarto.hu) 2020-ig visszamenőleg olvashatók a statisztikák havi bontásban. Lásd a lenti táblázatot. [18] [19] [20] [21]

Év	Összes igénylés [db]	Tárolóelemet tartalmaz [db]	e-aláírás funkció tartalmaz [db]	e-aláírás funkció tartalmaz [%]
2020.	1.058.777	986.511	20.743	2,39
2021.	1.350.533	1.306.010	16.246	1,60
2022 február végéig	278.324	278.324	3.491	1,25
2016-tól 2021 decemberéig összesen	**7.770.800**	**7.186.858**	**289.889**	**4,76**

1. táblázat eSzemélyi igénylések statisztikája, forrás: https://nyilvantarto.hu/hu/statisztikak

Felhívnám a figyelmet, hogy a fenti táblázat utolsó sora nem tartalmazza az idei év első két hónapjára vonatkozó adatokat. [20]

Amint az a statisztikákból látszik a magyar állampolgárok csak igen alacsony százaléka rendelkezik eSzemélyi igazolványán elektronikus aláírás létrehozásra alkalmas tanúsítvánnyal. Továbbá sajnálatos módon 2020 óta csökkenő tendenciát mutat az egyébként is alacsony arányban igényelt e-aláírás szolgáltatás.

KUTATÁSMÓDSZERTAN

Jelen tanulmány legfőbb kutatási célja annak megállapítása, hogy az emberek mennyire tartják bizalomra méltónak az eSzemélyi igazolványt és általában az elektronikus aláírásokat Magyarországon. Mint azt már korábban is említettem az eSzemélyi számos használati esettel bír, mint például elektronikus aláírás, az állampolgárok akár nagyobb értékű vagyontárgyak (gépjármű, ingatlan) megvásárlására is szerződhetnek használatával. Cél továbbá az emberek attitűdjének felderítése az elektronikus aláírásokkal szemben, hogy mélyreható betekintést nyerhessünk a kérdéskörbe.

A téma sok kérdést felvet, különösképpen akkor, ha abból a feltevésből indulunk ki, hogy az emberek kevésbé bíznak meg az elektronikus aláírásokban, mint a hagyományos, kézi aláírásokban. A főbb kutatási kérdések az alábbi táblázatban olvashatók.

Sorszám	Kutatási kérdés
K1	Megbíznak-e annyira az elektronikus aláírásokban, mint a hagyományos aláírásokban?
K2	Milyen tényezők befolyásolják az elektronikus aláírásba vetett bizalmat?
K3	Milyen tényezők hátráltatják az elektronikus aláírások elterjedését?
K4	Hogyan lehetne elősegíteni az elektronikus aláírások széleskörű használatát?

2. táblázat Kutatási kérdések (saját szerkesztés)

A kutatás végrehajtásához kvalitatív kutatási módszertant választottam, egészen pontosan a fókuszcsoportos kutatást. A kvalitatív kutatási módszertanok az emberek tapasztalataira építve juttathatnak új információkhoz. [22]

Sandelowski [23] azt írja, hogy a kvalitatív kutatási módszertanok a döntéshozatalt is támogathatják különféle területeken. Sandelowski ugyan egészségügyi területen alkalmazta a módszertant, megállapításai más tudományterületekre is alkalmazhatók.

A fókuszcsoportos beszélgetések segítségével betekintést nyerhetünk az emberek érzelmeibe, érzéseibe, vagyis attitűdök kutatására alkalmas. A kötetlen beszélgetés kellőképpen felhőtlen légkört biztosíthat ahhoz, hogy bátrabban nyilatkozzanak a résztvevők így olyan váratlan információk is felszínre kerülhetnek, melyekkel a kutatást lebonyolító moderátor nem is számolhat előre. [24]

A módszer segíthet meggyőződések felszínre hozásában, de ami talán a legfontosabb jelen kutatás szempontjából, hogy megérthetünk bizonyos magatartásformákat. [24]

A fókuszcsoport egyik további előnye, hogy a standardizált kérdőívekhez képest gyorsabban végrehajtható. Továbbá a kérdések, a beszélgetés nyílt jellege is előnyös tulajdonság, különösen jelen kutatás esetében, hiszen a fenti kutatási kérdések megválaszolásához mélyebb beszélgetésekre, további felmerülő kérdésekre és hosszabb magyarázatokra lehet szükség. [25] [24]

Legtöbbször termékekkel, márkákkal, reklámkampányokkal kapcsolatos fogyasztói attitűdök mérésére használatos. [25] Jelen kutatásban az eSzemélyi tekinthető terméknek, és az

e-aláírás a termék igénybe vehető szolgáltatásának ezért is alkalmas lehet a kutatási kérdések megválaszolására a fókuszcsoportos kutatás.

Természetesen hátrányai is vannak a módszernek, bizonyos esetekben nehezen rendszerezhető és értelmezhető adathalmaz lehet az eredménye, melyet a kutató félreértelmezhet. [24] Kelemen-Erdős [26] szerint a fókuszcsoportos beszélgetések eredményei bár nem tekinthetők reprezentatívnak, lehetővé teszik egymásnak ellentmondó nézetek és vélemények bemutatását és kompromisszumokra ösztönöznek.

Véleményem szerint a hátrányok ellenére a fókuszcsoportos kutatás a legalkalmasabb jelen kérdéskör felderítésére, hiszen az eSzemélyivel és az elektronikus aláírásokkal kapcsolatos attitűd felszínre hozása a cél, amelynek megfogalmazására az átlag állampolgár valószínűsíthetően nem is gondol.

A csoportok létszámát tekintve úgy nevezett mini-csoporttal dolgoztam, amely általában 4-6 fős létszámú. A kisebb létszámnak köszönhetően nem aprózódnak el a beszélgetések és valószínűleg a mögöttes, mélyebben gyökerező vélemények is felszínre jöhetnek. Az összetételt tekintve konfliktus csoportokat alakítottam ki, ami bizonyos szempontok szerint inhomogén összetételt jelent. [25]

Két fókuszcsoportos beszélgetést készítettem, csoportonként öt részvevővel. A csoportok összetételüket tekintve vegyes csoportok abból a szempontból, hogy a résztvevők eSzemélyi igazolványán van-e telepítve elektronikus aláírásra szolgáló tanúsítvány.

A két vegyes csoport az aktív korúak közül az alábbi táblázatban felsorolt két korcsoportra tagozódik.

Sorszám	**Korcsoport**	**Létszám**
1	18-30 éves	5 fő
2	31-65 éves	5 fő

3. táblázat Fókuszcsoportok (saját szerkesztés)

A fókuszcsoportos beszélgetéseken összegyűjtött adatokat többféle módszerrel is elemezhetjük: állandó összehasonlítás módszere, klasszikus tartalomelemzés, diskurzuselemzés stb. [27] Kelemen-Erdős [28] tizenkét kutató megkérdezésének kiértékelésére a Grounded Theory (GT) módszert használta tanulmányában, amely a szolgáltatás-domináns logika (SDL) és a vásárló domináns logika (CDL) viszonyát vizsgálta.

Kelemen-Erdős és Mitev [29] szintén a Grounded Theory (GT) módszert alkalmazta 95 interjúból összegyűjtött adatok kiértékelésére a fogyasztói attitűdöket és percepciókat vizsgáló tanulmányában.

A fókuszcsoportos beszélgetések során összegyűjtött adatok kiértékeléshez a GT módszert választottam, mert ennek segítségével tudományosan elfogadott formában lehetséges kvalitatív adatokból szisztematikusan eredményeket kinyerni. [26]

Az adatok kódolása során az ún. open coding (nyílt kódolás) megközelítést alkalmaztam. A kialakult kódokat ezt követően axial coding (axiális kódolás) segítségével kategóriákba csoportosítottam, végül a kategóriákat összefogására kialakítottam egy core category-t (fő kategóriát). A kódokat és a kategóriákat ’[’ és ’]’ jelekkel körül határoltan jelöltem. [30]

KUTATÁSI EREDMÉNYEK, KÖVETKEZTETÉSEK

Az adatok kódolása során megállapítható volt, hogy az interjúalanyok véleménye kortól és előképzettségtől függetlenül egy fő kategória felé mutattak ez pedig a ***[Használati esetek hiánya és ismerethiány]***.

Az alábbi táblázatban kiemelem a legfontosabb kategóriákat és kódokat hierarchiába rendezve, amelyek a GT elemzés során felmerültek.

[Használati esetek hiánya és ismerethiánya]		
[Nincs használati eset]		
	[Nincs megfelelő infrastruktúra]	
		[Kártyaolvasó]
	[Új használati esetekre lenne szükség]	
		[Fizetés]
		[Összevonás más okmányokkal]
		[Ügyvéd]
		[Autókereskedés]
		[Postai kézbesítés]
	[Könnyebbé kellene tenni a használatát]	
		[Aktiválás]
		[Mobilalkalmazás]
		[Ingyenes kártyaolvasó]
	[Átláthatóbbá kell tenni a használatát]	
		[Felhőszolgáltatás]
[Ismerethiány]		
	[Alapszintű ismeretek hiánya]	
		[Biztonság]
		[Technológiai szakadék]
		[Ügyintéző nem tájékoztat]
		[Oktatás]
	[Népszerűsíteni kellene az eSzemélyit és az elektronikus aláírást]	
		[Tájékoztató anyagok]
		[Kedvezmény használat esetén]
		[Reklámkampány]
		[Kötelezés]
		[Filmek]
		[Veszélytelen próbálkozás]

4. táblázat GT elemzés kategóriák, kódok (saját szerkesztés)

A *K1 kutatási kérdés* azt vizsgálja, hogy az elektronikus vagy a hagyományos aláírás bizalomra méltóbb az emberek szemében. A magyar jogszabályi környezet is sugall egyfajta bizalmatlanságot, hiszen ahogy azt korábban is írtam, az elektronikus aláírások nem használhatók korlátlanul, meghatározásra került ugyanis egy 50 millió Forintos felső értékhatár az elektronikus aláírással történő kötelezettség vállalásokra.

A beszélgetésekből kiderül, hogy a technológiával szembeni általános bizalom nem elég szilárd. Az okozza a problémát, hogy nem rendelkeznek megfelelő ismeretekkel arról, hogy milyen körülmények között, milyen esetekben használható biztonságosan az eSzemélyi igazolvány elektronikus aláírás funkcionalitása. Ezt támasztják alá a [Alapszintű ismeretek hiánya] kategória.

A fiatalabb és a középkorú korosztály számára nem okozna problémát, hogy használja az elektronikus aláírás szolgáltatást a megengedett maximális értékhatárig, de a legtöbben azt a határozott véleményt képviselték, hogy nincsenek tudatában annak, hogy egyáltalán milyen használati esetei lehetnek Magyarországon az eSzemélyienk és az elektronikus aláírásnak, továbbá a technikai feltételek sem adottak ahhoz, hogy a mindennapi élet részévé válhasson az elektronikus aláírás, ami tovább gyengíti a technológia felé tanúsított általános bizalmat ([Nincs használati eset] és [Nincs megfelelő infrastruktúra])

A bizalmat befolyásoló tényezőkkel a *K2 kérdés* foglalkozik. Megállapítható, hogy a bizalmat az előképzettség és az életkor is befolyásolhatja. Az adatokból látszik, hogy a megkérdezettek – néhány kivételtől eltekintve – nem rendelkeznek elégséges ismeretekkel a témakörben (nem ismerik a digitális aláírás technológia működését, a különbséget az elektronikus és a digitális aláírás között stb.). Természetesen nem tekinthető reális elvárásnak az állampolgárokkal szemben, hogy mély kriptográfiai ismeretekkel rendelkezzenek, de a használathoz feltétlenül szükséges mélységű ismeretek birtokában kellene lenniük.

A [Technológiai szakadék] kategóriából látszik, hogy a nyugdíjas korosztály, akik életük jelentős részében a hagyományos aláírásokhoz szoktak hozzá, és nem rendelkeznek gyakorlattal a számítástechnikai eszközök használatában valószínűleg ellenállást tanúsítanának az új technológiával szemben. Szintén az ismeretek hiányára vezethető vissza a probléma, viszont esetükben legtöbbször olyan mértékű technológiai szakadék jelentkezhet, amely már áthidalhatatlan. Megállapítható, hogy a technikai felkészültség alacsony szintjéből következik az általános bizalom alacsony szintje.

A *K3 kérdés*, 'Milyen tényezők hátráltatják az elektronikus aláírások elterjedését?'. A beszélgetésekből látszik, hogy alapvetően két fő probléma gátolja a technológia térhódítását: [Ismerethiány] és [Nincs használati eset].

Az [Ismerethiány]-t tovább bontva azt tapasztalhatjuk, hogy sok esetben már az eSzemélyi igénylés, a Kormányablakban történő ügyintézés során nem kapnak az ügyfelek tájékoztatást arról, hogy milyen tulajdonságokkal rendelkezik az eSzemélyi, milyen szolgáltatások vehetők igénybe. Ennek több oka is lehet (ügyintézők oktatásának hiányosságai, motiváltság hiánya stb.), ezek felderítése azonban nem része jelen tanulmánynak.

Olyan esetekről is beszámoltak az interjúalanyok, ahol az ügyintézők az új okmány átadásakor közölték, hogy „úgysem jó semmire", mert nem áll rendelkezésre a szükséges infrastruktúra.

Felmerült az interperszonális bizalom hiánya magánszemélyek közötti szerződéskötések esetén. Egyes interjúalanyok tartanának attól, hogy a másik fél a szerződéskötés során valamilyen módon csalást követ el (pl. ellopja/lemásolja a kártya adatokat). Vagyis az ismerethiány a specifikus bizalmat is gyengítheti. ([Biztonság])

Az [Ismerethiány]-t támasztja alá, hogy az interjúalanyok többsége még csak felszínesen sem ismeri a technológiát – felhasználói szempontból sem. Legtöbben nem voltak tisztában azzal sem, hogy van-e tanúsítvány a kártyájukon, ha van, akkor az meddig érvényes.

Ezen a ponton az [Ismerethiány] és a [Nincs használati eset] kategóriák között kapcsolatot lehet felfedezni: azért sem rendelkeznek információkkal a saját eSzemélyi igazolványaikról (tanúsítvány lejárata stb.), mert nem használják a szolgáltatásaikat napi szinten.

Az interjúalanyok hiányolták a különféle tájékoztató anyagokat, a step-by-step leírásokat, útmutatót a kártyaolvasó kiválasztásához, megvásárlásához. Ezek az információk az eszemelyi.hu portálon megtalálhatók, ezzel azonban az interjúalanyok nem voltak tisztában.

A használati esetek hiánya a megkérdezettek szerint végsősoron abból fakad, hogy kártyaolvasó szükséges a használatához. A kártyaolvasóval több problémát is jeleztek az interjúalanyok: nincs ismeretük arról, hogy milyen típusú kártyaolvasóval kompatibilis az eSzemélyi ([Ismerethiány]), pénzbe kerül és nem érzik, hogy megtérülne a vásárlásba fektetett összeg. Könnyítené a használatot egy mobilalkalmazás, amellyel kiváltható lenne a kártyaolvasó. Ilyen alkalmazás létezik eSzemélyiM néven, ezt azonban nem ismerték, ami szintén az [Ismerethiány]-t támasztja alá.

K4 kutatási kérdés: 'Hogyan lehetne elősegíteni az elektronikus aláírások széleskörű használatát?' Több kategóriában is születtek javaslatok arra nézve, hogy milyen intézkedések segítenék elő az eSzemélyi és az elektronikus aláírás terjedését Magyarországon.

Először is: [Nincs használati eset]: új használati esetek bevezetésével ([Új használati esetekre lenne szükség]), amelyek a mindennapi életben gyakran előfordulnak motiválhatók lennének az állampolgárok az eSzemélyi használatára:

- legyen lehetőség bankkártya helyett fizetésre használni,
- legyen összevonva az eSzemélyibe több okmány (TAJ kártya, vezetői engedély, diákigazolvány, bankkártya, SZÉP kártya stb.),
- postai kézbesítéskor legyen használható a küldemények átvételének igazolására,
- ügyvédnél, közjegyzőnél legyen lehetőség elektronikus aláírásra használni,
- autókereskedésekben legyen lehetőség elektronikusan aláírni a segítségével,
- bankokban legyen lehetőség elektronikus aláírásra használni.

Használati esetek szintjén a specifikus bizalom erősnek bizonyult a beszélgetések során, a megkérdezettek csak egy-két esetben említettek olyan tényezőket, amelyek negatívan befolyásolnák a bizalmat.

A K3 kérdés tárgyalásánál említett interperszonális bizalom hiányosságait hivatott pótolni az ügyvéd/közjegyző hivatalába vetett intézményi bizalom. Ügyvédi/közjegyzői felügyelet és ellenjegyzés mellett a specifikus bizalom erősödne a megkérdezettekben.

Az [Új használati esetekre lenne szükség] szorosan kapcsolódik a [Nincs megfelelő infrastruktúra] és az [Ismerethiány] kategóriákhoz is. A használati esetek kibővítéséhez feltétlenül szükséges, hogy a technikai feltételek rendelkezésre álljanak, valamint az is, hogy az állampolgárok tisztában legyenek a lehetőségeikkel.

Kapcsolódik a [Könnyebbé kellene tenni a használatát] kategória is: az infrastruktúra hiányosságait [Mobilalkalmazás]-sal és [Ingyenes kártyaolvasó]-val javítanák az interjúalanyok. A [Mobilalkalmazás] használatát hasonlóan képzelnék el, mint a mobiltelefonos fizetést: az állampolgár mobiltelefonja teljesen felcserélhető módon használható lenne az eSzemélyi helyett hitelesítésre és elektronikus aláírásra egyaránt.

A kártyaolvasó készülék teljes egészében kiváltható egy okostelefon és az eSzemélyiM alkalmazás segítségével. Az [Ingyenes kártyaolvasó]-t csak azon állampolgárok számára lenne érdemes biztosítani, akik ezt külön igénylik.

A beszélgetések során felmerült egy olyan állami [Felhőszolgáltatás] létjogosultsága, amely – a tarhely.gov.hu megoldáshoz hasonló módon – tárolná és elérhetővé tenné az érintett felek számára az aláírásra szánt, vagy korábban aláírt dokumentumokat. Itt megjelent az interperszonális bizalom hiánya és az igény intézményi bizalomra: hajlandóbbak lennének használni a technológiát, ha lenne egy olyan intézményi megoldás, amely segít az elektronikus aláírások használatának nyomon követésében.

Egyik szolgáltatása lehetne, hogy egy aláírásra váró dokumentumhoz kapcsolódóan meg lehessen jelölni az aláíró személyeket, majd az elektronikus aláírásokat be is gyűjthetné az érintett felektől. További szolgáltatása a korábban aláírt dokumentumok kereshető módon történő nyilvántartása lehetne.

Az [Ismerethiány] csökkentésére is hangoztak el javaslatok a beszélgetések során. [Népszerűsíteni kellene az eSzemélyit és az elektronikus aláírást], ezt pedig többféleképpen is elképzelhetőnek tartották a megkérdezettek.

A népszerűsítést már a Kormányablakban az ügyintézők is megkezdhetnék. Hasznos lenne, ha az eSzemélyi okmány kézhezvételét követően az ügyintézők felügyelete és segítségnyújtása mellett egy első próbát tehetnének ([Veszélytelen próbálkozás]) az elektronikus aláírás használatára.

A legtöbbször elhangzott javaslat az intenzív [Reklámkampány] volt, amelyet az év különböző szakaszaiban két-három héten keresztül TV, rádió és „Youtube" reklámok keretében lehetne kivitelezni. A javaslatok szerint olyan reklámokra lenne szükség, melyek kihangsúlyozzák az eSzemélyi és az elektronikus aláírás használatának előnyeit, amelyekből látszana, hogy a mindennapi életben milyen helyzetben és hogyan hasznos az eSzemélyi.

Ahogyan azt korábban is említettem, a megkérdezett hiányolták a [Tájékoztató anyagok]-at, ilyen anyagok azonban rendelkezésre állnak, csak sajnálatos módon ezeket nem ismerték. A fent említett [Reklámkampány] ezekre is kitérhetne.

Ehhez kapcsolódik a [Filmek] kategória: a reklámokhoz hasonlóan a magyar mozifilmekben és sorozatokban is megjeleníthetők lennének az eSzemélyi előnyei. A szereplők a cselekmény során az eSzemélyit „használva" észrevétlen módon ösztönözhetnék a nézőket.

Felmerült az eSzemélyi és az elektronikus aláírás használatának kötelezővé tétele is ([Kötelezés]) ez azonban sok problémát felvetne (infrastruktúra igény, állampolgárok ellenérzése stb.)

A [Kötelezés] mellett felmerült az is, hogy magyarországi szolgáltatók/szálláshelyek stb. biztosíthatnának kedvezményt az eSzemélyi használatáért cserébe ([Kedvezmény használat esetén]) annak érdekében, hogy az állampolgárok motiváltabbak legyenek. Ez a megoldás többek számára valószínűleg sokkal vonzóbb alternatíva lenne. Ide kapcsolódik az [Összevonás más okmányokkal] kategória is, ezen a ponton merült fel ugyanis a SZÉP kártyával történő összevonás.

Az [Alapszintű ismeretek hiánya]-t [Oktatás]-sal lehetne orvosolni. A beszélgetések alapján ez középiskolai és felsőoktatási szintre bontható tovább. Középiskolai szinten meg lehetni alapozni az eSzemélyivel és az elektronikus aláírással kapcsolatos felhasználói szintű ismeretanyagot a választott szaktól függetlenül, például az osztályfőnöki órák keretében.

A felsőoktatásban résztvevők számára szaktól függetlenül, de kreditpontért cserébe létre lehetne hozni egy olyan tantárgyat, amely gyakorlati szempontból mutatná be a magyar közigazgatás rendszerét (az állami szervek rendszere, az állampolgárok lehetőségei, az ügykörök, az ügytípusok stb.)

ÖSSZEFOGLALÁS

Amint az a fentiekből látszik Magyarországon elsősorban nem a bizalom hiánya a legfőbb akadálya az elektronikus aláírás terjedésének. Megjelenik ugyan gátló tényezőként, de az alapvető problémát az okozza, hogy az állampolgárok nincsenek tisztában az eSzemélyi és az elektronikus aláírásban rejlő lehetőségekkel.

Az infrastruktúrafejlesztés megkerülhetetlen előfeltétele a technológia térhódításának, önmagában azonban még ez is kevés. Oktatással, az elektronikus aláírást népszerűsítő kampányokkal az állampolgárokat olyan tudásszintre kell hozni, mely birtokában magabiztosan aknázhatják ki az eSzemélyi nyújtotta előnyöket.

KÖSZÖNETNYILVÁNÍTÁS

Először is szeretném megköszönni Dr. Kelemen-Erdős Anikó tanárnőnek, az Óbudai Egyetem Keleti Károly Gazdasági Kar egyetemi docensének a cikk megírásához nyújtott hathatós módszertani segítségnyújtásért és iránymutatásért!

Továbbá, ezúton is szeretnék köszönetet mondani a fókuszcsoportos beszélgetések résztvevőinek azért, hogy hajlandók voltak értékes idejükből a kutatási témámra is áldozni! Köszönöm továbbá konstruktív és nyílt hozzáállásukat, valamint azt, hogy véleményeikkel, ötleteikkel hozzájárultak jelen cikk elkészüléséhez!

FELHASZNÁLT IRODALOM

[1] The European Parliament and The Council of The Euroepean Union, „REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Official Journal of the European Union, 23 07 2014.

[2] Belügyminisztérium, „eSzemélyi - Miért hasznos az eSzemélyi," [Online]. Available: https://eszemelyi.hu/az-eszemelyi/#miert-hasznos-az-eszemelyi. [Hozzáférés dátuma: 14 03 2022].

[3] Belügyminisztérium, „eSzemélyi - Szolgáltatások," [Online]. Available: https://eszemelyi.hu/szolgaltatasok/. [Hozzáférés dátuma: 14 03 2022].

[4] N. Jogszabálytár, „414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól," 01 01 2022. [Online]. Available: https://njt.hu/jogszabaly/2015-414-20-22. [Hozzáférés dátuma: 19 03 2022].

[5] SimpLEGAL, „Elektronikus aláírás magyarországon - gyakorlati útmutató," 11 12 2020. [Online]. Available: https://simplegal.hu/wp-content/uploads/2020/12/Elektronikus-alairas-Magyarorszagon_Riport-2020.pdf. [Hozzáférés dátuma: 19 03 2022].

[6] A. Gelei és I. Dobos, „Bizalom az üzleti kapcsolatokban - A didaktikus adatelemzés egy alkalmazása," Közgazdasági szemle, kötet: 63, szám: 3, pp. 330-349, 2016.

[7] R. C. Mayer, J. H. Davis és F. D. Schoorman, „An Integrative Model of Organizational Trust," Academy of Management Review, kötet: 20, szám: 3, pp. 709-734, 1995.

[8] F. Fukuyama, Bizalom - A társadalmi erények és a jólét megteremtése, Budapest: Európa Könyvkiadó, 2007.

[9] D. H. McKnight és N. L. Chervany, „Trust and Distrust Definitions: One Bite at a Time," in R. Falcone, M. Singh, and Y.-H. Tan (Eds.): Trust in Cyber-societies, LNAI 2246, 2001, pp. 27-54.

[10] P. M. Erdősi, Az elektronikus aláírás mérése, Budapest: NEMZETI KÖZSZOLGÁLATI EGYETEM Közigazgatás-tudományi Doktori Iskola, 2019.
[11] K. D. Paine, Guidelines for Measuring Trust in Organizations, The institute for public relations, 2003.
[12] T. Lynn, Data privacy and trust in cloud computing : building trust in the cloud through assurance and accountability, Palgrave Macmillan: Cham, Switzerland, 2021.
[13] M. Aranyossy és B. A. Magisztrák, „A vásárlói bizalom hatása az e-kereskedelmi vásárlási hajlandóságra (Magyar-lengyel összehasonlító vizsgálat),” Marketing & Menedzsment, kötet: 50, szám: 3-4, pp. 73-87, 2016.
[14] J. B. Thatcher, M. Carter, X. Li és G. Rong, „A Classification and Investigation of Trustees in B-to-C e-Commerce: General vs. Specific Trust,” Communications of the Association for Information Systems, kötet: 32, szám: 4, pp. 107-134, 2012.
[15] S. Mason és A. Stanfield, „Authenticating electronic evidence,” in Electronic Evidence, London, University of London Press: Institute of Advanced Legal Studies, 2017, p. 193..
[16] K. Szivós, „Az elektronikus okiratok dogmatikai alapjai és szabályozási környezetük,” in Innovatív magánjogi megoldások a társadalmi-gazdasági haladás szolgálatában, Miskolc, Magánjogot Oktatók Egyesülete, 2020, pp. 20-25.
[17] P. Kiss, „Az elektronikus aláírás,” GIKOF Journal, kötet: 2, szám: 3, pp. 60-69, 2003.
[18] Belügyminisztérium - Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság, „Elektronikus közszolgáltatásokat összefoglaló monitoring jelentés,” [Online]. Available: https://nyilvantarto.hu/letoltes/statisztikak/2021_I_feleves_adatokat_tartalmazo_monitoring_jelentes.pdf. [Hozzáférés dátuma: 14 03 2022].
[19] Belügyminisztérium - Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság, „eSzemélyi igénylések megoszlása az okmányon lévő adatok alapján - 2020.,” [Online]. Available: https://nyilvantarto.hu/letoltes/statisztikak/eSZIG_statisztika_2020december.xlsx. [Hozzáférés dátuma: 14 03 2022].
[20] Belügyminisztérium - Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság, „eSzemélyi igénylések megoszlása az okmányon lévő adatok alapján - 2021. december,” [Online]. Available: https://nyilvantarto.hu/letoltes/statisztikak/eSZIG_statisztika_2021_december.xlsx. [Hozzáférés dátuma: 14 03 2022].
[21] Belügyminisztérium - Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság, „eSzemélyi statisztika - 2022 február,” [Online]. Available: https://nyilvantarto.hu/letoltes/statisztikak/eSzemelyi_statisztika2022_februar.xlsx. [Hozzáférés dátuma: 14 03 2022].
[22] Lorelli S. Nowell, Jill M. Norris, Deborah E. White, and Nancy J. Moules, „Thematic Analysis: Striving to Meet the Trustworthiness Criteria,” International Journal of Qualitative Methods, kötet: 16, pp. 1-13, 2017.
[23] M. Sandelowski, „Using qualitative research,” Qualitative Health Research, kötet: 14, pp. 1366-1386, 2004.
[24] N. K. Malhotra, Marketingkutatás, Budapest: KJK-KERSZÖV Jogi és Üzleti Kiadó, 2002.
[25] E. Neumann-Bódi, T. Gyulavári, A. Mitev, Á. Neulinger, J. Simon és K. Szűcs, A marketingkutatás alapjai, Budapest: Aula Kiadó, 2012.
[26] A. Kelemen-Erdős és A. Molnár, „Cooperation or Conlfict? The Nature of the Collaboration of Marketing and Sales Organizational Units,” Economics and Culture, kötet: 16, szám: 1, pp. 58-69, 2019.

[27] A. J. Onwuegbuzie, W. B. Dickinson, N. L. Leech és A. G. Zoran, „A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research," International Journal of Qualitative Methods, kötet: 8, szám: 3, pp. 1-21, 2009.
[28] A. Kelemen-Erdős, „Dead-end Development or Real Progress? Paradigm Shift Initiatives in Marketing Theory," International May Conference on Strategic Management, kötet: XV, szám: 1, pp. 26-38, 2019.
[29] A. Kelemen-Erdős és A. Mitev, „Holisztikus szolgáltatásélmény - vendég-utazás és kölcsönös értékteremtés dimenziói az art- és romkocsmák példáján," Marketing & menedzsment, kötet: 50, szám: 3-4, pp. 88-101, 2016.
[30] Delve, „How To Do Open, Axial and Selective Coding in Grounded Theory," [Online]. Available: https://delvetool.com/blog/openaxialselective. [Hozzáférés dátuma: 04 06 2022].

PERFORMANCE OPTIMIZATION AND SYSTEM MONITORING OF SMALL AND MEDIUM-SIZED SOLAR POWER PLANTS

KIS- ÉS KÖZEPES MÉRETŰ NAPELEMES ERŐMŰVEK TELJESÍTMÉNYOPTIMALIZÁLÁSA ÉS RENDSZERFELÜGYELETE

BOZSIK Nándor[1]

Abstract

Solar energy will be one of the cornerstones of sustainable development and energy supply in the future. As more and more solar systems are built and connected to the utility grid, there will be an increasing need to monitor these systems. System monitoring tools are used to optimize electricity performance and maintain grid stability based on real-time generation data from solar systems. One of the most useful and spectacular elements of modern solar systems is the remote monitoring of online systems. This allows the operation of the solar system to be monitored. You can check the present and past data via the Internet, either with a smartphone or any Internet-connected device. This study shows, among other things, how system management helps the efficient and safe operation of solar systems.

Keywords

solar panel, renewable, system management, inverter, optimizer, smart meter

Absztrakt

A napenergia a jövőben a fenntartható fejlődés és az energiaellátás egyik alappillére lesz. Ahogy egyre több napelemes rendszer épül és csatlakozik a közüzemi villamosenergia-hálózatba, egyre nagyobb a szükség lesz ezeknek a rendszereknek a felügyeletére. A rendszerfelügyeleti eszközök a napelemes rendszerekből származó valós idejű termelési adatok alapján a villamosenergia teljesítményének optimalizálását és a hálózat stabilitásának megőrzését szolgálják. Sokak számára ismert a korszerű napelemes rendszerek egyik hasznos és látványos eleme az online rendszerfelügyelet, a távoli monitoring. Ennek segítségével nyomon követhető a napelemes rendszer működése. Ellenőrizhető a jelen- és a múltbéli adatok az interneten keresztül, akár egy okostelefon vagy bármely internethez kapcsolódó eszköz segítségével. Ez a tanulmány többek közt azt mutatja be, hogyan segíti a rendszerfelügyelet a napelemes rendszerek hatékony és biztonságos működését.

Kulcsszavak

napelem, megújuló, rendszerfelügyelet, inverter, optimalizáló, okosmérő

[1] bozsik.nandor@uni-obuda.hu | ORCID: 0000-0002-6798-3844 | PhD Student, Óbuda University Doctoral School on Safety and Security Science | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A Föld népessége folyamatosan növekszik, ami együtt jár az energiafogyasztás jelentősen emelkedésével. Az energiahatékonyság javulása ugyan mérsékeli a fokozódó energiakeresletet, viszont a megújuló energiaforrások növekvő felhasználása kulcsfontosságúvá vált a fosszilis energia részleges kiváltására. A megújuló energia felhasználása felértékelődik, még akkor is ha sokszor kisebb mennyiségben, elszórtan áll rendelkezésre, a termelése nem szabályozható eloszlású vagy erősen függ az időjárás alakulásától. [1] A megújuló energiaforrások hasznosítása az EU klíma- és energiapolitikájában is egyre nagyobb jelentőséggel bír. A megújuló energiahasználat növelését indokolja az importált fosszilis energiafüggőség csökkentése, illetve az energia szektor káros környezeti hatásainak mérséklése. Így van ez Magyarországon is, ahol a megújuló energiaforrások kutatása több évtizedre tekint vissza. [2] [3]

Az utóbbi évtizedben a napelemes rendszerek elterjedése jelentősen hozzájárult nemcsak a fogyasztók önellátásához, hanem az ország decentralizált villamosenergia-termeléshez is. A háztartási napelemes kiserőművek 2015-ben 504 TJ, 2020-ban már 4291 TJ villamosenergiát állítottak elő, ez 8,5-szeres növekedést jelentett öt év alatt. A 2015-ös 0,4%-os részarányuk 2020-ra 7,13%-ra nőtt az összes megújuló energiákból. [4] Ezalatt folyamatosan fejlődött a napelemes rendszerekhez kapcsolódó technológia is. Ezeknek az elektronikájának (főleg az inverter és a teljesítményoptimalizáló) szállítása a becslések szerint 2020-ban 113 GW villamos teljesítmény volt világszerte. [5] A gyártói rangsor alapján 2020-ban a Huawei volt a legnagyobb napelem inverter szállító világszerte, a piaci részesedése közel 23 százalék volt. A Huaweit a Sungrow Power Supply és az SMA követte a második, illetve a harmadik helyen a szállítók sorában. A Herfindahl-Hirschman-index az inverter gyártók adatsorából számítva 0,12 értéket ad, ami alapján az inverter piac alacsony koncentrációs besorolású, egyik gyártó sincsen monopolhelyzetben.[6] [7]

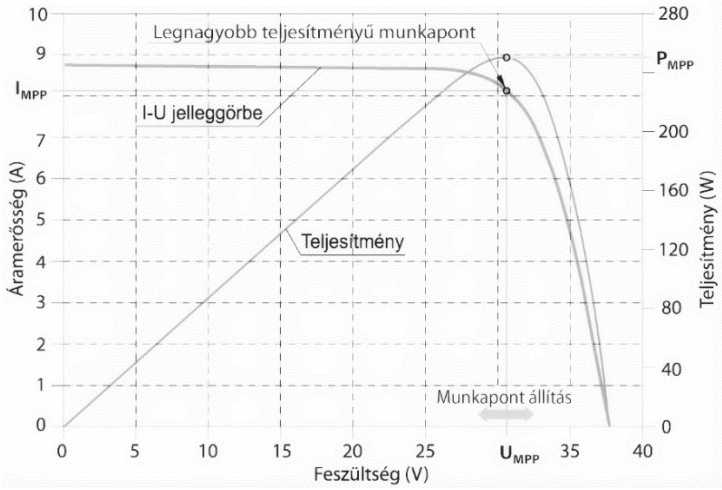
Az inverter és gyakran a vele együttesen alkalmazott teljesítményoptimalizáló kiválasztása a napelemes rendszerek tervezésének egyik legfontosabb eleme. Az inverter legfőbb feladata a napelem táblák által termelt egyenáramot a hálózatnak megfelelő feszültségű és frekvenciájú váltakozóárammá alakítsa át. Későbbiekben szó lesz róla, hogy ezek az inverterek több funkcióval is rendelkeznek, optimalizálják az áramtermelést, biztonsági feladatokat látnak el, adatgyűjtést és távfelügyeletet biztosítanak. Egyes típusai a saját fogyasztók berendezéseit is vezérelni tudják. Ezek képesek együttműködni okosmérőkkel és távoli rendszerfelügyeleti eszközökkel, azokat informálni és az onnan érkező utasításokat végrehajtani. Az inverterek mellet gyakori rendszerelem a teljesítményoptimalizáló. Ennek feladata a napelem panelek közötti teljesítmény különbségek kiegyensúlyozása, illetve az üzemeltetés során fellépő hibák, zavarok kezelése. A termelést zavaró leggyakoribb jelenség az árnyékolás okozta teljesítményvesztés, ill. egy-egy napelem modul meghibásodása. Ezeket a teljesítmény kieséseket az optimalizálók a napelem modulok szintjén kezelik, a többi modulra való hatás nélkül. Az inverter és az optimalizáló együttműködését a közöttük lévő adatkapcsolat segíti, amely így nagyobb hatásfokú rendszert eredményez. [8]

INVERTEREK

A napelemes inverterek – de igaz ez más megújuló energiatermelésben használt inverterre is – a napelem által megtermelt egyenáramot alakítják át váltakozó árammá. Az

inverter alapvető működésének megértéséhez először a napelem működését kell megérteni. A napelem áramköri szempontból, úgy működik, mint egy áramgenerátor, ami a teljesítménykorlát eléréséig tartja a közel állandó áramerősséget, miközben a feszültségérték változik és csak a teljesítmény korlát elérése után „törik le" az áramgörbéje (1. ábra). (Megjegyzendő, hogy ennek úgymond „ellenkezője" a feszültséggenerátor, ott teljesítménykorlát eléréséig tartja a feszültségértéket miközben az áramerősség változik.) Az előbbi tulajdonság hátterében a napelemek félvezető technológiája áll. A napelemek, ha sorba kötjük őket, akkor a feszültségük, ha párhuzamosan, akkor az áramerősségük adódik össze. [9]

Az inverter elektronikájának másik fő feladata a munkapont állítás, követés (MPPT, Max Power Point Tracking). Az MPPT valamilyen algoritmussal keresi meg az U-I görbén azt a munkapontot, ahol a feszültség-áram szorzata maximális (1. ábra). Ezt szokták úgy is szemléltetni, hogy keresik azt a legnagyobb területű téglalapot, ami az I-U görbe alatt szerkeszthető meg úgy, hogy a téglalap két szemközti csúcsa közül az egyik az origóban a másik az I-U görbén van, ez utóbbit nevezik a legnagyobb teljesítményű munkapontnak. A téglalap területe arányos a napelem teljesítményével, az oldalak I_{MPP} (maximális teljesítményhez tartozó áram) és U_{MPP} (maximális teljesítményhez tartozó feszültség) a szorzatuk pedig P_{MPP} (maximális teljesítmény).

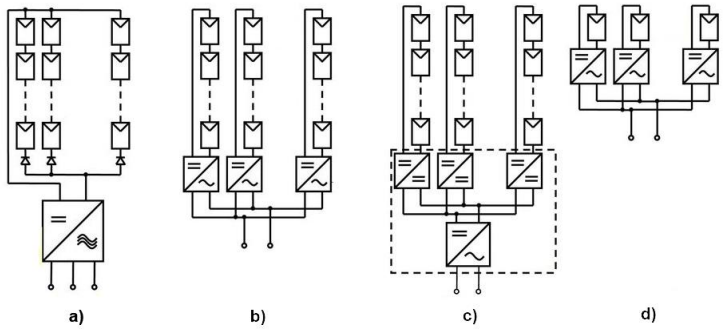


1. ábra I-U, P-U diagram, [10] alapján saját szerkesztés

A napelemek félvezető tulajdonságai miatt a leadott teljesítményük nem csak a (megfelelő hullámhosszúságú) napfény intenzitásának függvénye, hanem erősen függ a cellák hőmérsékletétől is. A cellák hőmérsékletének növekedésével csökken a napelem hatásfoka.

A rendszer kapcsolási topológiai

A napelem modulok és az inverter(ek) kapcsolata sokféle struktúrájú lehet. Ez függ a rendszer méretétől, üzemeltetés céljától, környezettől, földrajzi adottságoktól stb.. A 2. ábrán a leggyakoribb topológiák láthatók.



2. ábra Inverter topológiák, [11] alapján saját szerkesztés

A központi inverterek (2.a ábra) esetén a napelemek sorba (sztring), majd ezek párhuzamosan vannak kötve, annak függvényében, hogy az inverter milyen feszültség ill. áramtartományban üzemelnek optimálisan. A sorba kötött napelemek száma az inverter bemeneti feszültségtartományát, míg a párhuzamosan kapcsolt sztringek száma az inverter bemeneti áramtartományát határozzák meg. Az ilyen struktúrájú kapcsolásoknál azonos típusú és teljesítményű napelemeket használnak, a sztringeken belül a napelemek száma megegyezik.

A sztringinverterek (2.b ábra) esetén minden egyes sztring saját inverterrel rendelkezik, majd ezek kimenetei csatlakoznak egy közös gyűjtő váltakozó áramú sínre (AC sín).

A multisztring-inverterek (2.c ábra) az egyes sztringek, egy-egy DC-DC konverteren keresztül csatlakoznak egy közös egyenáramú gyűjtő sínre (DC sín), ami pedig az inverter bemenetére csatlakozik.

A mikroinverterek (2.d ábra) olyan DC-AC konverterek, amelyek minden egyes napelem maximális teljesítményének meghatározása mellett alakítják át az egyenáramot váltóárammá, tulajdonképpen a napelem panelnek saját „mini invertere” van. [12]

A teljesítményoptimalizálók (Power Optimizers) a mikroinverterek alá tartoznak viszont azoknál költséghatékonyabbak. Az optimalizálók alkalmazásakor a napelemenkénti munkapont-meghatározás és a DC-AC átalakítás külön történik. Az optimalizálók esetében minden egyes napelemen egy elektronikus egység van, amely a mérést és a beavatkozást végzi, ezek állítják be a munkapontot. A vezérlés és a DC-AC átalakítás a központi inverterben történik. Mivel a munkapont keresés napelemenként történik, így az inverter egyszerűbb kialakítású, olcsóbb és megbízhatóbb. Az optimalizáló és az inverter közötti kommunikáció a DC kábeleken történik, így nincs járulékos vezeték kiépítésre szükség. [8] [12]

Előnyök, hátrányok

A központi inverterek abszolút előnye a relatíve alacsony költség, viszont cserébe megköveteli azonos teljesítményű, tájolású és dőlésszögű napelem panelek használatát. Az árnyékolást rosszul tűri, minden esetben kerülendő.

A sztring inverterek alkalmazása akkor költséghatékony, hogy ha az egyes sztringek árnyék mentesek és minden modulja azonos tájolású és dőlésszögű. A hátránya éppen ebből fakad. Egy sztring akár csak egy lánc csak annyira erős, amennyire a leggyengébb

láncszeme. Amennyiben egy panel teljesítménye csökken, az kihat az egész sztringre. Ennek legfőbb okai az árnyékolás, sztringen belüli különböző tájolás és valamely panel meghibásodása. [8]

Az előbb már volt utalása rá, hogy a mikroinverterek lényegében egy önálló, egypaneles napelemes rendszerek. Az önállóságból adódik, hogy panelek bármilyen konfigurációba vagy tájolásba szervezhetők. A rendszer semmilyen téren nem kötött, bármikor könnyen bővíthető. Lehetővé teszik a panelszintű rendszerfelügyeletet. Előnye még a minimális egyenáramú kábelezés és védelem, a panelektől indulva az egész rendszer váltakozóáramú. Ennek egyik oka, hogy az egyenáramú kábelezés drágább, mint az váltakozóáramú. A másik oka pedig, hogy az egyenáramú védelem bonyolultabb, mivel az egyenáram esetén nincs nullátmenet így az ívoltás nehézkesebb a váltakozóáramhoz képest. Hátránya, hogy a mikroinverterek a legdrágább megoldások a wattonkénti költség alapján. Nagyobb méretű rendszereknél, a sztring inverterek (optimalizálóval vagy anélkül) költséghatékonyabbak, mint a mikroinverteres rendszerek. [12]

A teljesítményoptimalizálók esetén a munkapontkeresés (MPPT) modulonként történik, így az inverter egyszerűbb szerkezetű lehet, csak a DC/AC átalakítás a feladata. Használatával az árnyékolás miatt fellépő különbségek nem csökkentik az egész rendszer teljesítményét, így olyan helyekre is kerülhetnek napelemek, ahol korábban nem volt érdemes. Ezért ezek a berendezések megbízhatóbbak és a költségek is kisebbek. Az optimalizáló egységek az inverteren keresztül külön-külön adatkapcsolatban vannak az adatgyűjtő rendszerrel, így modul szintű rendszerfelügyeletet lehet megvalósítani. Az adatátvitel a DC kábeleken keresztül történik, tehát plusz vezetékek kiépítésére nincs szükség. A hátrányt itt is - mint a mikroinverternél - a magasabb kiépítési költség jelenti a sztring inverterekhez képest. [13]

Előnyök és hátrányok általában: a sztring inverterek a legelterjedtebb és legkedvezőbb árú inverterek. Ezek akkor működnek a leghatékonyabban, ha az azonos tájolású napelemeket árnyékolás mentesen sok napfény éri. A mikroinverterek és a teljesítmény-optimalizálók használata pedig ott javasolt, ahol az előbbiek felsoroltak nem biztosíthatók, tehát részben árnyékos, ill. különböző tájolású napelemekből áll a rendszer. [13]

RENDSZERFELÜGYLET

A napelemes rendszerek hatékony rendszerfelügyeletéhez, szükség van a rendszer és a környezeti változók értékeire és ezek eljuttatására a feldolgozó egységekhez, amik lehetnek az inverterek, a központi egységek vagy a hálózati vezérlők. Ezek az adatok a rendszer feladatától, méretétől függően az alábbi paraméterek:

- feszültség (V),
- áram (A),
- hőmérséklet (K) inverter és napelem,
- teljesítmények mind a hatásos, és meddő teljesítmény (W; var),
- villamos fogyasztás, energia (kWh),
- berendezés aktuális és archívált adatai,
- több napelemes eszköz kezelése és összehasonlítása,
- automatikus üzenet küldése a berendezés hibái esetén,
- automatikusan generált jelentések;

Környezeti paraméterek:

- napsugárzás közvetlen, közvetett és talajról visszavert érték,
- levegő hőmérséklet,
- szélirány és erősség,
- páratartalom,
- tájolás és dőlésszög,
- árnyékolás, domborzat.

Internet of Things

Ezeknek a paramétereknek a mérését sok esetben IoT-szenzorokkal (internet of things, dolgok internete) oldják meg. Az elnevezés többet takar, mint csupán szenzort. Ezek az IoT-k egy eszközben tartalmazzák az érzékelőt, a jelátalakítót és az adatok továbbításához szükséges kommunikációs adaptert. A jelátalakítók legtöbbször analóg-digitális átalakítók, mert a mért fizikai jellemző analóg folyamatos jel, míg a továbbításhoz mintavételezett, diszkrét (digitális) jelre van szükség.

Általánosságban az IoT-k hálózatba kötött elektronikai eszközök sokasága, amelyek egyedi azonosítóval rendelkeznek, így egyértelműen beazonosíthatók. Az egyik a fő feladatuk valamilyen fizikai jellemző mérése, feldolgozása és továbbítása a rendelkezésre álló kommunikációs csatornán. A másik fő szerepük a végrehajtás (kapcsolás, szelep vezérlés, stb.) Az előbbieket szokás szenzoroknak az utóbbiakat beavatkozóknak nevezni. [14] Előfordul még az „intelligens eszköz” elnevezés is. Az IoT elterjedésének köszönhetően 2021-ben, több mint 10 milliárd aktív IoT eszköz volt a világon. Ez a szám becslések szerint 2030-ra eléri a 25,4 milliárdot. Az IoT-eszközök által generált adatmennyiség, pedig várhatóan 2025-re eléri a 73,1 ZB-t (zettabájt). [15]

Kommunikáció

Az IoT-k által gyakran használt adatátviteli rendszer az alacsony energiafogyasztású, nagy kiterjedésű kommunikációs hálózatok, az LPWAN-ok. Ezek a nagy területet lefoglaló kommunikációs hálózatok alapjába véve abban különböznek a „klasszikus” mobilhálózatoktól, hogy bár kicsi az adatátviteli kapacitásuk cserébe viszont alacsony az energia igényük. Az alacsony energiafelvételnek köszönhetően egy elem élettartama elérheti a 10-15 évet használattól függően, ebből adódik az alacsony karbantartási költség is. Az LPWAN-oknak főleg a környezeti szenzorok adatkapcsolatánál van nagy szerepe. Ezek a hálózatok képesek több száz vagy ezer szenzor adatait megbízhatóan, vezeték nélkül továbbítani a központi inverterbe, hálózatfelügyeleti rendszerbe. Az LPWAN-on belül a két legelterjedtebb adatkommunikáció, a LoRa és a NB-IoT. A kettő között a legnagyobb különbség, hogy a LoRa szabadon szervezhető és nyílt licence, addig a NB-IoT celluláris (mobilkommunikációs cellákhoz kötött), licencelt technológia. [16]

A napelemes rendszerek inverterei beállított időközönként mérik és regisztrálják (mintavételezik) a rendszer energiahozamát. A pillanatnyi, ill. az összesített adatokat az inverter rendszeresen elküldi az üzemeltetőnek, kivitelezőnek. Ezek az adatok a készülék kijelzőjéről vagy az internetről is hozzáférhetők (megfelelő jogosultság mellett) a tulajdonos számára. Ez az egyik módja annak, egy beállítási probléma, vagy esetleges hiba miatt be-

következő hozamveszteség, vagy időszakos be nem tervezett leállás kiderüljön. Az inverterek különböző kommunikációs modullal rendelkeznek, a leggyakoribbak a WLAN (IEEE 802.11 szabvány, közismert néven wifi), a GSM-modul vagy a LAN. A helyszíni szervizeléshez, pedig RS-232, RS-485 vagy USB porttal rendelkeznek. [17]

A rendszerfelügyelet a telepítőnek is ugyanúgy hasznos, mint a tulajdonosnak, hiszen a hibákról azonnal hibaüzenetet kap. A hiba sokszor csak szoftveres beavatkozást igényel így a módosítás, javítás legtöbbször távolról is elvégezhető, így jelentős költség és idő takarítható meg.

Inverter szintű monitoring

A gyártók webszervereket tartanak fenn, ahol a rendszer fontosabb működési adatai folyamatosan nyomon követhetők a pillanatnyi teljesítmény és az aktuális, napi, havi, éves energiahozam. Ugyanitt kalkuláció van a megtakarított CO2 kibocsátásról is. Az archívum megjeleníthető diagram formátumban is, itt célszerű kWh/kWh fajlagos energiahozam kijelzést ellenőrizni, ahol viszonyítási alapként érdemes ellenőrizni, hogy a magyarországi viszonyok között 1 kWp névleges teljesítményű napelem 1-1,2 MWh éves energiahozamot produkál. (A kWp vagy kilowattpeak a napelem standard körülmények között mért csúcsteljesítménye, valóságban ritkán teljesül, összehasonlítás végett adják meg a gyártók.) Ettől eltérő értéknél érdemes megkeresni a hozamveszteség okát, amely legtöbbször árnyékolásból fakad. Eltérés esetén több nap görbéjét összehasonlítva beazonosítható az árnyék forrása, amit legtöbbször a fejlődő fák okoznak vagy időközben épített, felszerelt árnyékot okozó kémény, antenna, stb.. [10]

Napelemszintű monitoring

Az inverterszintű monitoring jobb esetben is csak az egy sztringre kapcsolt napelemek együttes termelési adatait képes megjeleníteni. Addig a napelemszintű monitoring minden egyes napelem energiahozamát és teljesítményét képes külön-külön kezelni. A valamilyen okból teljesítmény csökkenést mutató napelem modulok azonnal feltárhatók, így nem marad észrevétlen egyetlen egy elszennyeződött, sérült, stb, napelem modul sem. Az ilyen monitoring rendszerek nagy előnye a séma megjelenítés, ahol is fizikailag is jól behatárolhatók a rendellenesen működő rendszerelemek, képesek megmutatni a „gyengén teljesítő" paneleket. A jobb szemléltetés végett színárnyalatok mutatják az egyes napelem panelek adott időszakra számított energiahozamát, a hozamok számszerűen is hozzá vannak rendelve a panelekhez. [10]

OKOSMÉRŐK

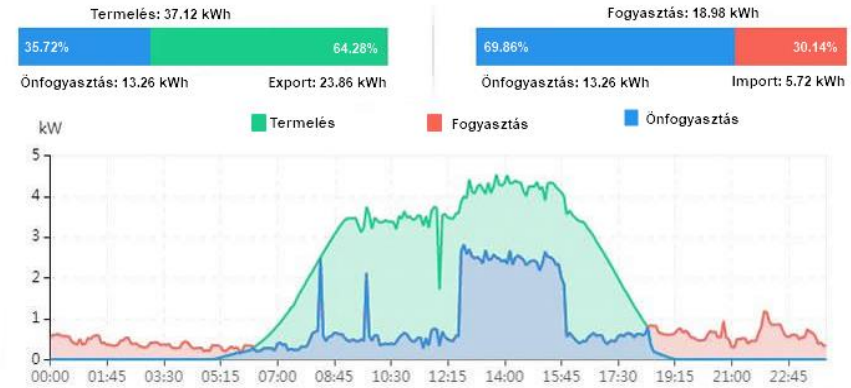
A napelemes rendszerek villamosenergia-termelése sokban függ a panelek dőlésszögétől és tájolásától, az időjárástól, valamint az árnyékhatásoktól. Eközben maga az épület sem fogyaszt egyenletesen villamosenergiát. Ezek nyomon követésére, felügyeletére alkalmas berendezés az okosmérő, más néven Smart Meter. A segítségével ellenőrizhető, hogy a termelésünk mikor fedezi a fogyasztásunkat, ill. mikor szükséges ezen felül a hálózatból vételezni a hiányzó energiát. Ellenőrizhető az is, amikor túltermelésünk van és azt betápláljuk a villamos hálózatba. Már a napelemes rendszer tervezésénél az egyik fő szempont a fogyasztás ismerete, törekedni kell a lehető legjobb termelés-fogyasztás egyensúlyára. Az okosmérő fontos tulajdonsága még, hogy képes az akkumulátor töltés-kisütését

vezérelni az inverteren keresztül. A háromfázisú rendszereknél a különböző terhelések okán a fázisokat külön-külön méri. A méretét tekintve az okosmérő kicsi, nem igényel sok időt, sem a szerelése, sem az installálása.

Rendszerfelügyelet és fogyasztás-tervezés okos fogyasztásmérővel

A Smart Meter segít megismerni fogyasztásunk dinamikáját és ennek ismeretében kialakítani annak leghatékonyabb profilját (3. ábra). A Smart Meter monitorozó egységgel nyomon követhető:

- a napelemes rendszer által megtermelt villamosenergia kWh-ban,
- az ebből azonnal, a házon belül elfogyasztott villamosenergia kWh-ban,
- az áramszolgáltatói hálózatból vételezett villamosenergia kWh-ban,
- az áramszolgáltatói hálózatba termelt villamosenergia kWh-ban
- amennyiben van akkumulátor, akkor a töltés/kisütés villamosenergia kWh-ban.



3. ábra Fogyasztás-termelés görbe, [18]

A grafikon alapján manuálisan beállítva vagy program segítségével automatizálva érdemes a nagy teljesítmény igényű elektromos készülékeinket – klíma, bojler, elektromos autó töltés, stb. – használni, ilyenkor ugyanis a napelemes rendszer által termelt villamosenergia helyben történik felhasználásra, nem vagy csak minimális fölösleg kerül betáplálásra a hálózatba (3. ábra). Akkumulátor megléte esetén ez a fölösleg töltésre is kerülhet, ezzel a tranzit mentes megoldással az amúgy is környezetbarát megújuló energiatermelésünk még inkább „zöldebb” lesz. [19]

A gyakorlatban a rendszer termelésének ismeretében tudjuk a különböző háztartási gépeket ki-be kapcsolni, hogy a lehető legnagyobb hányada legyen kihasználva a megtermelt villamosenergiának. Az ilyen fogyasztói hozzá állást segíti még, hogy anyagilag is érdekelté teszi a fogyasztót, ha az áram export-import árkülönbség nagy. A már említett akkumulátoros energia tárolás mindenképpen szükségessé teszi az okosmérő használatát, ez állítja be ugyanis a visszatöltési korlátokat (power export limitation control). [20]

ÖSSZEFOGLALÁS

A napelemes rendszerek magukkal hozták a rendszerfelügyelet és az intelligens-hálózatok technológiáját. Ezek az eszközök hozzájárultak a megújuló villamosenergia-termelés egy új és magasabb szintjéhez. A háztartások napelemes rendszereinél ezt a szerepet az inverterek és a teljesítményoptimalizálók töltik be. Ezek a technológiák gyakran kapcsolódnak az otthonok okos (smart home) rendszereihez. Az okosotthonok eszközei képesek beavatkozás nélkül egymással kommunikálni, adatot gyűjteni és ezeket továbbítani. Az eszközök közötti kommunikáció lehet mind vezetékes, mind pedig a vezeték nélküli a feladattól, elhelyezkedéstől függően. [21] A rendszerfelügyelet kétirányú kommunikációja lehetővé teszi, hogy a megtermelt villamosenergia a megfelelő fogyasztóhoz vagy tárolóhoz (akkumulátorhoz) kerüljön, illetve bizonyos feltételek teljesülése esetén a közüzemi villamos hálózatba kerüljenek betáplálásra. A felügyeleti rendszer képes a megújuló villamosenergia és a hálózati energia költséghatékony kezelésére, miközben figyelembe veszi a villamosenergia pillanatnyi tarfiáját, a háztartási gépek terhelési profilját és az akkumulátorok töltöttségi szintjét. [22]

Az rendszerfelügyeleti eszközök, inverterek, optimalizálók a folyamatos fejlesztéseknek köszönhetően egyre kompaktabbak, intelligensebbek lesznek, miközben áruk az általuk nyújtott szolgáltatásaikhoz képest arányaiban nem növekszik. Az elosztott villamosenergia-rendszer fejlődése is hozzájárul ezeknek az eszközöknek a fejlődéséhez. A napelemes rendszerek szerveződése is egyre elterjedtebb lesz. A hálózat felé egy termelőként lesznek képesek fellépni. Ezek hasonlóak a manapság ismert virtuális erőművekhez (virtual power plan, VPP). [23] Ehhez elengedhetetlen a rendszerfelügyeletek részéről az egymással kommunikálni képes korszerű inverterek, optimalizálók használata. A korszerű hálózati kommunikáció lehetővé teszi, hogy a hálózat bemeneteit, a napsugárzás mértékének és a közüzemi szolgáltató kilowattóra árainak megfelelően alakítsák, amelyek óráról órára változhatnak. Tulajdonképpen úgy működik, mint bármely piac, ahol az árak a kereslet-kínálat függvényében változnak. Ezek a költséghatékony megoldások a napelemes rendszerek – közvetve más megújulók – további fejlődéséhez járulnak hozzá. [24]

FELHASZNÁLT FORRÁSOK

[1] Bozsik, N. ”A kelet-közép európai országok energiafelhasználásának elemzése”, JOURNAL OF CENTRAL EUROPEAN GREEN INNOVATION 6 : 3 pp. 37-62. Paper: 2 , 26 p. 2018.

[2] Meyer, N., Magda, R., Bozsik, N. ”The role of renewable energies in the new EU member states”, JOURNAL OF EASTERN EUROPEAN AND CENTRAL ASIAN RESEARCH 8 : 1 pp. 18-25. , 8 p., 2021.

[3] Takács, I. ”A megújuló és nem megújuló energiahordozókra alapozott erőművi technológiák energiamegtérülési rátája és externáliái (CO2)”, TÉR-GAZDASÁG-EMBER, vol. 3, no. 1, pp. 91–106, 2015.

[4] Magyar Energetikai és Közmű-szabályozási Hivatal, http://mekh.hu/eves-adatok (letöltés időpontja: 2022.05.11.)

[5] M. Jaganmohan, ”Global solar PV inverter and optimizer shipments 2015-2025 (in megawatts, alternating current)”, Statista, https://www.statista.com/statistics/790664/solar-pv-inverter-and-optimizer-global-shipments/ (letöltés időpontja: 2022.05.21.)
[6] M. Jaganmohan, ”Global PV inverter market share by shipments 2020, based on shipments”, Statista, https://www.statista.com/statistics/1003705/global-pv-inverter-market-share-shipments/ (letöltés időpontja: 2022.05.21.)
[7] Uhrin, G., ”A verseny intenzitásának mérhetősége”, https://www.gvh.hu/data/cms1000455/Uhrin%20G%C3%A1bor.pdf (letöltés időpontja: 2022.05.11.)
[8] Naplopo.hu, SolarEdge napelemenkénti munkapont-optimalizálók alkalmazása, https://www.naplopo.hu/tudastar/szakcikkeink-hasznos-irasaink/334-solaredge-napelemenkenti-munkapont-optimalizalok-alkalmazasa (letöltés időpontja: 2022.04.21.)
[9] Budai Cs., Napelemes rendszerek érdekes kérdései, 2016, https://docplayer.hu/5538249-Napelemes-rendszerek-erdekes-kerdesei.html (letöltés időpontja: 2022.04.22.)
[10] Varga P., Napelemes rendszerek, 2016, https://docplayer.hu/44797118-Napelemes-rendszerek.html (letöltés időpontja: 2022.05.11.)
[11] S. Sadineni, J. Realmuto and R. Boehm ”An Integrated Performance Monitoring and Solar Tracking System for Utility Scale PV Plants”, American Society of Mechanical Engineers, Power Division (Publication) POWER. 2., 2011, doi: https://doi.org/10.1115/POWER2011-55243
[12] Boros V., Teljesítményoptimalizálás és más előnyök, A napelemek gyakorlati működéséről II., Villanyszerelők lapja 2015/9.
[13] UNBOUNDSolar: String Inverters vs. Micro-Inverters vs. Optimizers: Which Is the Best?, https://unboundsolar.com/blog/micro-inverters-vs-string-inverters (letöltés: 2022.04.22.)
[14] Demeter K., Losonci D., Nagy J., Horváth B., ”Tapasztalatok az ipar 4.0-val – egy esetalapú elemzés. ” Vezetéstudomány - Budapest Management Review, 50 (4). pp. 11-23. doi: https://doi.org/10.14267/VEZTUD.2019.04.02
[15] [1Jovanovic, B. Internet of Things statistics for 2022 - Taking Things Apart, DataProt, https://dataprot.net/statistics/iot-statistics/ (letöltés időpontja: 2022.04.22.)
[16] Ratliff, L. LORA Alliance - LPWAN Market Report – 2019 https://lora-alliance.org/wp-content/uploads/2020/11/ihsmarkit_berlin_2019_0.pdf (letöltés időpontja: 2022.03.11.)
[17] M. Belouda, A. Mami, ”Embedded solution for data acquisition and management strategy dedicated to a hybrid renewable energy source for remote electricity supply”, Microprocessors and Microsystems, Volume 90, ISSN 0141-9331, doi: https://doi.org/10.1016/j.micpro.2022.104496
[18] Huawei: Fusionsolar reporting – Update December 2020, https://www.solar4ever.com.au/Huawei_Fusionsolar.php (letöltés: 2022.04.21.)
[19] Solar KIT, https://solar-kit.hu/okos-fogyasztarmeres-napelemes-rendszerhez/ (letöltés: 2022.04.21.)

[20] N. A. Khafaf, A. A. Rezaei, A. M. Amani, M. Jalili, B. McGrath, L. Meegahapola, A. Vahidnia, ”Impact of battery storage on residential energy consumption: An Australian case study based on smart meter data”, Renewable Energy, Volume 182, 2022, Pages 390-400, ISSN 0960-1481, https://doi.org/10.1016/j.renene.2021.10.005
[21] MANDIĆ D., ”A mesterséges intelligencia alkalmazása az okos otthonokban”, Biztonságtudományi Szemle 2022. IV. 1. szám
[22] I. Fatih, O. Kaplan, ”The Determination of Load Profiles and Power Consumptions of Home Appliances Energies” 11, no. 3: 607. doi: https://doi.org/10.3390/en11030607
[23] Herédi M., Virtuális erőművek kivitelezése, működtetése, Energetikai Szakkollégium, 2017, https://www.eszk.org/attachments/l341/besz/VPP_beszamolo_eszk.pdf (letöltés időpontja: 2022.04.21.)
[24] G. Marsh, Partner in power: Part two: Whilst the micro-inverter revolution looks set to spread, central and string inverters remain the mainstream., Renewable Energy Focus, Volume 12, Issue 3, 2011, Pages 38-42, ISSN 1755-0084, doi: https://doi.org/10.1016/S1755-0084(11)70062-X

THE PAST, PRESENT AND FUTURE OF ARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF SENIOR AND JUNIOR EXPERTS (PART 2)

A MESTERSÉGES INTELLIGENCIA MÚLTJA, JELENE ÉS JÖVŐJE A SENIOR ÉS A JUNIOR SZAKÉRTŐK SZEMSZÖGÉBŐL (2. RÉSZ)[1, 2]

HEITLERNÉ LEHOCZKY Mária[3] – KOLLÁR Csaba[4]

Abstract

Our research focused on the current state and possible future of artificial intelligence and its impact on society. In the first part, we described the methodology of the focus group research, which was identical in both cases, and the results of the senior expert group, and in the second part, after a detailed analysis of the junior expert focus group research, we compared the opinions of the two groups by means of comparative analysis. Finally, based on our results, we formulate practical recommendations for realising a human-centred future based on ethical AI.

Keywords

artificial intelligence, expert survey, research methodology, online focus group, Artificial Intelligence Workshop

Absztrakt

Kutatásunk a mesterséges intelligencia jelenlegi helyzetének és lehetséges jövőképeinek áttekintésére, társadalmi hatásaira irányult. Az első részben ismertettük a fókuszcsoportos kutatás módszertanát, mely mindkét esetben azonos volt, és a senior szakértői csoport eredményeit, ennek folytatásaként a második részben a junior szakértői fókuszcsoportos kutatás részletes elemzése után a két csoport véleményét vetettük össze komparatív elemzéssel. Végül eredményeink alapján gyakorlati ajánlásokat fogalmaztunk meg a humánfókuszú, etikus mesterséges intelligenciára épülő jövő megvalósításához.

Kulcsszavak

mesterséges intelligencia, szakértői megkérdezés, kutatásmódszertan, online fókuszcsoport, Mesterséges Intelligencia Műhely

[1] A tanulmány kutatási hátterének alapját a 2021-1-HU01-KA220-HED-000029536 azonosítószámú „HEDY – Life in the AI Era” című Erasmus+ pályázatban a nevezett szerzők által végzett fókuszcsoportos szakértői megkérdezés jelentette.

[2] A tanulmány első része a Biztonságtudományi Szemle 2022. évi, IV. évf. 1. számában jelent meg: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/208/184

[3] maria.lehoczky@gmail.com | ORCID: 0000-0003-0588-715X | PhD student, Óbuda University Doctoral School for Safety and Security Sciences | member, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola | tag, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

[4] 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

A JUNIOR SZAKÉRTŐI CSOPORT

A csoport bemutatása

Az alapsokaságot az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar gépészmérnöki, mechatronikai mérnöki és biztonságtechnikai mérnök szakos hallgatói alkották. Az alapsokaságon belül egy kisebb csoportot képeztünk, melybe azok tartoznak, akik felvették 2022. tavaszi a félévében a Kollár Csaba által meghirdetett „Mesterséges intelligencia a műszaki életben" című tárgyat. A tantárgyat felvett hallgatók számára küldtük ki email-ben a felkérést, hogy lenne-e kedvük részt venni egy, a mesterséges intelligencia kihívásaival, lehetőségeivel, kockázataival, s jövőjével kapcsolatos fókuszcsoportos beszélgetésen. Felkérésünkre 5 nappali tagozatos hallgató jelentkezett: Bárczi Dávid, Barna Bianka Rita, Bayaraa Burtejin, Benkő Noémi, Fábián Zsolt. A junior szakértői fókuszcsoportban így 3 nő és 2 férfi vett részt, a legfiatalabb résztvevő 20, a legidősebb 28 éves volt, az átlagéletkoruk 24 év. Mind az öt junior szakértőnk jelenleg biztonságtechnikai mérnök alapszakos hallgató, információbiztonsági specializáción/szakirányon. Előtanulmányaik között a következő képzéseket nevesítették: logisztikai ügyintéző, tűzvédelmi előadó, egészségügyi szakközépiskola, gimnázium, hálózati rendszergazda, gépész, gépgyártástechnológus, CNC programozó, rendszerüzemeltető.

A csoport körében vizsgált kérdések, területek

Nyitókör:

- Kérek egy rövid bemutatkozást: keresztnév, életkor, milyen karra/szakra jársz?

Ráhangolás:

Gyerekkorotokból milyen emlékeket tudtok felidézni a mesterséges intelligenciával, illetve a robotokkal kapcsolatban?

- Volt valamilyen robotos játékotok, vagy láttatok valamilyen robotokról, mesterséges intelligenciáról szóló gyerekfilmet?
- Az elmúlt néhány évben milyen mozifilmeket láttatok a mesterséges intelligenciáról?
- Miközben néztétek a filmet, vagy utána, milyen érzések, gondolatok fogalmazódtak meg bennetek? miért?

Főkérdések:

- Mit jelent számotokra a mesterséges intelligencia?
- Saját szavaiddal megfogalmazva milyen definíciót tudnál adni a mesterséges intelligenciáról?
- Mit gondoltok, mi a különbség a robotok és a mesterséges intelligencia között?
- Eddig milyen területeken találkoztatok a mesterséges intelligenciával a valós életben?
- Ezeken a területeken a mesterséges intelligencia megjelenésével, illetve az általa nyújtott szolgáltatásokkal elégedett voltál?
- Ha nem, mit hiányoltál? ha igen, mi tetszett leginkább?
- Mit gondoltok, mely területeken lehet számítani a mesterséges intelligencia gyors megjelenésére?
- Ez milyen veszélyeket és lehetőségeket rejt magában?
- Szerinted Te fel vagy készülve a veszélyek mérséklésére?
- Ha igen, akkor mit javasolnál másoknak, mit tegyenek?

- Ha ezt a kerekasztal beszélgetést 10 év múlva, 2032-ben ismételnénk meg, mit gondolsz, mennyivel lenne másabb a világ a mesterséges intelligenciának köszönhetően?
- Boldogabban, vagy gondterheltebbek lennénk?
- Mely problémákra fog adni megoldás a mesterséges intelligencia az elkövetkező években?
- Egyre hangsúlyosabban fogalmazódik meg az igény, hogy a mesterséges intelligenciát csak addig és csak olyan irányokba szabad fejleszteni, hogy az ne veszélyeztesse az emberiség fejlődését. Mit gondolsz, ez hogyan lehetséges?
- El tudsz képzelni olyan helyzetet/területet, amikor a mesterséges intelligencia nem gondolkodik humánusan?
- Mit gondolsz, a Te szakterületeden a mesterséges intelligencia milyen változásokat fog hozni?
- Ezek jók, vagy inkább rosszak lesznek a számodra?

Zárókör:

- Ha a mai beszélgetést egyetlen mondattal kellene zárnod, mi lenne a tanúsága a számodra?

A kutatás eredménye

A fókuszcsoport tagjai ismerték egymást így a beszélgetés könnyen elindult a bemelegítő kérdéssel. Hasonlóan a senior szakértőkhöz, gyermekkorukban mindannyian találkoztak olyan filmekkel, amelyekben mesterséges intelligencia vagy robotok szerepeltek és azóta is rendszeresen néznek olyan filmeket, sorozatokat, amelyek valamilyen formában érintik ezeket. Első gyermekkori emlékeiket a témában az általános iskolai időszakhoz kötötték: főleg filmeket soroltak fel, de a Lego játékokat is többen említették. A meghatározó filmélmények között szerepeltek a következők: Én a robot, Robotok, Terminátor, Mátrix, Én vagyok anya, Johnny 5, Bosszúállók, Transformers, Knight Rider, Gungdame, Starwars, 2001: Űrodüsszeia, Wall-e, Űrdongó, Big bug, Ex machina. Videojátékokat is megneveztek, többek között a Mário és a Hero neve hangzott el.

A mesterséges intelligenciáról szóló történeteket már gyermekként is ambivalens érzésekkel élték meg: milyen mértékben humánus („barát vagy ellenség" pl. a Terminátor filmek), etikus (különbséget tesz-e a jó és rossz között). Egyetértettek abban, hogy a filmek általában negatív színben tüntetik fel a mesterséges intelligenciát, ez pedig torz képet alakít ki az emberek többségében, akik pusztán ezek alapján alkotnak fogalmat a mesterséges intelligenciáról. Ezen tapasztalatok nyomán a résztvevők többsége inkább disztópikus jövőképet vizionált. A szakértői csoporttal szemben, ahol a filmek az inspirációk és komplex problémahelyzetek megoldási lehetőségeinek forrásaként jelent meg, a junioroknál az emocionális tartalmak (fenyegetés) domborodtak ki. Ennek hátterében állhat a személyes érintettségük, azaz az eljövendő életükben egyre nagyobb teret kap és meghatározó lesz a mesterséges intelligencia jelenléte.

A junior szakértők emellett fontosnak tartották azt is, hogy a mesterséges intelligenciával kapcsolatos társadalmi szinten kialakuló sztereotípiák alakításában a filmes ábrázolások meghatározók, ahogyan egy személy a mesterséges intelligenciával, robotokkal kapcsolatos valóságot észleli, megítéli saját életét, helyzetét, kialakítja a reakcióit. Ezek között is külön kiemelték az érzelmi befolyásolást, az ismeretlentől való félelem is alapja lehet

annak, hogy túlhangsúlyozzák a robotok szerepét a filmekben. Az egyik résztvevő szerint a filmkészítők a leendő veszélyekre hívják fel a figyelmet, ami alapvetően akár pozitív is lehetne, mert motiválhatja a tudatos felkészülést. Ezzel szemben úgy vélik, a hangsúly túlságosan eltolódott a disztópia irányába, amely nem az aktív megküzdésre készít fel, hanem kiszolgáltatottságot vetíti előre.

A következő kérdés arra irányult, hogy van-e olyan filmélményük, melyben a robotok, illetve a mesterséges intelligencia pozitív színben tűnik fel. A résztvevők több filmet is felidéztek, mint például a Transformers, a Knight Rider (bár ennél a filmnél a megítélés inkább vegyes), illetve olyan filmtartalmakat, melyekben a család olyan robotokat használ, amelyek megkönnyítik a család életét. A filmekkel foglalkozó ráhangoló kérdések alapján kibontakozott egy konszenzuson alapuló vélemény, amely a senioroknál is hasonlóan alakult: a filmek többségében a mesterséges intelligencia, illetve a robotok negatív szerepet játszanak, ahol mégis pozitív kép alakul ki róluk, ott rendszerint a robotnak az embert segítő archetípusa kerül előtérbe.

Ahogyan a senior szakértőknél, úgy a junioroknál is a mesterséges intelligencia és a robot fogalmának megkülönböztetése volt a következő téma. Egyetértettek abban, hogy a robot fizikai testet öltött mesterséges intelligenciaként is definiálható. Többek szerint fontos szempont, hogy a robotot milyen módon programozzák, mivel a mesterséges intelligencia képes tanulni, addig egy egyszerű robot csak egy meghatározott utasításkészlet szerint képes cselekedni. Míg a robot egy egységet képez (fizikai teste van), addig a mesterséges intelligencia egyszerre több, vagy sok helyen is megjelenhet, különböző formákban, illetve fizikai testekben. A mesterséges intelligencia e megközelítés szerint inkább adathalmaz, felhő, ami nincs fizikai helyhez kötve. Egy újabb megközelítés az érzelmek jelentőségére fókuszált: eszerint a robotok szenvtelen gépek, míg a mesterséges intelligencia (amelyik akár egy robotban is megjelenhet) sokkal fejlettebb, a kommunikáció, akár az emberekkel történő interakció tekintetében, lényegében rendelkezik alapszintű empátiával. Egyik részvevő így fogalmazott: „Mivel a mesterséges intelligencia tanul, ezért elképzelhető, hogy idővel képessé válik arra, hogy az emberért feláldozza magát, mert az érzelmek is megjelennek a tanulási folyamat következtében."

A mesterséges intelligencia definíciójának saját szavaikkal való megfogalmazása gondolkodásra késztette a csoporttagokat, többféle módon közelítették meg: „olyan program, ami arra lett kifejlesztve, hogy tanuljon, fejlődjön azért, hogy a mi életünket könnyebbé tegye", „pozitív változást hoz az életünkbe, de meg kell ismernünk ahhoz, hogy ne féljünk tőle", „se nem jó, se nem rossz, hanem az alkotójának egy tükörképe", „ha képes a tanulásra, akkor képes a változásra, tehát nem biztos, hogy olyan lesz, mint amilyennek eleve megteremtették". Lényegében egy, az embert szolgáló társ/teremtmény, amelynek a fejlődése feletti kontrollt meg kell őrizni. A senior szakértők a definícióban főleg a technikai paramétereket vették sorra. Egyik csoportban sem volt megegyezés egy jól körülhatárolható fogalmi megközelítésről.

Fontos szempontnak tartották azt, hogy milyen generációnak készül a definíció, mivel a résztvevők szüleinek sokkal nehezebb elfogadni ezeket a fogalmakat, mint a saját leendő gyerekeiknek, akik már bele fognak születni ebbe a közegbe.

A junior fókuszcsoport résztvevői a seniorokhoz hasonlóan a mesterséges intelligenciával az élet minden területén találkoztak: az online kereskedelmi platformok, az online

közösségi média, a biztonsági berendezések és megoldások, a személyi asszisztensek, a metaverzumok. Saját szakirányukban, az információbiztonság területén, a mesterséges intelligencia az arcfelismerésben, a rendszámfelismerésben, a biometrikus azonosításban, mozgáskövetésben, a hangazonosításban, a kézírás felismerésében jelent meg.

Az okostelefon használata természetes velejárója a junior szakértők huszonéves korcsoportjának, így annak lehetőségeit és a rajta futó alkalmazásokat jól ismerik. Az ujjlenyomat felismerés, a beépített személyi asszisztens, a tanulást (matematikát) segítő alkalmazás, a hangos szöveg automatikus gépi leírása, a gyerekekkel beszélgető virtuális dada szerepeltek a mesterséges intelligenciával támogatott említések között. Említették, hogy bizonyos alkalmazások sajnálatos módon az országkorlátozás miatt nem, vagy csak kiskapukkal érhetők el, illetve az alkalmazások nyelve rendszerint valamelyik világnyelven érhető csak el ezért, ahhoz, hogy ezeket érdemben használni lehessen, beszélni kell a magyar mellett valamilyen világnyelven is, például angolul. A matematikai megoldást segítő alkalmazással kapcsolatban megkérdeztük, hogy a résztvevők mennyire bíznak meg a mesterséges intelligenciában, mint szolgáltatásban. Általában vegyes a megítélésük, s inkább a saját számításaik ellenőrzésére használták, mivel számos esetben rossz megoldást adott az alkalmazás. Amikor a hallgató által számított eredmény és a gép által számított eredmény megegyezett, akkor a hallgató elfogadta, amikor viszont nem, akkor a hallgató a saját eredményét fogadta el. Ahogy egyikük megfogalmazta: „a gépi intelligenciának csak akkor hiszek, amikor a humán intelligenciával azonos eredményt ad".

Felvetettük a résztvevőknek, hogy véleményünk szerint a mesterséges intelligencia bizonyos területeken az átlaghoz képest jobban fog fejlődni, s lesznek olyan területek, amelyek lemaradnak. A csoporttagok úgy látják, hogy önmagában nem csak a különböző területek, hanem a különböző országok között is komoly fejlődésbeli különbségek lesznek. Az egészségügyi területen járatos csoporttag a húzóágazatok között az egészségügyet és ezen belül az orvost mellőző diagnózis felállítást említette, ehhez csatlakoztak a többiek az egészségügyi rendszereket ellátó és kiszolgáló gépek fejlődésével: (pl. automatikus szállítógépek). A csoporttagok a komplex biztonsági megoldásokat, a balesetek, káresemények megelőzésének a lehetőségét, az intelligens otthonok (domotika) széles körben történő elterjedését, az információbiztonság területén a logfájlok eddiginél lényegesen fejlettebb és gyorsabb elemzését, a kibervédelmet és ennek másik oldalát a kibertámadásokat, az oktatást és ezen belül a személyre szabott oktatást sorolták még fel.

A következő kérdéscsoport a mesterséges intelligencia veszélyeinek és lehetőségeinek a feltérképezésére irányult. A veszélyek között leghangsúlyosabban, ahogyan a seniorok csoportjában is, a makroszintű munkaerő-piaci változások, a munkahelyek elvesztése szerepelt, illetve ezzel kapcsolatban a hozzátették a proaktivitás fontosságát, azaz az embereknek fel kell készülniük még időben ezekre a változásokra, mert ha erre nem képesek, akkor vesztesei lesznek a mesterséges intelligencia elterjedésének. Veszélynek érzik még a mesterséges intelligencia önállóságának fokozódását, ami révén öntudatra ébred, s „elszabadul". Ennek elkerülésére fontosnak tartják a megfelelő „vészleállítógomb" beiktatását. A lehetőségek között, központi szerepet kap az ember kényelmének és biztonságának fokozása, ahogy a beszélgetés során ez több esetben is elhangzott.

A junior szakértők úgy gondolják, hogy a mesterséges intelligenciával rendelkező eszközök, berendezések, gépek (pl.: gépkocsi) „egymáshoz kapcsolódni tudjanak azért, hogy közösen tudjanak jó döntéseket hozni, ehhez pedig megfelelő infrastruktúra (pl.: 5G

hálózat) szükséges". A mesterséges intelligenciák összekapcsolását egyébként ennek ellenére vegyesen ítélik meg, utalva arra, hogy a mesterséges intelligencia együttműködése révén olyan irányba fejlődik, ami lehet rossz (a gépek az ember ellen fordulnak) és lehet jó (az összekapcsolódás a biztonságot fokozza) is. Ezek a tényezők a kontroll és a biztonság szükségletei köré szerveződnek.

A beszélgetés során a generációs különbségek visszatérő szempontként vetődtek fel, mert a mesterséges intelligenciát a különböző korosztályok eltérően ítélik meg. A fókuszcsoport tagjai szerint saját generációjuk – különösen azok, akik nem rendelkeznek megfelelő műszaki, informatikai ismeretekkel – gyakran nem is tudják, hogy mit jelent a mesterséges intelligencia, vagy ha tudnak valamit róla (pl. a filmélmények alapján), nem is érdeklődnek iránta, vagy negatív, elutasító álláspontra helyezkednek, vagy nem képesek felismerni, hogy az adott területen mesterséges intelligencia dolgozik. A fiatalok közül kevesen vannak, akik időt és energiát fordítanak arra, hogy szakmai-tudományos források alapján alakítsák ki saját véleményüket a mesterséges intelligenciáról. A csoport véleménye alapján a korábban megfogalmazott elvárt proaktivitás hiányzik a fiatalokból, amely a társadalmi szintű megküzdés kulcsa lenne. A résztvevők – bár személyes szabadságukat fontosnak tartják – elfogadják, hogy a mesterséges intelligenciára épülő alkalmazások folyamatosan megfigyelik őket, „nem tudunk mit tenni ellene".

A fókuszcsoport tagok szüleinek generációja – 45-60 év közötti emberek – a fiatalokhoz képest még kevésbé értik meg a mesterséges intelligenciát, félnek tőle, féltik tőle a jövőjüket, a munkahelyüket. A középkorú emberek még inkább a filmélményekre, a bulvársajtó (ál)híreire hagyatkoznak, ami összességében egy nagyon negatív, elutasító attitűdöt eredményez.

A résztvevőkhöz képest 10-15 évvel fiatalabb generáció (kistestvér, keresztgyerek, rokongyerek) és a résztvevők között is meglehetősen nagy különbség fogalmazható meg. Ez a legfiatalabb generáció már a mesterséges intelligencia jelenlétébe született bele, természetes számára, hogy előbb tanulja meg az okostelefon, tablet használatát, mint hogy beszélni tudjon. A mesterséges intelligenciával támogatott eszközök használata a kisgyerekek számára természetes, így az ezeknek az eszközöknek a használata révén kialakuló képességeik és készségeik már jobbak, fejlettebbek, mint a huszonéveseké. A mesterséges intelligenciával támogatott eszközök és tartalmak annyira izgalmasak a kisgyerekek számára, hogy szinte egész nap azzal foglalkoznak, így szocializációjukban ezek az eszközök és tartalmak egyre nagyobb szerepet töltenek be. Természetesen ez nem igaz mindenkire – a résztvevők is hoztak fel ellenpéldát – de magukhoz képest úgy gondolják, hogy a mesterséges intelligencia sokkal dominánsabban volt és van jelen a kisgyerekek életében és fejlődésükben meghatározóbb hozzájuk képest: „míg nekünk meg kellett tanulni a mesterséges intelligencia használatát, addig ők ebbe már beleszülettek, számukra ez már természetes".

A következő beszédtéma a médiában és a filmekben is a valódi világ mellett kialakuló mesterséges világok (virtuális világ, metaverzum) megjelenése volt, amelyek informatikai alapját a mesterséges intelligencia jelenti. Ezzel kapcsolatban a fókuszcsoport tagjai úgy gondolják, hogy jelenleg az emberek többsége még különbséget tud tenni a valós és a virtuális világ között, ugyanakkor az elkövetkező évtizedekben számolni kell azzal, hogy a Mátrix című filmben látottakhoz hasonló világ jön létre, azaz egyre inkább elmosódik a különbség a fizikai valóság és a virtuális tapasztalatok között, s az embernek egyre nehe-

zebb lesz tudatosítani az élmények forrását. A virtuális világok és a metaverzumok megváltoztatják emberi kapcsolatainkat, az interperszonális kapcsolatok átalakulnak, egyre nagyobb részük már nem a fizikai világban realizálódik, ez a téma ellentétes nézőpontokat hozott a felszínre. Az egyik résztvevő szerint a szenzortechnika és aktuátortechnika annyit fog fejlődni, hogy egyre kevésbé fog feltűnni a fizikai kontaktus hiánya. Egy másik résztvevő szerint ezek a mesterséges intelligencia által létrejött virtuális világok segíthetnek majd abban, hogy az introvertált, a fizikai világban félénk és visszahúzódó emberek megnyíljanak. A harmadik résztvevő szerint nem pótolható a „kézzel fogható", valós emberi érintés, jelenlét semmilyen eszközzel, legfeljebb részben helyettesítheti azt.

A fókuszcsoport résztvevőit arra kértük, hogy próbálják „megjósolni" a jövőt, vagyis azt, hogy mi lesz 10 év múlva, 2032-ben a világban. Az egyik csoporttag Elon Musk nevét és tevékenységét meghatározónak tartja ebben a folyamatban, megemlítve a testbe építhető chipet, amelyik fogyatékos, lebénult embertársaink számára visszaadhatja a mozgás szabadságát. Egyetértettek abban, hogy a technológia egyre gyorsabban fejlődik, alakulhat jó és rossz irányban is és számos útválasztási döntés lehetséges, ami megnehezíti a reális tényeken alapuló jövőbelátást. Egyikük így fogalmazott: „lehet, hogy 10 év múlva a mesterséges intelligencia kutatás ott fog állni, mint ma, de lehet, hogy 10 év múlva a mesterséges intelligencia olyan szinten lesz, hogy mindenki önvezető autókkal fog járni". Egy másik vélemény szerint „én sokkal nyugodtabb lennék akkor, ha egy pozitív világkép lenne 10 év múlva és azt mondhatnám, hogy a mesterséges intelligenciának köszönhetően az én szüleim biztonságban vannak az intelligens otthonukban". Bár 10 év múlva a fókuszcsoport tagjai alapvetően egy boldogabb, biztonságosabb, kényelmesebb világban szeretnének élni a mesterséges intelligenciának köszönhetően, azt azért nem szeretnék, ha annyira elkényelmesednének, hogy az élet minden területén már csak az unalmas élet „élménye" maradna. Fontos kérdés volt a 10 évvel későbbi világ leírásakor, hogy mennyire lehet majd átadni a teljes irányítást a mesterséges intelligenciának. Az önvezető gépjárművek technikai megoldásait elemezve ismét megerősítették a résztvevők, hogy az egyes gépjárművek egymáshoz és a nagyobb rendszerekhez (pl.: intelligens város) kapcsolódása inkább csökkenti a biztonsági kockázatokat, de az nem lehet jó fejlesztési irány, hogy amikor a mesterséges intelligencia az autóban nem tud döntést hozni, akkor hirtelen átadja az irányítást az embernek, aki lehet, hogy éppen alszik az önvezető autóban. A hangsúly azon van, hogy „amikor az ember megbízik a mesterséges intelligencia döntéseiben, különösen a gyors döntéseiben, akkor nem jó, ha hirtelen át kell venni az irányítást, mivel az ember reakcióideje lassúbb, mint a mesterséges intelligenciáé, ezért szinte biztos, hogy rossz döntést fog hozni, vagy ösztönszerűen rosszul fog cselekedni". Ugyanakkor, amikor nincsenek ilyen helyzetek, akkor az elvárás az, hogy a mesterséges intelligencia biztosítja a biztonságot, s ha a kontroll biztonságosan átvehető, akkor azt az ember bármikor megtehesse. A fókuszcsoport tagjai a kontrollt is szükségesnek tartják, az automatikusan működő rendszereknél fontosak az olyan biztonsági megoldások, amikor meghibásodás, vagy kibertámadás esetén nem működik, vagy rosszul, vagy veszélyesen kezd el üzemelni a gép, akkor legyen egy vészleállító „gomb", aminek aktiválása után az eszköz biztonságosan leáll. Az optimális megoldást a résztvevők abban látják, hogy a technika fejlődésének köszönhetően növekszik a bizalmunk a mesterséges intelligenciával támogatott eszközök irányába, ugyanakkor ez a bizalom csak addig mehet el, amíg még lehetőség van bármikor biztonságosan átvenni az irányítást a mesterséges intelligencia felett.

A jövő globális problémáira, vagy legalábbis azok egy részére a mesterséges intelligencia a résztvevők szerint képes lesz valamilyen megoldást kínálni. Ugyanakkor nem lenne szabad az életünket csak a mesterséges intelligencia megoldásaira bízni, mivel a globális problémák megoldásánál most és a jövőben egyaránt szükség van olyan felelősségteljesen meghozott emberi döntésekre, amelyek aztán különböző törvényekben, szabályokban, szabályzatokban tudnak realizálódni. Ez természetesen nem zárja ki a lehetőségét annak – vélik a résztvevők – hogy a döntéshozók ne támaszkodjanak a mesterséges intelligencia döntéstámogatására. Épp ellenkezőleg: „a humán döntés jobb lehet, ha a sok adatot a mesterséges intelligencia dolgozza fel, hogy az ember jobban átlássa az adatokból levonható következtetéseket" – fogalmazott az egyik résztvevő.

Az oktatás során mi gyakran említjük a Sheridan-féle skálát, ami a gép autonómiájával foglalkozik. A fókuszcsoport tagjai úgy gondolják, hogy az elképzelhető, hogy a jövőben a gépek tanítják/fejlesztik a gépeket, s így időről-időre egyre fejlettebbekké válhatnak, ugyanakkor a gépeket tanító gépeknél olyan alapértékek tanítása kötelező, amelyek alapvetően az asimovi törvényekre vezethetők vissza. A képet árnyalja, hogy a mesterséges intelligenciában rejlő erőt a politikai hatalom saját céljaira is felhasználhatja, ezért fontos, hogy egy független tudományos-szakmai tanácsadó testület közösen határozza meg a fejlesztési irányokat, melyek alapvetően az emberiség érdekeit szolgálják. A tanítással kapcsolatban a fókuszcsoport tagjai között diszkusszió alakult ki arról, hogy mit kellene megtanítani a mesterséges intelligenciának: (1) tanulja meg az emberiség egész történelmét, majd ennek alapján hozzon döntést, vagy (2) az említett tanácsadó testület válogassa ki, hogy mi az a tudás, amit a mesterséges intelligenciának meg kell tanulnia ahhoz, hogy humánus döntéseket hozzon, vagy (3) a mesterséges intelligenciával a jót és a rosszat egyaránt meg kell tanítani, de azt is, hogy meg tudja különböztetni a jót a rossztól. A vitát azzal a konszenzussal zártuk, hogy ha a résztvevők majd, mint végzett mérnökök a mesterséges intelligencia tanításával, fejlesztésével foglalkoznak, akkor fontos, hogy a mesterséges intelligencia mindent tanuljon meg az emberi történelemből, hogy megfelelően megalapozott döntést tudjon hozni, de fontos, hogy megtanítsuk a mesterséges intelligenciát arra is, hogy mi a jó és mi a rossz, tehát meg tudja különböztetni ezeket a fogalmakat és az ezekhez kapcsolódó konkrét történéseket egymástól.

A résztvevők markáns különbséget tettek a mesterséges intelligencia polgári és katonai fejlesztési lehetőségei és irányai között. A polgári fejlesztésekkel kapcsolatban úgy gondolták, hogy fontos a fentebb említett nemzetközi, független, az emberiség fejlődését szem előtt tartó, humanista szakértőkből álló mesterséges intelligenciát tanító csapat. Fontos az is, hogy a csapat tagjai különböző szakterületekről érkezzenek, s pályafutásukkal szolgáljanak rá arra, hogy a mesterséges intelligencia tanítása során a humanista gondolkodás vezérli őket.

Egyik résztvevő felvetette annak gondolatát, hogy ahhoz, hogy a mesterséges intelligenciát hatékonyan és humánus elvek alapján lehessen fejleszteni, szükség van arra, hogy még jobban megismerjük azt, hogy az emberek hogyan működnek, hogyan gondolkodnak, hogyan, és milyen értékek mentén hoznak döntést. Az emberi gondolkodás (és álmodás) képekként történő megjelenése – ahogy az egyik résztvevő felidézte tudományos érdeklődése egyik példáját – a mesterséges intelligencia segítségével nem csak az emberi gondolkodás még jobb megértése miatt szükséges, hanem azért is, hogy ezáltal jobb mesterséges

intelligenciát lehessen fejleszteni. A résztvevők alapvetően úgy gondolják, hogy a mesterséges intelligenciát valamiféle érzelmi intelligenciával is fel kellene „okosítani": „ha megtanítod neki, hogy mi a boldogság, akkor meg kell neki tanítani, hogy mi a szomorúság is, hogy a mesterséges intelligencia különbséget tudjon tenni a két fogalom között". A mesterséges intelligenciát nem csak ellenőrzött módon tanítjuk, hanem abból is tanul, amit a külvilágból érzékel, tehát fel kell készíteni arra is, hogy a külvilágból szerzett információkat az emberiség számára és érdekében megfelelő módon tudja majd feldolgozni.

A fókuszcsoport tagjai számára – mivel mérnöki tanulmányokat folytatnak – nem voltak ismeretlenek a lágyszámítási módszerek, így a fuzzy logika sem. Ennek mentén úgy gondolják, hogy az igen-nem, jó-rossz bináris logikát érdemes jobban árnyalni a mesterséges intelligencia tanításánál. „A jó irány az lenne, ha a mesterséges intelligencia humánusan gondolkodna", s a jövőben a felhasználói területek nagy többségénél agressziómentesen viselkedne, vagyis „nem bántaná az embert, nem korlátozná az ember szabadságát". Az álláspontot diverzifikálja, hogy az alapvetően békésen viselkedő mesterséges intelligencia is kerülhet olyan helyzetbe, amikor agresszívan kell viselkednie. Az egyik résztvevő a családi humanoid robotot hozta fel példaként, aki alapvetően kedves, segíti a családot, részt vesz a gyerek nevelésében, de amikor egy betörő támadja meg a családot, akkor akár agresszió árán is megvédi a betörővel szemben a családtagokat. Itt az emberhez hasonlóan a támadás elhárításának a mértéke lehet a megoldás. A robotnak képesnek kell lennie felismerni az adott helyzetet, s ennek alapján csak a szükséges mértékig szabad ellenlépést tennie a támadóval szemben. Ez – véli az egyik résztvevő – az alapján is lehetséges, hogy „a mesterséges intelligencia a szenzorok segítségével folyamatosan monitorozza az ember biológiai állapotát, s ha a védendő személy pulzusa felgyorsul például a stressz miatt, akkor tudatosul a robotban, hogy baj van, cselekednie kell".

A bizalom kérdése felmerült a beszélgetés során a társas intelligenciával rendelkező robotokkal kapcsolatban is a robot/humanoid és az ember dada, illetve nagymama vonatkozásában. A robot sokkal tudatosabban fog viselkedni, ami kiszámíthatóbb (tehát egy humán dadával szemben akár megbízhatóbb is lehet), ugyanakkor fontos, hogy a humanoid képes legyen a családban, a családi életciklusok változásával együtt fejlődni, alkalmazkodni. Különösen érdekes a speciális nevelési igényű gyerekek mellett a jövőben megjelenő humanoid dada, amelyik az átlagos szülőkhöz képest sokkal nagyobb tudással rendelkezhet az ilyen gyerekek nevelésében, fejlesztésében, tehát – elvileg – sokkal eredményesebben képes az ilyen gyerekekből kihozni azt a maximumot, amivel később minél teljesebb életet tudnak majd élni.

Mivel a résztvevők biztonságtechnikai mérnök szakos hallgatók, ezért külön kérdésként foglalkoztunk a katonai robotok használatával. A katonai robotok esetében úgy gondolják, hogy a mesterséges intelligencia képes olyan feladatokat ellátni, amelyek révén a katonai akciók eredményesebben hajthatók végre, kevesebb a saját oldalon a humán katonai veszteség, a katonák biztonságos távolságból tudják nyomon követni, vagy irányítani a robotkatonákat. Ugyanakkor veszélyként merülhet fel, hogy ha a robotkatona felismeri, hogy alkalmazásának célja az, hogy feláldozza magát az emberért, akkor meglehet, hogy fellázad ez ellen. A megoldást az egyik résztvevő abban látja, hogy „mekkora szabadságot engedek a robotkatonának. Ha a robotkatona szabadsága erősen beszabályozott, akkor a katonát képes kiszolgálni, támogatni, például azzal, hogy viszi a nehéz csomagokat, vagy képes felderíteni és akár megsemmisíteni az ellenséget, de azt nem tudom elképzelni, hogy

mellettem egyenrangú félként harcoljon". Miközben több szakirodalom foglalkozik a robot-robot harccal, vagyis amikor a robotkatona harcol robotkatona ellen, a fókuszcsoport tagjai úgy vélik, hogy ez nem minden esetben jelent megoldást. Három okot neveztek meg ezzel kapcsolatban: (1) ha a robotot a háttérből ember irányítja, s az irányítás megszűnik, akkor a robot harcképtelenné válik, tehát könnyen megsemmisíthető az ellenség részéről, (2) az elektromágneses impulzusfegyverek képesek akár az önjáró, akár a háttérből vezérelt robotkatonákat harcképtelenné tenni, (3) az egymással szemben álló robotkatonák technikai fejlettségbeli különbsége eldöntheti a harc kimenetelét. Megemlítették azt is, hogy miközben a hagyományos hadviselésnél alkalmazott szabályok (rules of engagement /ROE/) viszonylag egyértelműen fogalmaznak a harci cselekményekkel kapcsolatban, addig különösen az autonóm harcjárművek, illetve humanoid robotkatonák esetében ezek a direktívák még nem állnak rendelkezésre.

A mesterséges intelligencia katonai felhasználási lehetőségeivel kapcsolatban ismét felmerült az a kérdés, hogy mekkora autonómiát engednének meg a résztvevők a jövő katonai és polgári humanoid, vagy általánosságban mesterséges intelligenciával támogatott robotjai számára. A kérdés elbizonytalanította a résztvevőket, részint amellett próbáltak meg állást foglalni, hogy a gépeknél inkább korlátozni és minimalizálni kell az agressziót, illetve, ha a robot lecsatlakozik a hálózatról, akkor át kell váltania egy egyszerűbb működésre, ami minimális funkciókat engedélyez a számára (pl., hogy megkeresse a legközelebbi felcsatlakozási pontot), bár katonai robotoknál erre nem láttak reális megoldást, pont a speciális felhasználás miatt.

A résztvevők 10 év múlva, már végzett biztonságtechnikai mérnökként úgy gondolják, hogy olyan szakmai területen helyezkednek el, ahol napi szinten fognak találkozni a mesterséges intelligencia lehetőségeivel, így például az információbiztonság, a haditechnika, vagy a nemzetbiztonság területén. Örömmel vennének részt a mesterséges intelligencia fejlesztésében, tanításában.

A fókuszcsoportos beszélgetés zárásaként a következő összegző mondatokat fogalmazták meg a résztvevők: „érdekfeszítő beszélgetés volt, jó volt megtapasztalni a sokféle, akár egymástól eltérő véleményt is", „számomra is nagyon jó volt, az eltérő véleményünk alapja szerintem az volt, hogy ki mennyire bízik meg a mesterséges intelligenciában", „nagyon hasznos, érdekes, informatív beszélgetés volt", „nagyon szerteágazó a véleményünk, s igazából nem tudjuk, hogy mi lesz az elkövetkező tíz évben a mesterséges intelligenciával, csak sejtéseink vannak", „a sokszínű gondolkodásmód és bizonytalan jövőkép mellett meg kell találnunk egyfajta konszenzust, ami révén kialakítható a mesterséges intelligencia és a közös jövőnk".

A JUNIOR SZAKÉRTŐK VÉLEMÉNYE ALAPJÁN MEGFOGALMAZOTT KÖVETKEZTETÉSEK, JAVASLATOK

A junior szakértők a mesterséges intelligencia területén járatos egyetemi hallgatók voltak, akik életkoruknál fogva a senior szakértőktől eltérő tapasztalatokkal és idői perspektívával tekintettek a kérdésekre. A mesterséges intelligenciával kapcsolatos maradandó gyermekkori film és egyéb élményeik emocionális hatása élénken élt bennük. A junior szakértők egyetértettek abban, hogy a mesterséges intelligencia fejlődési tempójának és irányának kiszámíthatatlansága következtében a potenciális jövőképek széles határok között mozognak. Úgy vélték, hogy ha a társadalmi tudatosság és proaktivitás helyett az érdeklődés

hiánya és a félelmek alakítják az emberek attitűdjeit, ezzel a passzivitással a technopesszimista forgatókönyv önbeteljesítő jóslatként valósulhat meg. A disztópikus jövőkép visszatérő eleme volt a megnyilvánulásaiknak, amely reális fenyegetés lehet az életük alakulásában. A mesterséges intelligencia társadalmi megítélésében egyhangúan megegyeztek abban, hogy a középkorúak és idősek korosztályában a félelem dominál, amely egyrészt a médiareprezentációra vezethető vissza, másrészt a bizonytalanság következtében kialakuló természetes emberi reakció. A fiatal felnőttek, azaz a saját generációjuk nem ismeri fel a mesterséges intelligenciát, tájékozatlanok, nem is foglalkoztatja őket, ezért a veszélyeket sem mérik fel, kiszolgáltatottak, beletörődő attitűddel viszonyulnak a mesterséges intelligenciához. A gyerekek széles körében már szocializációjuk természetes velejárója a mesterséges intelligencia jelenléte és számukra nem jelent fenyegetést pl. az adataik felhasználása, amit az idősebbek kevésbé fogadnak el. A generációk attitűdjeinek eltérései szintén visszatérő gondolati szervezőerő volt.

A mesterséges intelligencia és a robotok definiálása a junior szakértőknél nem eredményezett egységes álláspontot, ahogyan az elméletalkotók is különböző meghatározásokat használnak, inkább gyűjtőfogalomként értelmezhető. A mesterséges intelligencia feletti kontroll szükségletét hangsúlyozták, mint elengedhetetlen komponens, pl. egy biztonságot nyújtó vészleállító gomb formájában, amely a fenyegetéssel szembeni aktív megküzdés eszközeként értelmezhető és a vágyott optimista forgatókönyvhöz vezet. A mesterséges intelligencia veszélyei közé sorolták a munkanélküliség tömegessé válását, illetve a technika fejlődésével egyre fokozódó autonómia következtében kialakuló „öntudatra ébredést" és ezzel társultan az emberi faj elleni agresszív fellépést. A mesterséges intelligencia mindkét esetben az emberiség szolgálata helyett az alárendelt szerepből riválissá válik, ami manapság a félelemmel együtt járó bizalmi deficitet erősíti.

A junior szakértők a mesterséges intelligencia alkalmazásainak széles körét ismerik [1], maguk is használnak néhányat leginkább az okostelefonok segítségével. Ezek hátrányaként a nyelvi és a földrajzi elérhetőség szabta korlátok mellett nagyobb szerepet kapott a megbízhatóság kérdése, példaként egy számítási feladatokat végző, téves eredményeket is generáló alkalmazást említettek.

Kiemelték még az interperszonális kapcsolatok várható minőségi változását, amely a virtuális világok és a fizikai valóság közti határok összemosódásával létrejövő multidimenzionális élményekre épül, ennek megítélése ellentmondásos volt, a résztvevők mind pozitív, mind negatív véleményeket is megfogalmaztak. A kényelem, a biztonság és boldog élet reménye határozták meg a reményeiket, de egyben azt a veszélyt látják, hogy unalmassá, „túl kényelmessé" válik a világ. A 2032-ben elképzelt világban többek között az intelligens városok, otthonok, gépjárművek biztonságos, kiszámítható és humánus döntéseket hozó működését várják. Nagy horderejű döntések esetén továbbra is felelősségteljes emberi döntéshozókat, testületeket tartanak elfogadhatónak, akik a döntéstámogató rendszereket használják.

A junior csoportban megfogalmazott vélemények tartalmában a fentiekből azonosíthatók azok a pszichológiai szükségletek, amelyeket Ryan és Deci [2] öndetermináció elméletükben írtak le. Eszerint az embereknél három alapszükséglet különböztethető meg:
(1) az autonómia, azaz a szabad döntések és cselekvések lehetősége, amelyet a „nem humánus döntéseket hozó", vagy „öntudatra ébredő", az emberi fajjal versengő mesterséges intelligencia fenyeget;

(2) a kompetencia, azaz az énhatékonyság érzésének igénye, amelyet a mesterséges intelligencia feletti kontroll elvesztése, és az „elkényelmesedés" fenyeget;
(3) a kapcsolódás szükséglete, azaz a szeretetre, tiszteletre épülő kapcsolatok kialakítása, amelyet a virtuális világok multiverzuma fenyeget.

A szakértők a további témáknál is kidomborították az emberi vonások szükségességét a mesterséges intelligencia bizonyos alkalmazásainál, pl. szociális, érzelmi intelligencia szükségessége, vagy a gondjaira bízott személy védelme érdekében tanúsított agresszió. Ez utóbbi különösen a katonai mesterséges intelligencia, ill. robotok felhasználása esetén fontos kérdés, pl. az ember-robot, illetve a robot-robot harc esetén a hagyományos hadviselés szabályainak érvényessége.

A SENIOR ÉS A JUNIOR SZAKÉRTŐK VÉLEMÉNYÉNEK KOMPARATÍV ELEMZÉSE

A senior és a junior szakértők tapasztalatbeli és felfogásbeli különbségeik ellenére számos területen hasonlóan gondolkodtak.

A mesterséges intelligenciához köthető karrier hátterében mindkét csoportban felismerhető a gyermekkori film és egyéb élmények hatása a pályaválasztásra. A stabil pályaidentitással rendelkező seniorok körében kiegészült azzal, hogy a folyamatos fejlődési lehetőség és a megélhetés biztosításával elkötelezettek a szakmai munkájuk iránt. A két csoport közti generációs különbségből fakadóan a juniorok a jövőre irányuló idői perspektívából közelítették meg a kérdéseket, míg a senioroknak tágabb rálátása van a mesterséges intelligencia múltjára, jelenére, jövőjére. Mindkét csoport számos mesterséges intelligenciára épülő alkalmazást ismer, leginkább az okos otthonok (domotika), intelligens városok, autonóm járművek, egészségügyi és gyógyszeripari alkalmazások, gazdasági pl. banki, katonai területen, mezőgazdasági, környezetvédelmi, oktatási célú felhasználás.

Annak ellenére, hogy a fókuszcsoportok tagjai kompetens szakértők voltak, a mesterséges intelligencia definíciójában nem alakult ki konszenzus egyik csoportban sem, ez egybevág azzal, hogy a szakirodalomban is számos különböző meghatározás létezik, ezért inkább gyűjtőfogalomnak tekinthető. Mindkét csoportban tartalmilag a biztonságosság és kényelmesség köré szerveződtek az asszociációk, amelyet a junorok emocionális színezettel fogalmaztak meg (jó-rossz, félelemkeltő), a seniorok pedig a racionális (technikai, gazdasági) oldalt ragadták meg. A robotok és a mesterséges intelligencia megkülönböztetésében a robotokhoz fizikai megtestesülést társítottak, mindkét csoportban megjelentek az egyik póluson a kiber-fizikai rendszerek a másokon pedig a humanoid/animoid robotok, ez utóbbiak szociális, emocionális készségeikkel felruházva. Mindkét csoportban egyetértettek abban, hogy a robotok és a mesterséges intelligencia médiareprezentációjában jelentősen több a disztópikus ábrázolás, ahol az emberi faj létét fenyegetik, ezért a mesterséges intelligencia társadalmi percepciójában a negatív emocionális tartalmak dominálnak, elsősorban a félelem jellemző.

A fókuszcsoportok szakértői részletesen kifejtették a mesterséges intelligenciával kapcsolatos kockázatokat, kihívásokat, amelyek az alábbi fő területeket érintették:

- Társadalmi szintű bizalmatlanság: a mesterséges intelligencia gyakran olyan kontextusokban jelenik meg, amely fenyegetést jelent, visszaélések eszközévé válhat, így gyanakváshoz, elutasításhoz vezet.

- Transzparencia hiánya: komplexitásánál fogva magas szinten képzett, tapasztalt szakemberek számára is kihívást jelent a mesterséges intelligencia gyakorlati alkalmazásainak kockázatelemzése, pl. a potenciális veszélyek feltárása (hibás programozás, hibás tanítás, kibertámadás), az ezek következtében fellépő anyagi vagy más erőforrásbeli károk megbecsülése.
- Torzítások, diszkrimináció, amely leképezi az emberi döntéshozatal szisztematikus hibáit, pl. az előítéletekkel terhelt (vallási hovatartozás, nemi identitás) adatokra épülő gépi tanulás eredményeképpen alakulhat ki.
- Az információ- és adatbiztonság a szabályozatlanság és átláthatatlanság miatt egyre kevésbé garantálható, az adatok felhasználása áttekinthetetlenné válik, a privát szféra és az az emberi jogok sérülhetnek, pl. társadalmi kredit rendszere.
- A mesterséges intelligenciát tisztességtelen politikai, gazdasági hatalmi célok érdekében alkalmazzák, a demokratikus értékek és az emberi jogok sérülnek.
- Munkaerő-piaci átstrukturálódás: egyrészt az emberi munka mesterséges intelligenciára épülő technológiával való helyettesítése tömeges munkanélküliséget okozhat megfelelő átképzések hiányában. Másrészt a mesterséges intelligencia fejlesztéséhez megfelelően képzett munkaerő iránti egyre növekvő kereslet kielégítése munkaerőhiányt okozhat, ma még nem ismert új szakmák megjelenése várható. A munkaerő-piaci átrendeződés a társadalmi egyenlőtlenségek fokozódásához, a társadalom szétszakadásához vezethet.

A junior szakértők szerint a generációk eltérő módon viszonyulnak a mesterséges intelligenciához. Minél fiatalabb a személy, annál elfogadóbb és természetes számára, az idősebbek pedig bizalmatlanok, fenyegetőnek találják. A szakértők szerint a veszélyek megelőzését szolgáló lépéseket, intézkedéseket nem lehet halogatni, a kedvezőtlen folyamatok ma még kontroll alá vonhatók, a jövő alakítható és ebben a szakembereknek is aktív szerepet kell vállalniuk.

A szakértők bíznak abban, hogy a mesterséges intelligencia 10 év múlva az emberiség jóllétét és kényelmét fogja szolgálni, hozzájárul az életminőség javulásához, humánus és etikus módon fog működni. Ennek érdekében a társadalom minél szélesebb körét fel kell készíteni a mesterséges intelligencia várható hatásaira és használatára. Mindkét csoport szerint a virtuális világok, metaverzumok és a fizikai valóság közti határ elmosódik, elképzelhető, hogy a virtuális világba terelődik a boldogságkeresés, a hús-vér emberi kapcsolatokat az avatárok által konstruált világok válthatják fel, az érzékszervi tapasztalatokat a szenzortechnika fogja pótolni.

A mesterséges intelligencia humánközpontúságának egy speciális területe a hadviselés, ahol az agresszió és a hagyományos hadviselési szabályok alkalmazása számos kérdést vet fel. A seniorok a szabályozás oldaláról közelítették meg a kérdést: ezen a területen a mesterséges humánum bevezetése szükséges, azaz az emberi beavatkozás lehetősége mindvégig adottságként jelen legyen, az ellencsapás mértéke ne legyen jelentősen nagyobb a csapásnál. Nem lehet cél az ellenfél totális elpusztítása sem, a háborúkra vonatkozó nemzetközi jogi szabályok, előírások betartása továbbra is követelmény kell, hogy maradjon. A hadviselési szabályokat ki kell dolgozni a mesterséges intelligenciával működtetett eszközökre is. A juniorok technikai szempontból vizsgálták a kérdést: a robotkatonák alkalmazásáról megállapították, hogy kockázati tényezőként számolni kell a kontrollálhatatlanná válással, ill. a háború kimenetelét eldöntő technikai fejlettséggel. A robotok és a mesterséges

intelligencia agresszív viselkedéséről a juniorok megállapodtak abban, hogy az ember testi épségének védelme érdekében elfogadható lehet, példaként egy gyermeket a betörővel szemben védelmező családi robotot képzeltek el, amely a gyermek fiziológiás reakciói segítségével vált védelmező üzemmódra.

Mindkét csoportban kifejezték az etikus mesterséges intelligencia megteremtésének fontosságát, ennek hiányában a disztópikus jövőre vonatkozó aggodalmaikat reális fenyegetésnek érzékelik. A mesterséges intelligencia ember által alkotott „teremtmény", amely az emberi fajjal békében együtt élő társsá vagy riválissá válhat a koevolúció során. A junior szakértőknél gyakrabban jelentek meg emocionális színezetű vélemények, míg a seniorok konkrét tapasztalatokat, ismereteket osztottak meg, ezáltal tényszerűbb, racionálisabb formában fejezték ki álláspontjukat.

További tartalomelemzési szempont lehet későbbi kutatásokban – mely jelen cikk kereteit meghaladja – az ember pszichológiai szükségleteinek vizsgálata a mesterséges intelligenciára vonatkozó attitűdökben. Kiindulásként szolgálhat pl. a széles körben ismert Maslow [3] féle öt szintű szükséglet-hierarchia A fiziológiás szükségletek kielégítésének biztosítása a termelés és szolgáltatások területén, már a jelenleg is alkalmazott eljárások tovább fejlesztésével, egyre kényelmesebbé teheti az életet, de a tartós komfortérzet unalomhoz vezethet. A biztonságszükségletek a mesterséges intelligencia kiszámíthatóságára, megbízhatóságára, a kockázatok és veszélyek minimalizálására irányulnak, pl. a „védelmező robot" is ezt a célt szolgálja. A hovatartozás és szeretet szükségletének kielégítésére már ma is léteznek szociális robotok („szerethető robot"), az emberrel empatizáló, érzelmi és társas intelligenciával rendelkező mesterséges intelligencia töltheti be ezt a szerepet. A megbecsülés szükséglete akkor elégül ki, ha az ember megőrzi az autonómiáját és alkotóképességét, ezzel mások elismerését kivívja, pl. aktívan szerepet vállal a mesterséges intelligencia fejlesztésében, vagy a szabályozó testületek munkájában, élethosszig tartó tanulással képes a munkaerő-piaci kihívásoknak megfelelni. Végül az önmegvalósítás számára tág lehetőség nyílik nemcsak a metaverzumokban, hanem a kényelmes élettel járó több szabadidő kreatív eltöltésével.

Mindkét csoport hasznosnak találta a fókuszcsoportban a tapasztalatok és vélemények kölcsönös megismerését, a közös gondolkodást, újabb nézőpontokat ismertek meg, tudatosították a fenyegetések széles körét.

ÖSSZEGZŐ GONDOLATOK, KÖVETKEZTETÉSEK

A mesterséges intelligencia fejlődésében kritikus szakaszba lépett az emberiség, egyszerre rejti magában a lehetőséget az emberek életminőségének ugrásszerű javulására, de a disztópikus jövő is realizálódhat, ahogyan explicit módon a szakértők is kifejtették. Sinderman [4] és munkatársai a mesterséges intelligenciával kapcsolatos öt attitűdöt különböztettek meg, amelyekben visszatükröződik e két irány: bizalom a mesterséges intelligenciában, a mesterséges intelligencia hasznos lesz az emberi faj számára, ezzel szemben a mesterséges intelligencia félelmetes, fenyegető, az emberi faj pusztulásához vezet, munkanélküliséget okoz számos területen. A potenciális fenyegetések csökkentése érdekében nem elegendőek a nemzetközi szervezetek szabályozó intézkedései (pl. UNESCO [5], OECD [6], [7]), társadalmi szintű fellépés szükséges a demokratikus értékek és az emberi jogok védelmében, a közjó és jóllét növelésében, a személyes adat- és információbiztonság fokozásában. A társadalmi bizalom javításához az intelligens rendszerek etikus fejlesztésében

biztosítani kell a hatékonyságot, az átláthatóságot, a professzionalizmust, ki kell jelölni a felelősségi köröket és a visszaélések lehetőségét minimalizálni szükséges, ahogyan ezt egy 700 fős szakértői közösség is deklarálta [8]. A szakértők, Tilesch és Hatamleh [9] megállapításához hasonlóan, a humánközpontú mesterséges intelligencia létrehozásában egy globálisan elfogadott, megvalósítható mesterséges intelligencia vízió kialakítását sürgetik, amely az általános emberi értékekre épül, az eltérő érdekeket harmonizálja, egységes szabályozási keretbe foglalja, a paradigmaváltás azonban csak akkor válik teljessé, ha az emberiség a lelkiismeretességre és tudatosságra alapuló új világképet hoz létre, ezzel biztosítva a faj fennmaradását.

FELHASZNÁLT IRODALOM

[1] Kollár Cs.: A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában in Kiberbiztonság/Cybersecurity, edited by Z.Rajnai Biztonságtudományi Doktori Iskola, Budapest, 2019, ISBN: 978-963-449-185-9. letöltés: https://drkollar.hu/blog/2020/01/27/kiberbiztonsag-cybersecurity-uj-ingyenesen-elerheto-kiadvany/

[2] Ryan, R. M., Deci, E. L., Self-determination theory: Basic psychological needs in motivation, development, and wellness. 2017. New York: Guilford Publishing

[3] Maslow, Abraham H. A Theory of Human Motivation (1943), Originally Published in Psychological Review, 50, 370-396. letöltés: http://psychclassics.yorku.ca/Maslow/motivation.htm

[4] Sindermann, C., Sha, P., Zhou, M. et al. Assessing the Attitude Towards Artificial Intelligence: Introduction of a Short Measure in German, Chinese, and English Language. Künstl Intell 35, 109–118 (2021). letöltés: https://doi.org/10.1007/s13218-020-00689-0

[5] UNESCO: PRELIMINARY STUDY ON THE ETHICS OF ARTIFICIAL INTELLIGENCE (COMEST), 2019.: https://en.unesco.org/artificial-intelligence/ethics/cases#biasedai

[6] OECD (2019) Artificial Intelligence in Society. letöltés: https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm

[7] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. letöltés: 22/05/2019, letöltés: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[8] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems 2019. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. 1st ed.: IEEE. letöltés: https://ethicsinaction.ieee.org/#series

[9] G.A.Tilesh, o. Hatamleh: Between brains, Taking back our futrein the AI age, GTPublishDrive; Publishdrive ed. edition, 2020.

COVID-19 safety at work

Occupational safety measures and consequences of a coronavirus pandemic in healthcare

A COVID-19 munkabiztonsága

Koronavírus világjárvány munkabiztonsági intézkedései és következményei az egészségügyben

SIMON Mátyás[1]

Abstract

In the field of occupational safety and health, one of the biggest challenges of recent times has been to define and apply occupational safety and health conditions and rules for health and healthcare workers involved in the control of the coronavirus epidemic. Our research covered the procedures applied at the patient care departments of Hungary's largest health care, teaching and research universities, as well as occupational health and safety documentation prepared for covid care departments, such as risk assessments, personal protective equipment benefits, and prevention and collective protection measures. The COVID-19 coronavirus epidemic has caused severe damage to both society and the economy, and has posed a huge challenge to the health sector and thus to occupational safety and health professionals. The pandemic also reminded us that prevention and risk assessment are the most important tools for occupational safety and health.

Keywords

COVID-19, pandemic, occupational safety, occupational health, health emergency, epidemic prevention, occupational safety measures

Absztrakt

A munkavédelem szakterületén az elmúlt időszak egyik legnagyobb kihívása lett a koronavírus járvány elleni védekezésben résztvevő egészségügyi és egészségügyben dolgozók munkabiztonsági és munkaegészségügyi feltételeinek, valamint szabályainak meghatározása és alkalmazása. Kutatásunk Magyarország legnagyobb egészségügyi ellátó, oktató és kutató egyetem betegellátó szervezeti egységeinél alkalmazott eljárás rendekre, utasításokra, valamint a covid ellátó osztályokra készített munkavédelmi szakmai dokumentációkra, így a kockázatértékelésekre, egyéni védőeszközök juttatás rendekre, továbbá a megelőzésre és a kollektív védelemre hozott intézkedésekre terjedt ki. A COVID–19-koronavírus-járvány súlyos károkat okozott mind a társadalomban, mind pedig a gazdaságban, valamint hatalmas kihívás elé állította az egészségügyi területet és ezzel a munkavédelmi szakértőket is. A pandémia arra is emlékeztetett bennünket, hogy a munkavédelem legfontosabb eszközét a megelőzést, valamint a kockázatok értékelését komolyan kell venni.

Kulcsszavak

COVID-19, pandémia, munkavédelem, munkahelyi egészségvédelem, egészségügyi vészhelyzet, járvány elleni védekezés, munkabiztonsági intézkedések

[1] matyas.simon86@gmail.com | ORCID: 0000-0002-2714-857X | PhD student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztoságtudományi Doktori Iskola

BEVEZETÉS

Az első hírek 2019 decemberében érkeztek, miszerint a kínai Vuhanban egy újfajta vírus okoz megbetegedéseket, még elképzelhetetlennek tűnt, hogy az életünket egy kibontakozóban lévő világjárvány milyen elsöprő gyorsasággal fogja megváltoztatni. Ekkor még annyit lehetett tudni, hogy egy influenzához hasonlító, cseppfertőzéssel terjedő vírus okoz súlyos megbetegedéseket, ami leginkább az idősebb korosztályra veszélyes. Pár hét elteltével – 2020. március első napjaiban – már Magyarországon is diagnosztizálták az első eseteket, ami megkongatta a vészharangot.

A munkavédelem szakterületén az elmúlt időszak legnagyobb kihívása lett a koronavírus járvány elleni védekezésben résztvevő egészségügyi és egészségügyben dolgozók munkabiztonsági és munkaegészségügyi feltételeinek és szabályainak meghatározása és alkalmazása. Az egészségügyi ellátó szervezetnek azonnal reagálniuk kellett a járványra, betartva a jogszabályi előírásokat, valamint a kormányzati határozatokat, hatósági utasításokat és javaslatokat. A koronavírus hazai megjelenése után az egészségügy területén megvizsgáltuk a pandémia elleni védekezés rendszerét és annak eredményességét. Kutatásunk célja a Magyarországon működő legnagyobb egészségügyi ellátással foglalkozó orvosi egyetem koronavírus-járvány elleni védekezési gyakorlatának és módszereinek felmérése. A vizsgálat során arra kerestük a választ, hogy az egészségügy ellátó területén munkavédelmi szempontból milyen kihívásokkal és problémákkal küzdöttek meg, hogyan kezelték az előírt, illetve javasolt szabályokat, milyen szükséges intézkedéseket tettek és határoztak meg, továbbá hogyan kerültek beépítésre a szabályozási rendszerbe.

SZAKIRODALMI ÁTTEKINTÉS

A COVID–19-koronavírus-járvány súlyos károkat okozott mind a társadalomban, mind pedig a gazdaságban, ezt Köllő és Reizer tanulmánya is megerősíti, miszerint a világjárvány első hulláma során bevezetett korlátozások és gazdasági zavarok jelentős negatív hatással volt a munkaerőpiacra és a gazdasági szereplőkre egyaránt. Mindez megjelent a foglalkoztatottak számának változásában és jelentősen növekedett a jövedelemi egyenlőtlenségek aránya. [1]

Pandémiás helyzetben az új eljárás rendekhez szükséges információkat a járvány kialakulásának, terjedésének nyomon követéséért felelős járványügyi szervezetek biztosítják. A járvány elleni védekezéséhez a különböző szakmai szervezetek, mint például az Egészségügyi Világszervezet (WHO), vagy Magyarországon a Nemzeti Népegészségügyi Központ tájékoztatói fontos információkat biztosíthatnak, amelyeket a munkavédelem szakterületén is alkalmazni szükséges. Ezt Faragó Ferenc kutatása is megerősítette, miszerint a munkáltatók „A védekezési eljárások kidolgozásához elsősorban a kormányzati utasításokat és szabályokat vették figyelembe a vállalatok, mert a járvány kezdeti szakaszában főként a kormányzati kommunikáció, a Magyar Kormány által létrehozott Operatív Törzs tájékoztatói voltak a széles körben elérhető információforrások. A vállalatok emellett kikérték a szakmai szervezetek (Népegészségügyi Szakigazgatási Szerv stb.) javaslatait is.” [2]

Az Egészségügyi Világszervezet (WHO) szerint a munkavédelem feladata, hogy a dolgozók testi, lelki, szociális jó közérzetének elősegítése és megtartása minden foglalkozásban, a dolgozók körében a munkakörülményekből származó egészségi károsodások

megelőzése, a dolgozók védelme az egészségük ellen ható veszélyektől, továbbá olyan munkakörnyezet biztosítása és fenntartása, amely a dolgozók fiziológiai és pszichológiai adottságaihoz alkalmazkodik.

A munkavédelem összetett szakterület, ebben kapcsolódik össze a munkaegészségügy, a munkahigiéné és a munkabiztonság. [3] A három terület együttesen teremti meg a munkavállalók biztonságos munkakörülményeit, a tevékenység elvégzéséhez szükséges személyi és tárgyi feltételeket egyaránt.

A Munkahelyi egészség- és biztonságirányítás - Általános iránymutatások a biztonságos munkavégzéshez a COVID-19 világjárvány idején tárgyú ISO/PAS 45005 szabvány 2020. decemberében jelent meg és célja, hogy a pandémia, így például a koronavírus-járvány munkahelyi hatásainak kezelésére iránymutatást adjon. A szabvány a járványt kockázatalapú és a lehetséges intézkedésekre vonatkozó gyakorlati útmutatással kezeli, így hangsúlyosan megjelenik a tervezés, a kockázatok felmérése és értékelése, valamint a feltárt kockázatok hatékony kezelésére tett intézkedések fontossága. A biztonságos munkavégzés személyi és tárgyi feltételeinek biztosítása a munkáltató kötelezettsége, ennek érdekében munkaszervezéssel (fizikai elkülönítés, távmunka, home office), munkavállalók tájékoztatásával, higiénés feltételek biztosításával, valamint belső szabályok meghatározásával intézkedhet.[4]

Elsősorban műszaki és szervezési intézkedésekkel kell megteremteni a munkavállaló számára az egészséges és biztonságos munkavégzéshez szükséges feltételeket, melyhez a munkáltató köteles a kockázatokat mennyiségileg és minőségileg értékelni.

A Munkahelyi egészségvédelmi és biztonsági irányítási rendszer (MEBIR) a szervezetek kockázatkezelő stratégiájának alapvető részét alkotják. A MEBIR alapkövetelménye a kockázatalapú megközelítés, azaz a szervezet kockázatainak felmérése és erre hozott intézkedések meghatározása. [5] A munkavállalók egészségét és biztonságát veszélyeztető kockázatokra – különösen az alkalmazott munkaeszközökre, veszélyes anyagokra, a munkavállalókat érő terhelésekre, valamint a munkahelyek kialakítására – a munkáltatónak rendelkeznie kell kockázatértékeléssel. A kockázatértékelés során kerülnek azonosításra a veszélyek, a veszélyeztetettek köre, a veszély jellege, valamint a veszélyeztetettség mértéke továbbá összeállításra kerül az intézkedési terv a kockázatok csökkentése érdekében.

A munkavédelem alapvetően kockázatértékelés során feltárt kockázatokra és ennek csökkentéséhez szükséges intézkedésekre épül. Szabó Gyula így fogalmazta meg értekezésében: „A kockázatcsökkentés munkavédelmi elveinek megfelelően a kockázatértékelést jobb és jobb megoldások megvalósítására kell felhasználni, pl. a veszély kiküszöbölésére, több veszélyére közös védelmi intézkedés kidolgozására, az egyébként elfogadható védelmek hosszú távon tervezett kiváltásával.” [6]

A biológiai tényezők hatásának kitett munkavállalók egészségének védelméről szóló 61/1999.(XII.1.) EüM. rendelet szerint ahhoz, hogy a munkavállaló biztonságát és egészségét fenyegető kockázatot meg lehessen becsülni, továbbá a szükséges intézkedések meghatározhatók legyenek, a munkáltatónak minden olyan tevékenységnél, amely feltehetően biológiai tényezők kockázatával jár, meg kell határoznia a munkavállalókat érő expozíció jellegét, időtartamát és mértékét [7].

51/2013. (VII. 15.) EMMI rendelet „Az egészségügyi szolgáltatás keretében használt, éles vagy hegyes munkaeszközök által okozott sérülések megelőzésére, az ilyen eszközök használatából eredő kockázatok kezelésére, valamint az egészségügyi tevékenységet

végző személyek tájékoztatására és képzésére vonatkozó követelményekről" írja elő az egészségügyi intézmények számára a jogszabályban meghatározott kockázatértékelésen túl a megelőzés tervezését [8].

A preventív intézkedések, valamint a kollektív védelem kialakítása után, ha nincs elérhető, jobb megoldás, az egyén személyi védelmével kell a kockázatokat az egészséget nem veszélyeztető mértékűre csökkenteni, ezért a munkavállalókat egyéni védőeszközökkel kell ellátni.

A munkáltató alapvető feladata, hogy az elvégzett kockázatbecslés alapján meghatározza az egyéni védőeszközök juttatásának a rendjét, valamint kiválasztja a munkavállalókkal szemben fennálló kockázatok ellen védelmet nyújtó megfelelő védőeszközt.

A világ különböző munkaterületei más-más egészségi kockázatot jelenthet a munkavállalók számára. Ahogy a környezetvédelemre is, úgy a munkafolyamatok alakulására is jelentősen kihatott a modernizáció és a fejlődés, ami egyben előnyt és hátrányt is jelenthet. Előnyként hozható, hogy a technika fejlődésével biztonságosabbá váltak a munkakörnyezetek, azonban ezzel együtt új, ismeretlen kockázatok is megjelentek [9].

Az egészségkárosító tényezők leginkább a munkakörnyezetből erednek. Ezeket az ártalmakat az alábbi öt nagy csoportba sorolhatjuk:

- fizikai kóroki tényezők: zaj, rezgés, vibráció, esés, botlás, elcsúszás, áramütés, hőhatás, sugárzások
- kémiai kóroki tényezők: porok, aeroszolok, vegyi anyagok
- biológiai kóroki tényezők: baktériumok, vírusok, gombák, élősködők
- pszichoszociális kóroki tényezők: munkahelyi terhelés
- ergonómiai kóroki tényezők: vibráció, kényszer pozíció, természetellenes testtartás, pihenés/aktivitás egyensúlytalanság

A kóroki tényezők előfordulását lényegesen meghatározza az adott munkakör, a végzett munkafolyamatok, valamint a munkavégzés során használt munkaeszközök, tehát összefüggésbe hozható a munkakörnyezettel. Az egészségügyi intézményben dolgozók munkahelyi kóroki tényezőinek megoszlásának vizsgálatából megállapítható, hogy a leggyakoribb kockázati tényezők a pszichoszociális, ergonómiai és biológiai kóroki tényezők.

Az Emberi Erőforrások Minisztériuma által kiadott kézikönyv irányokat fogalmazott meg az egyéni védőeszközökkel, hulladékkezeléssel, betegek elhelyezésével, szállításával és higiéné előírásokkal kapcsolatban. Az izolációs kórtermekbe csak korlátozott számú dolgozó léphet be, és a belépési feltételekről megfelelő képzést szükséges kapniuk. Az izolációs kórtermekbe belépő munkatársak mozgását folyamatosan adminisztrálni szükséges, továbbá az izolációs kórtermekbe belépési engedéllyel rendelkező dolgozókról listát kell vezetni, hogy a dolgozók mozgása visszakövethető legyen. Az izolációs kórtermekbe való belépésre feljogosított dolgozók száma korlátozott, a kórterem ajtaját csukva kell tartani, a fertőzés többi betegre való átterjedése lehetőségének csökkentése érdekében.

MÓDSZERTAN

Kvalitatív kutatásunk Magyarország legnagyobb egészségügyi ellátó, oktató és kutató egyetem betegellátó szervezeti egységeire, azaz a klinikákra terjedt ki. Az adatgyűjtés 15 a koronavírussal fertőzött betegek ellátásában résztvevő klinika helyszíni bejárásával és

a munkavédelemmel kapcsolatos dokumentációk, utasítások, eljárásrendek és nyilvántartások áttanulmányozásával történt. A helyszíni bejárások és ellenőrzések száma meghaladta a 100 alkalmat, valamint a munkavédelmi szakami dokumentációk áttanulmányozása történt, ami 4500 oldal szakmai anyag áttekintését jelentette. Ezzel vizsgálatra kerültek a koronavírus elleni küzdelemben résztvevő munkavállalók védelmére kialakított eljárás rendek, utasítások, valamint a covid ellátó osztályokra készített munkavédelmi szakmai dokumentációk, így a kockázatértékelések, egyéni védőeszközök juttatásának rendje, továbbá a megelőzésre és a kollektív védelemre hozott intézkedések. Továbbá a bevezetett és alkalmazott protokollok megfelelősségének vizsgálata is megtörtént a koronavírus elleni küzdelemben résztvevő munkavállalók tapasztalatainak felmérésével. A felmérések a helyszíni bejárások alkalmával történtek meg a covid osztályon dolgozó munkavállalók kikérdezésével.

KÖVETKEZTETÉSEK

A munkavédelmi szakterületet nagy hangsúllyal érintette a koronavírus járvány. A munkabiztonsági szakmai feladatok ellátását a szakterületet érintő jogszabályok mentén szükséges végezni, ami egy nagyon részletesen szabályozott szegmens.

Kockázatok azonosítása és értékelése

A munkavédelem egyik fő feladata a kockázatértékelések és a kapcsolódó munkavédelmi dokumentumok, munkautasítások elkészítése a koronavírussal fertőzött betegeket ellátó szervezeti egységek részére. A munkahelyen jelenlévő biológiai kóroki tényezők kockázatával járó tevékenységek természetesen eddig is jelen voltak, de újra kellett értékelni a minőségi és mennyiségi kockázatokat, és a korábbinál jóval szigorúbb intézkedéseket kellett meghatározni tekintettel a COVID-19 tulajdonságaira, illetve a kapcsolódó tevékenységek megváltozására. Így azokon a munkahelyeken, ahol az új koronavírussal fertőzött betegek ellátását kezdték meg, a korábban kidolgozott kockázatértékelések és kapcsolódó utasítások felülvizsgálatára volt szükség, illetve az újonnan létrehozott COVID osztályok komplett dokumentációjának összeállítására. Kidolgozásra került egy COVID specifikus kockázatértékelés - mely magában foglalja a munkahelyi-biológiai-kémiai-pszichoszociális kockázatok értékelését –, és ez alapján kerültek elkészítésre a dokumentumok. A kockázatértékelések felülvizsgálata a klinikákkal, a kórházhigiénés és a foglalkozás-egészségügyi szakterületekkel együttműködve kerültek elkészítésre.

Megelőzés - prevenció

A koronavírus első hullám kezdetén információs, és tájékoztató plakátok készítése történt a munkavállalók számára, nem csak az egyéni védőeszközök kapcsán, hanem a megelőzés további lehetőségeiről is, így a kézhigiéné fontosságáról, a távolságtartásról, és a további általános magatartási szabályokról.

A pandémia kezdetén hatósági állásfoglalás alapján meghatározásra került a Covid -19 hulladékok csomagolásának, kezelésének, az eddigieknél szigorúbb szabályai. A speciális egészségügyi - fertőző hulladék a pandémia alatt hozzávetőlegesen a háromszorosára növekedett, így a megváltozott igények miatt soron kívüli oktatások és tájékoztatások ke-

rültek megszervezésre az érintett szervezeti egységek részére a koronavírussal fertőzött hulladékok kezeléséről a munkabalesetek és foglalkozás-egészségügyi megbetegedések megelőzése érdekében.

Kollektív védelem

A koronavírus ellátó területeknél, ahol közvetlenül a betegellátást végzik, ott három zóna került kialakításra:

- teljesen szeparált vörös zóna,
- szürke zóna és
- zöld zóna.

A vörös zónában a koronavírussal igazoltan fertőzött betegek ellátása zajlik, a szürke zóna a vörös és zöld zóna közötti területet választja el vagyis átmeneti zónaként funkciónál, míg a zöld zónában a koronavírussal igazoltan nem fertőzött betegek ellátása történik. A zóna kialakítása a betegek védelme mellett az egészségügyi és egészségügyben dolgozók kollektív védelmét is ellátja, hiszen a fertőző betegek elkülönítésével csökkenti a fertőzés kockázatát, továbbá az egyéni védőeszközök viseléséből származó fizikai terhelést is. A Covid ellátó osztályok kialakításával egyidőben megkezdődött az egészségügyi megfigyelő kamerák telepítése is, a kamerák a vörös zónákba kerültek elhelyezésre, hogy az ott fekvő betegeket 24 órában meg lehessen figyelni a biztonságos szürke és zöld zónákból. Így az orvosi és ápolói személyzet kockázata a fertőzéssel szemben csökkenthető, ezzel elősegítve a kollektív védelmet.

Az egészségügyi terület zónás kialakításával kapcsolatban tűzvédelmi feladatok is szükségessé váltak, a kialakítási folyamatokat néhány esetben olyan átalakítások kísértek, melyek befolyásolták az épületrész tűzvédelemi előírásait, így ezeken a területeken módosítani kellett a menekülési utak jelzéseit, a tűzriadó tervet, illetve új kézi tűzoltó berendezések kihelyezéséről kellett gondoskodni.

A rendszeresen megtartásra kerülő, új belépő munkavállalók részére szervezett kötelező oktatások – ADR, környezetvédelem, polgári védelem, vagyonvédelem, munkavédelem, tűzvédelem, infekciókontroll témakörökben – valamint a kötelezően előírt éves ismétlődő oktatások átszervezésre kerültek. A képzések hibrid megoldással, azaz személyesen és online formában is meghallgathatók, illetve csak online formában. Ennek eredményeként a személyes jelenlét csökkenthetővé vált, amely a fertőzés átadásának lehetőségét szintén csökkentette.

Egyéni védőeszközök

A járvány kezdetén sarkalatos kérdés volt az egyéni védőeszközök használata, és ezen belül is a légzésvédők használatával kapcsolatos félreértések eloszlatása, a helyes használat oktatása, és a szabványos eszközök kiválasztásának segítése. Információs anyagok kerültek összeállításra a légzésvédőkkel kapcsolatban, melyben részletesen ismertettük a részsecskeszűrő félálarcok típusait, szabályos használatát, fel- és levételének módját, és hogy egy ilyen típusú egyéni védőeszköz milyen kockázatokkal szemben véd, és miben különbözik például a sebészeti maszkoktól. Kezdetben nagy energiákat kellett fektetni abba, hogy a megfelelő - komfortos, szabványos és biztonságos- egyéni védőeszközök kiválasztása történjen meg, azóta is folyamatosan ellenőrzésre kerül, hogy a beszerezni kívánt

egyéni védőeszközök a vonatkozó szabványoknak megfelelnek-e. A megnövekedett védőeszköz használat miatt a veszélyes hulladékok mennyisége is ugrásszerűen megnőtt, így a környezetvédelmi szakterületnek elsődleges feladata volt ezen hulladékok megfelelő gyűjtésének, kezelésének és elkülönítésének megszervezése.

Célellenőrzések

Szintén az első feladatok közé tartozott, hogy a betegellátást végző szervezeti egységeknél a COVID specifikus célellenőrzések megtartásra kerüljenek, a különböző betegzónák (triage-ok) területén szükséges munkavédelmi szabályok kialakításával, és szakmai tanácsadással igyekeztünk az ott dolgozók munkáját segíteni az egészséget nem veszélyeztető és biztonságos munkakörnyezet megteremtésében.

KÖVETKEZTETÉSEK, JAVASLATOK

A koronavírus elleni küzdelemben résztvevő munkavállalók védelmére kialakított eljárás rendek, utasítások, valamint a covid ellátó osztályokra készített munkavédelmi szakmai dokumentációk kerültek elkészítésre, mint például a kockázatértékelések, az egyéni védőeszközök juttatásának rendje, valamint a foglalkozás-egészségügyi vizsgálatok rendje. Továbbá a megelőzésre és a kollektív védelemre vonatkozóan a munkáltatók intézkedéseket hoztak meg a munkavédelmi szakterület bevonásával. A pandémia elleni védekezés részeként létrejött új eljárás rendek, utasítások, szakmai dokumentációk megerősítették, hogy az egészségügyi területen dolgozó munkavállalókat érő kockázatok komplexek és a kockázatok eredményes feltárásához és szükséges munkaáltatói intézkedések meghatározásához a munkabiztonsági, munkaegészségügyi és a munkahigiéné szakterületeknek együtt, egymásra támaszkodva szükséges ellátniuk a szaktevékenységüket.

ÖSSZEFOGLALÁS

A pandémia a kiszámíthatatlan változások és a kihívások időszaka volt, sok új megoldás látott napvilágot, melyeket a járvány kényszerített ki. Az egyik lényeges tapasztalat, hogy jelentősen növekedett a munkavédelmi tudatosság a munkavállalókban, ez kitűnik a munkavállalói visszajelzésekből, a szakterületet érintő megkeresésekből, a bejárásokon tapasztalt pozitív változásokból, amely az egyéni védőeszközök szabályos, következetes használatában mutatkozik meg.

A koronavírus elleni küzdelemben résztvevő munkavállalók védelmére hozott megelőző, egyéni és kollektív védelmi lehetőségek feltátárása és alkalmazása megtörtént. Előtérbe került az egyén fellelősége, a személyes példamutatás fontossága, a fegyelmezett magatartás. Ennek a szemléletnek a munkavédelem területén különösen nagy szerepe van, ami sok esetben alul értékelt volt ezidáig. A pandémia arra is emlékeztetett bennünket, hogy a munkavédelem legfontosabb eszközét a megelőzést, valamint a kockázatok értékelését komolyan kell venni.

FELHASZNÁLT IRODALOM

[1] J. Köllő and B. Reizer, "A koronavírus-járvány első hullámának hatása a foglalkoztatásra és a vállalatok árbevételére," Közgazdasági Szemle., vol. LXCIII., pp. 345–374, 2021.

[2] Faragó Ferenc, “COVID-19 és munkavédelem Magyarországon működő vállalatok koronavírus-járvány elleni védekezési gyakorlatának kvantitatív felmérése,” Bánki Közlemények, vol. 3, no. 4, pp. 113–131, 2021.
[3] Jurányi R., Gubicza S., Munka- és tűzvédelem, akadémiai kiadó, 2020, ISBN 978 963 454 512 5
[4] ISO, “ISO/PAS 45005:2020 Occupational health and safety management — General guidelines for safe working during the COVID-19 pandemic.” https://www.iso.org/standard/64286.html (accessed May. 13, 2022)
[5] ISO, “ISO 45001:2018 Munkahelyi egészségvédelmi és biztonsági irányítási rendszerek (MEBIR).” http://szabvanykonyvtar.mszt.hu/ (Hivatkozva: 2022. 05. 14.)
[6] Szabó Gyula, “A munkavédelemi kockázatkezelés sajátosságai,” Bánki Közlemények, vol. 3, no. 1, pp. 5–12, 2020.
[7] 61/1999. (XII. 1.) EüM rendelet a biológiai tényezők hatásának kitett munkavállalók egészségének védelméről
[8] 51/2013. (VII. 15.) EMMI rendelet az egészségügyi szolgáltatás keretében használt, éles vagy hegyes munkaeszközök által okozott sérülések megelőzésére, az ilyen eszközök használatából eredő kockázatok kezelésére, valamint az egészségügyi tevékenységet végző személyek tájékoztatására és képzésére vonatkozó követelményekről
[9] Grónai É., Kapás Zs., Plette R., Munkaegészségügy, Complex Kiadó, 2009, ISBN 978 963 295 01 7
[10] Emberi Erőforrások Minisztériuma: A 2020. évben azonosított új koronavírus (SARS-CoV-2) okozta fertőzések (COVID-19) megelőzésének és terápiájának kézikönyve chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://koronavirus.gov.hu/sites/default/files/sites/default/files/imce/magyar_koronavirus_kezikonyv.pdf, 2020. (Hivatkozva: 2022. 05. 14.)

RISK MANAGEMENT IN CASE OF MONOCRYSTALLINE SOLAR POWER PLANT USING RISK ASSESSMENT MATRIX

KOCKÁZATKEZELÉS MONOKRISTÁLYOS NAPELEMES ERŐMŰ ESETÉN KOCKÁZATI MÁTRIX ALKALMAZÁSÁVAL

RÁCZ Ervin[1]

Abstract

Solar panels and solar power plants are quite widespread and play an important role in renewable electricity generation. Examining the global solar cell market, the monocrystalline solar cells occur for the most part. It is important to consider the upcoming risks involved before strating installation work and during operation. The basic purpose of risk management is to protect the condition of assets and reduce the likelihood of loss, thereby increasing the efficiency of the system. After identifying the risks, the areas that require more attention to maintain safe operation are identified. Nevertheless, it makes it easier to develop a risk mitigation strategy after realizing the risks. Taking into consideration that the monocrytalline solar cell has high dominance in the domestic and international solar market, it is important to examine the possible risks of a monocrystalline solar power plant in general and the possbile motogation strategy for high risks are considered.

Keywords

Solar cell, monocrystalline solar cell, risk management, risk assessment matrix, mitigation strategies

Absztrakt

A napelemek és a napelem erőművek elég széles körben elterjedtek, valamint fontos szerepet játszanak a megújuló villamosenergia-termelés területén. A globális napelem piacot vizsgálva a legnagyobb részt a monokristályos napelemek alkotják. A telepítési munkálatok megkezdése előtt és az üzemelés során fontos figyelembe venni a fellépő kockázatokat. A kockázatkezelés alapvető célja, hogy az eszközök állapotát megóvja és csökkentse a kiesés valószínűségét, ezzel növelve a rendszer hatékonyságát. A kockázatok feltárását követően meghatározom, hogy melyek azok a területek, melyek a biztonságos üzemelés fenntartása érdekében nagyobb odafigyelést igényelnek. Mindazonáltal, a kockázat realizálását követve könnyebb kidolgozni egy kockázatcsökkentési stratégiát. Tekintettel arra, hogy a monokristályos napelemek nagy dominanciát mutatnak a hazai és nemzetközi napelem piacon, fontosnak tartom megvizsgálni, hogy a monokristályos naperőmű esetén általánosságban milyen kockázatok léphetnek fel, illetve a magas kockázatok esetén milyen lehetséges enyhítő stratégiát lehet alkalmazni.

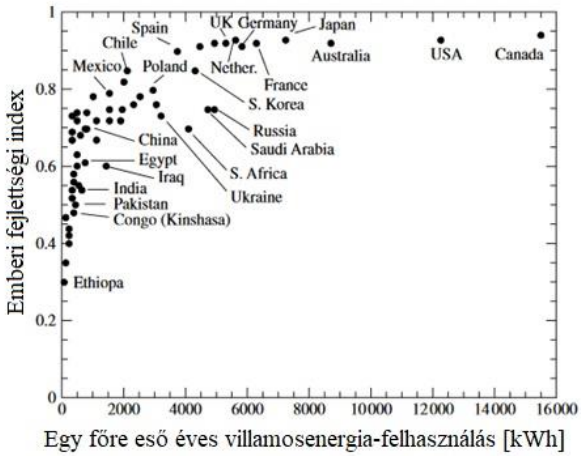
Kulcsszavak

Napelem, monokristályos napelem, kockázatkezelés, kockázati mátrix, enyhítő stratégia

[1] racz@uni-obuda.hu | ORCID: 0000-0002-7692-1397 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem

BEVEZETŐ

Az emberiség energiafogyasztásának igénye az utóbbi időben drámaian megnőtt. Az egy főre eső éves villamosenergia-fogyasztást a kutatók évente mérik és összehasonlítják, szembe állítják ezen értékeket országosan az emberi fejlettségi indexszel (angolul: Human Development Index, rövidítve: HDI). Ezáltal egy átfogó képet kaphatunk a villamosenergia-fogyasztás és az emberiség kapcsolatáról. Az 1. ábra egy 2000-es években készült HDI felmérést szemléltet, amelyet 60 országot, a Föld népességének 90%-át foglalja magába. Az emberi fejlettségi index három összetevőből – úgy, mint a születéskor várható élettartam, oktatásban megszerzett tudás és egy főre jutó vásáslóerő paritáson számított bruttó hazai termék (GDP) – kalkulált érték, amely 0 és 1 közötti értéket vehet fel [1]. Annak érdekében, hogy az életszínvonalat fejleszteni lehessen sok országban szükséges, hogy az éves energiafogyasztás százról néhány ezer kilowattórára megnövekedjen [1]. Többször felmerül a kérdés, hogyan lehet ezen igényt teljesíteni?



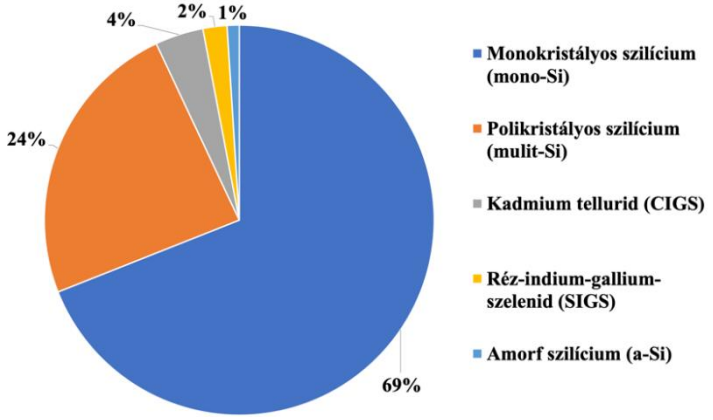
1. Ábra: Emberi fejlettségi index (angolul: Human Development Index, rovidítve: HDI) és egy főre eső éves villamosenergia-felhasználás kapcsolata országokra lebontva egy 2000-években készült felmérés alapján [1].

A korábbi évtizedekben domináns szerepet betöltő fosszilis energiahordozók égetésén alapuló villamosenergia-rendszerek a mai szempontból környezetkárosítónak minősülnek. A fosszilis energiahordozók elégetése üvegházhatású gázok (többek között szén-dioxid (CO_2)) kibocsátásával jár, mely a környezetre és az emberre káros hatással van. Figyelembe véve Magyarország 2018-as CO_2 kibocsátást elmondható, hogy 46,16% földgáz, 38,05% olaj és 19,93% szénégetésből származott. Bizonyos felmérések szerint a mai napig vezető szén-dioxid termelők hazánkban az energiaszektor, ami 72% a teljes kibocsátásunknak [2].

Számos más energiahordozó alternatíva létezik, amelyek tiszta, folyamatos és megújuló energiát jelentenek úgy, mint a nap-, szél-, víz-, biomassza és geotermikus energia. A megújuló energiaforrások világviszonylatban nagy figyelmet kapnak, azon belül is érdemes kiemelni a napelemet, amely a beeső fényt villamos energiává alakítja. A megújuló energiaforrásokat villamos energiává alakító eszközök működésük közben nem, vagy minimális károsanyag kibocsátással járnak, amely például a felület tisztán tartása során merülhet fel

[3]. Egyes adatok szerint 2014-ben a szén, mint energiaforrás volt a legmeghatározóbb villamosenergia-termelés tekintetében (39%), majd ezt követte a megújuló energiák (23%-al). Egyes prognózisok szerint a megújuló energiák várhatóan 2030 körül megelőzik a szenet, ezzel a legnagyobb energiaforrássá válnak, és 2040-re elérik a teljes energiatermelés 34%-át. A napenergia különösen azáltal, hogy költségei szempontjából versenyképesebb szintet ér el más energiaforrássokkal, a fejlődő országok hátrányos helyzetű emberek millióinak életét tudná fenntartani. Néhány piaci elemző szerint 2050-re a napelem használata 25%-ot is elérheti a villamosenergia-termelésben. Ezen meglátásmódot alátámasztja, hogy a napelemes rendszerek ára az elmúlt öt évben 50%-ot csökkent [4].

A 2. ábra szemlélteti, hogy 2015-ben melyek voltak azon napelem típusok, amelyek a világpiacon a leginkább megtalálhatók voltak. Jól látszik az ábráról, hogy a monokristályos napelem 69%-al, a polkristályos napelem 24%-al vett részt a világpiacon [4] [5].



2. Ábra: Globális napelem piacon található napelemek típusok eloszlása 2015-ös adatok alapján [4].

A napelemek üzemelése során számos kockázat léphet fel, melyeket még a telepítési munkálatok előtt célszerű felmérni és realizálni. A kockázatkezelés alapvető célja, hogy az eszközök állapotát megóvja és csökkentse a kiesés valószínűségét, ezzel növelve a rendszer hatékonyságát. A kockázatok feltárását követően meghatározzák, hogy melyek azok a területek, melyek a biztonságos üzemelés fenntartása érdekében nagyobb odafigyelést igényelnek. Mindazonáltal, a kockázat realizálását követve könnyebb kidolgozni egy kockázatcsökkentési stratégiát. *Tekintettel arra, hogy a monokristályos napelemek nagy dominanciát mutatnak a hazai és nemzetközi napelem piacon, fontosnak tartom megvizsgálni, hogy a monokristályos naperőmű esetén, általánosságban milyen kockázatok léphetnek fel, illetve a magas kockázatok esetén milyen lehetséges enyhítő stratégiát lehet alkalmazni.*

A témában már számos publikáció született, melyek során hasonló eredmények találhatók. Mindazonáltal ezen publikációk közül néhányat kiemelek. Sreenath és társai egy kockázati mátrix tanulmányt mutattak be, mely a reptéren telepített napelem rendszer lehetséges kockázatait térképezték fel, majd a magas kockázatok esetén enyhítő stratégiát javasoltak. Munkájukból kiderül, hogy 7 típusú veszély lép fel a reptér területére telepített napelemek esetén. A legmagasabb kockázatokat a káprázás előfordulása, a madarak becsapódása és a kommunikációs technológiával való interferencia okozta. A magas kockázatokra olyan enyhítő stratégiákat javasoltak, mint az előzetes káprázás-értékelés felmérése a hely-

színen, madarak jelenlétének monitorozása monitoring program segítségével és a napelemek megfelelő távolságra helyezése a kommunikációs eszközöktől [6]. Zhang és társai munkája tárgyalja a kínai megújuló energiafejlesztés főbb kockázatait és néhány szakpolitikai intézkedést javasolnak a kockázatkezelésre. Munkájukban pénzügyi kockázatokat, piacra lépés kockázatokat és technológiai kockázatok mutatnak be [7]. Kwak és társai a fotovoltaikus technológiák környezeti kockázatait vizsgálták. A munkájukban a napelemek felületéről lecsorgó víz környezeti hatásaira összepontosítottak kifejezetten a perovszkit napelemek esetén [8].

KOCKÁZATOK AZONOSÍTÁSA

A kockázati mátrix (angolul: Risk Assessment Matrix, rövidítve: RAM) egy kvalitatív kockázatértékelési eszköz, melynek nagy előnye, hogy áttekinthetővé válik a kockázathoz tartozó következmény súlyossága, és így a nem elfogadható kockázatok megfelelően azonosíthatók. Ezzel szemben a RAM hátránya, hogy egy szubjektív módszer, és az esemény bekövetkezésének valószínűségéhez megfelelő kategóriákat kell rendelni úgy, mint a bizonyos, valószínű, lehetséges, valószínűtlen és kivételes - fogalmak. Ugyancsak, a függőleges tengelyen lévő következmény súlyosságának mértéke is szubjektív következményi skálát alkot, melyek a katasztrofális, kritikus, jelentős, jelentéktelen és elhanyagolható súlyosságok. A kockázatok azonosítását követően a felmerülő kockázatokat a fentebb említett táblázatba, mátrixba helyezzük el annak alapján, hogy milyen kockázati súlyosságot és kockázati valószínűséget rendelünk az adott kockázathoz.

Kockázat súlyossága	**Kockázat valószínűsége**				
	Kivételes (1)	Valószínűtlen (2)	Lehetséges (3)	Valószínű (4)	Bizonyos (5)
Katasztrofális (A)	A1	A2	A3	A4	A5
Kritikus (B)	B1	B2	B3	B4	B5
Jelentős (C)	C1	C2	C3	C4	C5
Jelentéktelen (D)	D1	D2	D3	D4	D5
Elhanyagolható (E)	E1	E2	E3	E4	E5

1. Táblázat: Kockázati mátrix szín zónákkal való jelölése, ahol a zöld szín az elfogadható tartományt, a sárga szín az elfogadható egy bizonyos ideig tartomány és a piros szín a nem elfogadható tartományt jelöli.

Az így kapott táblázatot színkódolással látjuk el, amelyek a zöld, a sárga és a piros. A zöld színkódolás esetén a kockázat elfogadható tartományban van és nincs szükség beavatkozásra vagy enyhítő javaslatokra. A zöld színű tartományba eső kockázati indexek a C1, D2, D3, E1, E2, E3, E4. A sárga színkódolás felülvizsgálat után és/vagy korlátozott ideig elfogadható, a kockázati indexek az A1, A2, B1, B2, B3, C2, C3, C4, D3, D4, D5, E5.

A vörös tartományban (A3, A4, A5, B4, B5, C5) a nem elfogadható kockázatokat jelenti, ebben az ebestben feltétlenül szükséges enyhítő stratégiát javasolni.

Lehetséges kockázatok azonosítása

Ebben az alfejezetben a lehetséges kockázatok kerülnek azonosításra, amelyek a nem fizikai kockázatok, mechanikai kockázatok, környezeti kockázatok és elektromos kockázatok.

Nem fizikai kockázat

- Napelem modulok felületeinek ragyogása: A napelemek felületét egy reflexió csökkentő réteggel vonják be, de még így is előfordulhat, hogy a napelemek felületét ért beeső fény hatására a napelemek csillognak, ragyognak, amely kellemetlen hatást kelthet az emberek, madarak számára. Kifejezetten akkor érdemes számolni ezzel a kockázattal, ha a napelemerőművet lakott területek közelébe telepítették. Tekintettel arra, hogy a ragyogás, csillogás jelensége nem csak napelemek esetén fordulhat elő, hanem háztetőknél, ablakoknál is, e jelenség emberre gyakorolt hatása nem szignifikáns, elhanyagolható. A napelem üvegének reflexiója 2 – 4%. A korábbi kutatási eredmények szerint a legtöbb napelem lényegesen kevesebb fényt ver vissza, mint a lapos víz [9].
- Kommunikációs rendszerrel való interferencia: Egyes irodalmakban megemlítik az interferencia jelenséget a napelemek esetén, de ezzel akkor érdemes számolni, ha rendkívül érzékeny helyre telepítik a napelemeket, például a repülőtér közvetlen környezetébe. Sreenath és társai ebben az esetben magas kockázati indexet realizáltak és enyhítő stratégiaként a kommunikációs rendszerektől való nagyobb telepítési távolságot javasolták [6].

Fizikai (mechanikai) kockázat

- Komponensek öregedése: Az újonnan megvásárolt napelemek esetén a telepítést követve a gyártói garancia általában 20-25 év közé esik a tapasztalati értékek alapján. A hazánkat is erősen érintő klimatikus változások (pl.: gyakoribbá váló forró napok) a napelemek nagyobb mértékű, a korábbi évtizedekhez képest nagyobb intenzitású öregedéséhez vezethet. A telepítés során szükséges kiválasztani a napelem telepítésének lokációját, tájolását. A háztetőre szerelt napelem esetén a panel hőmérséklete meghaladhatja a $60\ °C$-ot, míg a szabadon álló napelem panelok panel hőmérséklete nem haladja meg az $50\ °C$-ot [10].
- Napelem panelek rögzítésről való leválása: A korábban említett különböző időjárási környezetnek kitett napelemek esetén a napelemek az alumínium szerkezetről leválhatnak, betörhetnek. A fizikai kockázatok nagyobb valószínűséggel történnek meg, ha a napelemek külső tényezőknek jobban kitettek. Ilyen külső tényezők a korábban említett szélsőséges időjárási viszonyok, illetve behatolás. Ezért is az esetek legnagyobb részében külső kerítéssel látják el a napelem farmokat, hogy illetéktelen behatolás minél kisebb valószínűséggel tudjon megtörténni.

Környezeti kockázat

- Madárcsapások: A madarak előfordulási valószínűsége kellően magas lehet a napelemek körül. A madarak jelenléte akkor jelentős, ha van pihenőhely, például fák

árnyéka, és élelmiszerek állnak rendelkezésre, például rovarok, élelmiszer-hulladék. A madarak egyre több helyen fordulnak elő pl.: parkolóházakban, épületek körül, utcákon, amely egy nem kívánatos jelenség több szempontból is. A napelemek védelmére már fejlesztettek olyan megoldásokat, amelyek a madaraktól való megóvást erősítik úgy, hogy a napelem felületét ne sértse meg. Ilyen megoldás látható az alsó 3. ábrán, de ilyen megoldás a madártüske (madarak elleni tüskesor) is.

3. Ábra: Napelem panel madáscsapásoktól való megóvására egy lehetsége megoldás, ahol a napelem alumínium keretére erősített drótszerű anyaggal körbekerítik a napelemet, ezzel meggátolva, hogy madarak (pl.: galamb) rakjon fészket a napelem alá [forrás: https://www.easypestsupplies.com.au/solar-panel-bird-mesh-kit].

- Területi elhelyezkedés: A heves széllökésekkel járó viharok gyakorisága megnövekedett az elmúlt időszakban és különösen a széllökésekkel járó fák kidőlése egyre többször fordul elő. Ezen jelenség a napelem felületének betörését, a tartószerkezeti egységek tönkre tevését és más súlyos problémákat eredményezhet. Megfelelő védekezési lehetőséget biztosíthat az időszakos karbantartás.

4. Ábra: Napelem panelek tűzkitörés utáni leégett állapotban [6].

Elektromos kockázat

- Elektromos tűzeset: A napelem panelok túlterhelése és rövidzárlata tűzkitörést eredményezhet, de ez ritkán fordul elő, mivel a szabványok ezen pontokat jól kezelik.

EREDMÉNYEK ELEMZÉSE

A kockázatok azonosítását követve a kockázatok kockázati valószínűségének és kockázati súlyosságának meghatározása a következő lépés. A 2. táblázat tartalmazza az egyes azonosított kockázatokhoz rendelt kockázat valószínűséget és kockázat súlyosságot.

Azonosított kockázat	Kockázat valószínűsége	Kockázat súlyossága	Kockázati index
Napelem felületének ragyogása	Valószínű	Jelentéktelen	D3
Kommunikációs rendszerrel való interferencia	Valószínűtlen	Jelentéktelen	D2
Komponensek öregedése	Valószínűtlen	Jelentéktelen	D2
Napelem panelek rögzítésről való leválása	Valószínűtlen	Jelentős	C2
Madárcsapások	Lehetséges	Jelentős	C3
Területi elhelyezkedés	Valószínűtlen	Jelentős	C2
Elektromos tűzeset	Valószínűtlen	Kritikus	B2

2. Táblázat: Az egyes azonosított kockázatokhoz rendelt kockázati valószínűséget és kockázati súlyosságot összefoglaló táblázat kockázati indexel ellátva.

A 2. táblázat utolsó oszlopában a kockázati indexek szerepelnek, amely alapján a végleges kockázati mátrix elkészült. A 3. táblázat a 2. táblázat alapján kapott kockázati indexeket tartalmazza.

Kockázat súlyossága	Kockázat valószínűsége				
	Kivételes (1)	Valószínűtlen (2)	Lehetséges (3)	Valószínű (4)	Bizonyos (5)
Katasztrofális (A)					
Kritikus (B)		B2			
Jelentős (C)		C2	C3		
Jelentéktelen (D)		D2	D3		
Elhanyagolható (E)					

3. Táblázat: A 2. táblázat alapján elkészített kockázati mátrix, feltűntetve az azonosított kockázatokhoz rendelt kockázati indexet.

A 2. és 3. táblázatokból kiderül, hogy piros mezőbe, pontosabban, elfogadhatatlan tartományba eső kockázat nem került azonosításra. Ezáltal azonnali enyhítő stratégiát nem szükséges javasolni. Mindezek mellett szükséges megnézni a B2, C2, C3 és D3 indexel ellátott kockázatokat, melyek a sárga zónába kerültek. Ezen sárga zónába eső azonosított kockázatok esetén az alábbi enyhítő javaslatokat lehet alkalmazni:

- A napelem felület ragyogásának mérését követően, a mérésből származó eredményektől függően válhat szükségessé a plusz antireflexiós réteg felvitele, de érdemes kihangsúlyozni, hogy a napelem felület ragyogásának kockázat súlyossága nem jelentős.
- A heves széllökésekkel járó viharok, fák kidöntése kockázatot jelenthet a napelem panelek rögzítésére. A kidőlt fák a területi elhelyezkedés hiányosságából fakadhat. Az egyre többször előforduló szélsőséges időjárási viszonyok szükségesség teszik a terület időszakos karbantartását.
- Madárcsapások ellen a fentebb bemutatott 3. ábrán látható elrendezés (madárháló) adhat sikeres védekezést a madárcsapásokkal szemben. Itt is érdemes elsőnek felmérni, hogy a madárcsapások mennyire gyakoriak, mennyi a madarak számára rendelkezésre álló pihenőhely mennyisége, illetve milyen mértékben fordulnak elő élelmiszer-hulladékok, valamint rovarok. Amennyiben ezt a kockázatot a felhasználó magasnak ítéli, a 3. ábrán bemutatott elrendezés szükségessé válik. Továbbá, érdemes lehet a madártüskék alumínium keretre való applikálása is.
- Elektromos tűzeset súlyossága kritikus, de nagyon alacsony az előfordulási valószínűsége, ha a telepítés minden egyes lépése szabályosan, a szabványokat betartva végződik. Az időszakos karbantartás megnövelheti a rendszer teljes életciklusának a szén-dioxid kibocsátását (pl.: traktorral való felület lemosás), de a nagyobb károk és üzemzavarok elkerülése érdekében szükségesség válhat. Továbbá, az időszakos karbantartás során a hőkamerával felszerelt drónnal való napelemek végig pásztázása segíti a hibadetektálást, amely megelőzheti a tűzesetet.

ÖSSZEFOGLALÁS

E cikkben a monokristályos naperőmű esetén, általánosságban fellépő kockázatokat vizsgáltam meg, azonosítottam be. Ezt követően az azonosított kockázatokhoz rendelt kockázat súlyosság és kockázat valószínűség alapján a kockázatok kockázati mátrixba kerültek beillesztésre. Összesen négy nagyobb kockázat került azonosításra, amelyek a nem fizikai-, fizikai-, környezeti- és elektromos kockázatok, melyek további felbontásra kerültek. Ezáltal hét darab kockázat – úgy, mint a napelem felületének ragyogása, kommunikációs rendszerrel való interferencia, komponensek öregedése, napelem panelok rögzítésről való leválása, madárcsapások, területi elhelyezkedés, elektromos tűzeset – részletes kifejtésre került. Az azonosítást követően a korábban felsorolt kockázatok kockázati mátrixba való beillesztése történt meg. A piros, elfogadhatatlan mezőbe nem került azonosításra kockázat. A sárga zónába eső azonosított kockázatok esetén enyhítő javaslatok kerültek kidolgozásra. A munkából látható, hogy az alkalmazott szubjektív módszer jónak bizonyul a kockázatkezelésre. A kockázatkezelés alapvető célját megfelelően kielégítő, vagyis az eszközök állapotának megóvását, és a kiesés valószínűségének csökkentését segíti elő. Mindazonáltal a módszer multidiszciplináris, vagyis elég széles területen is alkalmazható.

FELHASZNÁLT IRODALOM

[1] A. Luque and S. Hegedus, Eds., *Handbook of photovoltaic science and engineering*. Hoboken, NJ: Wiley, 2003.
[2] R. B. Jackson *et al.*, ‘Global energy growth is outpacing decarbonization’, *Environ.*

Res. Lett., vol. 13, no. 12, p. 120401, Dec. 2018, doi: 10.1088/1748-9326/aaf303.

[3] A. K. Pandey, V. V. Tyagi, J. A. Selvaraj, N. A. Rahim, and S. K. Tyagi, 'Recent advances in solar photovoltaic systems for emerging trends and advanced applications', *Renewable and Sustainable Energy Reviews*, vol. 53, pp. 859–884, Jan. 2016, doi: 10.1016/j.rser.2015.09.043.

[4] M. Malinowski, J. I. Leon, and H. Abu-Rub, 'Solar Photovoltaic and Thermal Energy Systems: Current Technology and Future Trends', vol. 105, no. 11, pp. 2132–2146, Nov. 2017, doi: 10.1109/JPROC.2017.2690343.

[5] E. Martinot, A. Chaurey, D. Lew, J. R. Moreira, and N. Wamukonya, 'Renewable Energy Markets in Developing Countries', *Annu. Rev. Energy. Environ.*, vol. 27, no. 1, pp. 309–348, Nov. 2002, doi: 10.1146/annurev.energy.27.122001.083444.

[6] S. Sreenath, K. Sudhakar, and A. F. Yusop, 'Solar photovoltaics in airport: Risk assessment and mitigation strategies', *Environmental Impact Assessment Review*, vol. 84, p. 106418, Sep. 2020, doi: 10.1016/j.eiar.2020.106418.

[7] X. Zhang, W. Ruoshui, H. Molin, and E. Martinot, 'A study of the role played by renewable energies in China's sustainable energy supply', *Energy*, vol. 35, no. 11, pp. 4392–4399, Nov. 2010, doi: 10.1016/j.energy.2009.05.030.

[8] J. I. Kwak, S.-H. Nam, L. Kim, and Y.-J. An, 'Potential environmental risk of solar cells: Current knowledge and future challenges', *Journal of Hazardous Materials*, vol. 392, p. 122297, Jun. 2020, doi: 10.1016/j.jhazmat.2020.122297.

[9] Y. B. Zhu, 'The Potential Hazard Analysis Method of Glare for Photovoltaic near airports or within', *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 392, p. 062148, Aug. 2018, doi: 10.1088/1757-899X/392/6/062148.

[10] V. Poulek, T. Matuška, M. Libra, E. Kachalouski, and J. Sedláček, 'Influence of increased temperature on energy production of roof integrated PV panels', *Energy and Buildings*, vol. 166, pp. 418–425, May 2018, doi: 10.1016/j.enbuild.2018.01.063.

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