ISSN 2676-9042

Vol 4, No 1, 2022.

2022, IV. évf. 1. 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
A moment of transience | **A mulandóság pillanata**
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 1, 2022. | **2022. IV. évf. 1. szám**

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

DOMJÁN András

andras.domjan@gmail.com

In terms of my qualifications, I am an electrical engineer, a certified safety engineer and a blasting engineer. I am using my knowledge in the field of counter-terrorism within the framework of the Police as the Head of Department of the Information Protection Department, and I am currently expanding my knowledge as a PhD student at the University of Óbuda Doctoral School of Security Studies. My research area is to examine the possibilities offered by the radio spectrum monitoring system to be used as part of complex establishment protection. Within this – in particular – the detection of remotely controlled IED and eavesdropping equipment based on parasitic RF radiation.

Végzettségeimet tekintve villamos mérnök, okleveles biztonságtechnikai mérnök és robbantástechnikai szakmérnök vagyok. A megszerzett ismereteimet a Rendőrség keretein belül a terrorelhárítás területén, információvédelmi osztály vezetőjeként kamatoztatom, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatójaként bővítem ismereteimet. A kutatási területem a komplex objektumvédelem részeként alkalmazásra kerülő rádióspektrum monitor rendszer nyújtotta lehetőségek vizsgálata. Ezen belül konkrétan a parazita RF-sugárzás alapján történő távvezérlésű IED-, és lehallgató berendezések detektálása.

FARAGÓ Ferenc

farago.ferenc@uni-obuda.hu

My name is Ferenc FARAGÓ, I am a certified environmental engineer, occupational safety engineer. My profession is safety: I have been working as an environmental expert for more than 20 years and I have occupational safety expert qualifications as well. I have worked primarily on developing corporate sustainability strategies for companies in Europe, the United States and the Far East. I am currently working in the management of a multinational manufacturing company as an EHS manager. I am trying to expand my knowledge at the Doctoral School on Security Sciences of the University of Óbuda. My main field of research is safety management, occupational safety performance measurement and forecasting the increase in accident risks. I am proud to be involved in the educational activities of the university, in the training of occupational safety professionals as an instructor, and as a consultant of dissertation students.

FARAGÓ Ferenc vagyok, végzettségemet tekintve okleveles környezetvédelmi mérnök, munkavédelmi szakmérnök. Hivatásom a biztonság: több, mint 20 éve dolgozom környezetvédelmi szakértőként és munkavédelmi szakértői jogosultságokkal is rendelkezem. Főként vállalati fenntarthatósági stratégiák kialakításával foglalkoztam európai, egyesült államokbeli és távolkeleti vállalatoknál. Jelenleg egy multinacionális gyártó vállalat menedzsmentjében dolgozom, mint környezetvédelmi és munkavédelmi vezető. Tudásomat az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában igyekszem bővíteni. Fő kutatási területem a biztonság menedzselése, a munkavédelmi teljesítménymérés és a baleseti kockázatok növekedésének előrejelzése. Büszke vagyok arra, hogy részt vehetek az egyetem oktatási tevékenységében, a munkavédelmi szakemberek képzésében oktatóként, illetve a szakdolgozó hallgatók konzulenseként.

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

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

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.

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.

KEMENDI Ágnes

kemendi.agnes@uni-obuda.hu

Ágnes KEMENDI holds M.Sc. degree in Economics and Dutch State Ingenieur degree. Agnes is PhD student at Doctoral School of Safety and Security Science, Óbuda University, Budapest, Hungary. Agnes has more than ten years of work experience. Her research interests include enterprise safety and security, information security, security awareness, continuous improvement mindset and the human factor in security.

Kemendi Ágnes okleveles közgazdász és holland állami mérnöki (Ing.) diplomával rendelkezik. Ágnes az Óbudai Egyetem és Biztonságtudományi Doktori Iskola PhD hallgatója. Ágnes több mint tíz éves munkatapasztalattal rendelkezik. Kutatási területei közé tartozik a vállalati biztonság, információbiztonság, biztonságtudatosság, folyamatos fejlesztési szemlélet, és az emberi tényező szerepe a biztonságban.

KISS Gábor

kiss.gabor@bgk.uni-obuda.hu

Dr. habil. Gábor KISS is associated professor and the Head of the Institute of Mechanical Engineering and Security Science at the Óbuda University. He received the PhD. degree in Mathematics and Computer Science from Debrecen University in 2013 and the Habilitation in Safety and Security Science from Óbuda University in 2020. Dr. KISS was guest scientist in the Faculty of Computer Science Freie Universität Berlin in 2003 and Universität Paderborn in 2006. Dr. KISS has published more than 180 refereed papers in Journals and Proceedings. He serves as an Editorial board member more Journals. He has been a Keynote speaker, Panelist speaker, Publicity chair, Program Committee or Organizing Committee member for more than 200 International Conferences. Dr. KISS is a member of the Hungarian Academy of Sciences, and more Hungarian and International Societies in Computer Science. Dr. KISS is an external expert of Bureau of Education, Hungary, National Research, Development and Innovation Office of Hungary and Massachusetts Institute of Technology. His research interests include computer science education, information security awareness, AI in self-driving vehicles.

Dr. habil. KISS Gábor egyetemi docens, az Óbudai Egyetem Gépészmérnöki és Biztonságtechnikai Intézetének vezetője. A Debreceni Egyetemen 2013-ban szerzett PhD fokozatot Matematika és Számítástudományból, 2020-ban pedig az Óbudai Egyetemen habilitált Katonai Műszaki Tudományból. Dr. KISS Gábor 2003-ban a Freie Universität Berlin Informatikai Karán, 2006-ban az Universität Paderborn Informatikai Karán volt vendégkutató. Több mint 180 referált tanulmány szerzője folyóiratokban és konferenciakiadványokban, valamint több folyóirat szerkesztőbizottsági tagja. Több mint 200 nemzetközi konferencián töltött be Keynote speaker, Panelist speaker, Publicity chair, Program Committee or Organizing Committee member tisztségeket. Dr. KISS Gábor tagja a Magyar Tudományos Akadémiának, valamint több magyar és nemzetközi számítástechnikai társaságnak. Dr. KISS Gábor külső szakértője az Oktatási Hivatalnak, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatalnak és a Massachusetts Institute of Technology-nak. Kutatási területe az informatikaoktatás, információbiztonság-tudatosság, mesterséges intelligencia az önvezető járművekben.

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.

MANDIĆ Dorottya

mandic.dorottya@uni-obuda.hu

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

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

MOLNÁR Albert

treblaranlom@gmail.com

I, Albert MOLNÁR, was born on June 27, 2001, in Transcarpathia, Uzhhorod. I speak English, Ukrainian and Russian at my native level. In September 2018, I started my studies on the course of technical management at the University of Óbuda at the Keleti Károly Faculty of Economics. From February 2022, although I am studying business development and at the same time doing research. During my undergraduate studies, I also participated in several TDKs and the 35th OTDs, in which I won 1 place. My research is based on the economic crisis forecasting systems of the V4 countries. In addition, I actively participate in university scientific conferences. From February 2022 I am actively assisting my colleagues and the students of the University of Óbuda in the successful publication of their work in the position of Vice-President at the Ferenc Jánossy Research community. In September 2021, I was admitted to the insurance company Aegon, where I work as a portfolio accounting intern. During my internship, I also developed my managerial and economic knowledge and gained a deep insight into economic processes.

Én, MOLNÁR Albert 2001. június 27. születtem Ungváron, Kárpátalján. Az angol, ukrán és orosz nyelvet anyanyelviszinten beszélem. 2018 szeptemberében megkezdtem tanulmányaimat az Óbudai Egyetemen a Keleti Károly Gazdasági Kar műszaki menedzsment képzésen, 2022 februárjától, pedig a vállalkozásfejlesztés szakon továbbtanulok és kutatásokat végzek. Az alapképzési tanulmányaim során számos TDK-n és a 35-ik OTDK is részt vettem, amelyiken első helyezést nyertem. Kutatásom a V4-es országok gazdasági válság előrejelzési rendszereken alapul. Ezen kívül aktívan részt veszek egyetemi tudományos konferenciákon is. 2022 februárjától a Jánossy Ferenc szakkollégiumban elnökhelyettes pozícióban aktívan segítem szaktársaimat és az Óbudai egyetem hallgatóságát a munkáik sikeres publikációjában. 2021 szeptemberében felvételt nyertem az Aegon biztosítási cégbe, ahol portfolió gyakornokként dolgozok. A szakmai gyakorlatom során a vezető és közgazdaságtani tudásaimat is fejlesztettem és egy mély betekintést nyerhettem a gazdasági folyamatokba.

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

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

and solutions for strengthening the information security of the Hungarian public administration.

információbiztonságának erősítését szolgáló eszközök, módszerek, megoldások felkutatása.

SIMON Dániel

simon.daniel277@gmail.com

I am Dániel SIMON, a student at the University of Óbuda, majoring in Business Development MSc. I like Accounting and Project Management and I plan to do my PhD in this field in the future. Besides, my research field is Technical Management, I am the Vice President of the Jánossy Ferenc Szakkollégium. I have achieved 3rd place in Vetathon technical competition.

SIMON Dániel vagyok az Óbudai Egyetem hallgatója Vállalkozásfejlesztés MSc szakon. Kedvelem a számvitelt és projektmenedzsmentet, a jövőben ebből tervezem doktorimat. Emellett a műszaki menedzsment a kutatási területem, a Jánossy Ferenc Szakkollégium alelnöke vagyok. A Vetathon műszaki versenyen 3. helyezést értem el.

SZABÓ Lajos

elnok@remok.hu

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

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

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 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.

SZABÓ László András több mint húsz éves vagyonvédelmi és mechanikus biztonságvédelmi tapasztalattal rendelkezik, saját fejlesztései, találmányai voltak. 2008 óta elmélyedt a biztonságmenedzsment területén végzettségei rendészeti igazgatásszervező biztonsági szakon, kriminológus és tudományos pályáját a Nemzeti Közszolgálati Egyetem Közigazgatástudományi Doktori Iskolájában kezdte, majd az Óbudai Egyetem Biztonságtudományi Doktori iskolájában folytatja. Kutatási területe a nemzetközi mig-

His research interests include international migration and criminal policy, as well as security management and innovation opportunities in managing migration.

ráció és a kriminálpolitika, illetve a biztonságmenedzsment és az innovációs lehetőségek a migráció kezelésében.

VARGA Zsófi

zsofivarga05@gmail.com

My name is Zsófi VARGA, I graduated as an international relations expert from Eötvös Loránd University. I have been working at the Ministry of Defence and at the Civil-military department of Hungarian Association of Military Science. The area of my research is about the cognitive dimension of Information Operations.

VARGA Zsófinak hívnak, az Eötvös Lóránd Tudományegyetemen végeztem, mint nemzetközi kapcsolatok szakértő. Jelenleg a Honvédelmi Minisztériumban, illetve a Magyar Hadtudományi Társaság Civilkatonai Szakosztályán dolgozom. Kutatási területem az információs műveletek kognitív dimenziója.

VIKTOR Patrik

viktor.patrik@uni-obuda.hu

My name is VIKTOR Patrik, I graduated as a technical manager at the University of Óbuda, and then I became a certified economist. I am currently doing my PhD. at the University of Óbuda, Graduate School of Security Sciences. I am also the President of the Jánossy Ferenc Szakkollégium and the President of the Tutorial Circle of the University of Óbuda. My research interests include self-driving vehicles, online education and renewable energy.

VIKTOR Patrik vagyok, műszaki menedzserként végeztem az Óbudai Egyetemen, majd ezután okleveles közgazdász lettem. Jelenleg az Óbudai Egyetem Biztonságtudományi doktori iskolába csinálom PhD-mat. Emellett a Jánossy Ferenc Szakkollégium elnöke vagyok és az Óbudai Egyetem Korrepetitori körének elnöke vagyok. Kutatási területeim: önvezető járművek, online oktatás és megújuló energiaforrások.

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 GyörgyBenedek, and later with Árpád "Pika" Nagy and Zoltán Sebestyén. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán Gasztonyi, from whom she learned the different techniques of oil painting. She is narrative painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött rá, hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában Benedek György festő és szobrászművésznél, majd később Nagy Árpád „Pika"-nál és Sebestyén Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere Gasztonyi Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes

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.

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 1, 2022. | **2022. IV. évf. 1. szám**

CONTENT | TARTALOM

ERGONOMIC GRIPS FROM COLD WEAPONS TO FIREARMS AND TOOLS ARE THE RESULT OF A VERY OLD DEVELOPMENT

ERGONOMIKUS MARKOLAT A HIDEGFEGYVEREKTŐL A TŰZFEGYVEREKEN ÁT A SZERSZÁMOKIG EGY NAGYON RÉGI FEJLESZTÉS EREDMÉNYEKÉNT

SZABÓ Lajos[1]

Abstract

In many cases, mankind has made tools, objects and buildings without having a precise, scientific basis for what they produce. Sometimes the results of guesswork and trial and error worked, sometimes they didn't. This paper analyses and presents a type of handle that fully meets all the current and scientific requirements of ergonomic hand tool design. It meets the requirements of hand tools and handguns developed over thousands of years ago and still used today in unchanged form. Its peculiarity is that its name, known in European languages, is known with a slant from the Hungarian original, but its meaning can only be understood in Hungarian.

Keywords

ergonomics, hand tools, cold weapons, firearms, grip, sabre

Absztrakt

Az emberiség nagyon sok esetben készített eszközöket, tárgyakat, épületeket úgy, hogy pontos, tudományos alapokkal nem rendelkezett arról, amit előállít. A találgatás, próbálgatás eredményei néha beváltak, néha nem. Ez a tanulmány egy olyan markolat-típust elemez és mutat be, ami teljesen megfelel az ergonomikus kéziszerszám tervezés minden jelen kori és tudományos követelményének. Megfelel, pedig több mint ezer éve fejlesztették ki, és mind a mai napig változatlan formában, kéziszerszámoknál és kézifegyvereknél alkalmazzák. Különlegessége, hogy az európai nyelveken ismert neve a magyar eredetiből ferdítésekkel ismert, de csak magyar nyelven értelmezhető a jelentése.

Kulcsszavak

ergonómia, kéziszerszámok, hidegfegyverek, lőfegyverek, markolat, szablya

[1] elnok@remok.hu | ORCID: 0000-0001-9375-2188 | Chairman of the Board of Trustees, Foundation for Law Enforcement and Private Security Education and Research (REMOK)| kuratóriumi elnök, Alapítvány a Rendvédelmi és Magánbiztonsági Oktatásért és Kutatásért (REMOK)

BEVEZETÉS

Ennek a munkának elsődleges célja a „Kutatók éjszakája" rendezvény sorozat 2021. évben az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán megtartott előadás tudományos munkaként való bemutatása. A rendezvény megtartása során az általános iskolai tanulóktól a felnőttekig megjelenő közönség „kiszolgálása" az elsődleges cél, ahol a megjelentek életkorától, ismereteitől függően változik az előadások tartalma.

Célom annak bemutatása, hogy a feltalálók eredményei sok esetben megelőzik a tudományt. Jelen esetben egy olyan találmány, ami több mint ezer esztendővel a tudományterület elnevezésének megszületésével és az első tudományos dolgozatok megjelenése előtt készült el. Egy olyan találmány, egy alapvetően könnyűlovassági kard-változat, ami egyedülálló a világon, de pontosan követhető az első megjelenése a legutolsó változatokig.

Külön érdekessége, hogy a szakirodalom, mely ezt vizsgálja, a legcsekélyebb érdeklődést a markolat tekintetében mutatja. Tudomásom szerint egyetlen olyan publikáció nincs, mely ergonómiai szempontból vizsgálta volna az eredeti találmányt. A markolatot mind a mai napig használjuk szerszámainkon, de a legtöbben nem ismerik az eredetét.

AZ ERGONOMIA ÉS A KÉZI SZERSZÁMOK, FEGYVEREK

Az ergonómia [1] kifejezést Wojciech Jastrzębowski alkotta meg,a görög εργον Ergon: munka és νομος Nomos: törvény szavakból, amit az 1857-ben készített könyvében publikált. A könyv címe: Rys ergonomji czyli nauki o pracy, opartej na prawdach poczerpniętych z Nauki Przyrody, magyarul; Az ergonómia, azaz a munka tudománya, a természettudományos alapokon alapuló igazságok alapján.
Az eredeti könyv akkor vált ismertté, amikor 1997-ben angol fordítással „*An outline of Ergonomics, or the Science of Work, based upon the thruts drawn fom the Science of Nature"* címen újranyomták, ami a következő azonosító számokon jelent meg: ISBN: 83-901740-9-X or ISBN: 83-87354-59-7. [2]

A világszerte dolgozó és publikáló kutatóknak majdnem több mint 100 évet kellett várniuk, mire megalakult az Ergonómiai Kutató Társaság 1949-ben (Ergonomics Research Society). Erről egy rövid közlemény jelent meg a Brit Orvosi Újság (British Medical Journal) 1950. április 29.-i számának levelezés rovatában. [3] A közleményt az Ergonómiai Kutató Társaság adta közre, azzal a céllal, hogy népszerűsítse a társaságot és tagokat, érdeklődőket toborozzon. Megtudhatjuk belőle, hogy; „*1949 júliusában emberek egy csoportja eldöntötte, hogy megalakít egy új társaságot, aminek a neve" Az ergonómiai Kutató társaság" ami ezután megalakult. Az Ergonómia a definíció szerint azt jelenti, hogy* „*Az ember és a munkakörnyezete összefüggéseinek vizsgálata", különösen az anatómiai, élettani és pszichológiai ismeretek alkalmazása az ebből eredő problémákra. Ez magában foglalja a különféleképp leírható területeit, mint „a gépek emberhez való igazítása" az embermérnökség – human engeneering – az ipari pszichológia egy része, amely nem társul szakmai útmutatással, stb. A társaság célja hogy összekapcsolja a munkásokat az alkalmazott pszichológia, fiziológia és anatómia és a mozgások vizsgálata területén.* [3]

A társaság tagjai nagy alapossággal és céltudatosan hozták létre társaságukat, az angol klub- és üzleti életben megszokott szervezeti alapokon. A cikk lényegében egy na-

gyon jól elkészített tömör hirdetés, ami nem csak a tudósokat, hanem az üzleti élet képviselőit is megszólította. Igaz, a ma megszokott hirdetések stílusától eltér, hiszen az azóta feledésbe ment „újságok levelezés rovata" stílusában íródott, ami egy nyelvészeti, irodalmi különlegesség volt. Pont ennek a stílusnak köszönhető, hogy pontosan tudjuk, kik voltak a társaság alapító tagjai, kincstárosa és titkárai, hol volt a társaság székhelye, mi a levelezési címe.

Az is nyilvánvaló csak ebből a rövid cikkből, hogy tudományos alapossággal kezdték definiálni kutatásuk célját, és magát az ergonómiát, ahogy az idézetből olvasható. A társasághoz többen csatlakoztak és a tagság szépen gyarapodott. Akik tagokká válva tanulmányokat készítettek, egyre újabb és pontosabb meghatározását adták az ergonómiának.

Csak az ezredforduló előtti, a XX. százas utolsó évtizedeiben vált széleskörűen elismert, és használt tudománnyá, melynek addigra már számos szabványa is elkészült és használatban volt. Az Ergonómiai Kutató Társaság által megfogalmazott kutatási területek: „*különösen az anatómiai, élettani és pszichológiai ismeretek"* nyitva hagyták a kaput további tudományok számára, és újabb kutatási irányokat tettek lehetővé.
Ennek következtében folyamatosan új és újabb kategorizálások készültek, melyek a kutatási irányokat és az alkalmazási területeket illették. A „*gép emberhez illesztése*"[3] már túlhaladottá vált. Egyre több területen kutattak, és publikálták eredményeiket a tudósok, aminek számos új ajánlás lett a következménye. Ezek néha igen gyorsan szabvánnyá alakultak, mindennapjaink részévé váltak. Nyilvánvaló, hogy az ipar és a technológia fejlődése, újabb eszközök újabb megoldásokat követelnek, mint például a szoftverek és azok képi megjelenítésének ergonómiája.

Megállapítható tehát, hogy mint tudomány, igen fiatalnak tekinthető. Az emberiség azonban mint nem önálló tudománnyal, már régóta foglalkozik az ergonómia által kezelt problémákkal és a történelem során követett olyan elveket, melyeket ez az új tudomány a magáénak tart.

A Berkley Egyetem Munkahelyi és Környezeti Egészség Centrum rövidített nevén COEH[2] egy szakcikket jelentetett meg arról, milyen régóta foglalkozott már az emberiség a munkahelyi balesetekkel és munkahelyi megbetegedésekkel [4]. A cikk az ergonómiához kapcsolható eseményeket, tényeket, adatokat az időszámításunk előtt 400-tól az 1980-as évekig veszi sorra. Még egy 1700-as években írt folyóiratot is bemutat, amit Bernardino Ramazzini (1633–1714) olasz orvos írt paciensei munkahelyi, foglalkozási megbetegedéseiről, amit „De Morbis Artificum," vagyis „A munkások betegségei" címmel jelentetett meg.

Egy hasonló összefoglaló cikk megjelent az Ergoweb nevű cég honlapján is [5], de természetesen magyar nyelven is megtalálhatóak ezek az információk, hiszen több egyetemi tankönyv és jegyzet [6, 7], és magyarul olvasható előadás [8] is tartalmazza.
Írásom alapvetően a kézzel történő munkavégzéshez és a szerszámok nyeléhez, fegyverek markolataihoz kapcsolódik, vagyis az ergonómia egy speciális szakterületéhez, a kézi szerszámokhoz.

[2] Center for Occupational and Environmental Health főoldala a Berkley Egyetem honlapján https://www.coeh.berkeley.edu/

A szakterületnek, amit antropometriának is neveznek, az egyik legismertebb hazai szakértője Szabó Gyula, akinek az előadásait diákjai rendszeresen „felteszik az internetre" [9], így még a laikus érdeklődők is ismereteket szerezhetnek.
Mivel, mert az említett tanár előadásai és jegyzetei sokkal szakszerűbbek és informatívabbak, mint az egy cikk bekezdésébe belefér, az ergonómiával kapcsolatos általános információkról szeretnék rátérni arra, miért alakulhatott ki az a speciális markolat típus antropometriai okokból. Az antropometria a görög antroposz: ember és a metron mérés, intézkedés szavakból származik, amit egy belga statisztikus Adolphe Quetelet[10] használt először 1835-ben készült tanulmányában, ami az átlagos ember méreteiről szólt. Külön tanulmányt érdemelne ennek a majd két évszázaddal előttünk élő statisztikusnak a munkája, és annak megértése, mi vitte rá arra, hogy számba vegye az emberi test méreteit, arányait és erről egy aprólékos és részletes kimutatást készítsen Azóta a kifejezés beépült az ergonómia mindennapi kifejezései közé, ami azt jelenti, hogy használati tárgyak méreteit az emberek átlagos méreteihez igazítják, így a legtöbb embernek ezek a szerszámok és eszközök kényelmesek lesznek. Úgyszintén az átlagos emberi mozgásokat és a különféle testhelyzetekben szokásos tartásokat is figyelembe véve, pontos méréseket végeznek a test és a végtagok optimális erőkifejtésének biztosítása érdekében, figyelemmel az alkalmazott szerszámokra és a munkavégzés tárgyára.

Ahogy Szabó Gyula írja Az ergonómia fogalma, története, területei és szemléleti kerete című előadásában, fontos a

- ***„Kialakítás a testméretek figyelembevételével***
- ***Igénybevétel csökkentése***
    - *Testhelyzetek és váltogatásuk*
    - *Izomerők*
    - *Testmozgások összhangja"* [11]

A kéziszerszámok tekintetében az alábbi szempontok azok, melyekre megtervezésük és legyártásuk során figyelnünk kell;

- Feladatra készülnek, teljesíteniük kell azt, amire készítettük.
- Mivel kéziszerszámok, könnyen kézbe vehetőnek, könnyen és kényelmesen kézben tarthatónak kell lenniük.
- Cél, hogy a lehető legkevésbé legyen fárasztó, vagy veszélyes a használatuk.
- Fontos, hogy huzamosabb használat esetén ne okozzon akut, vagy idült egészségkárosodást.

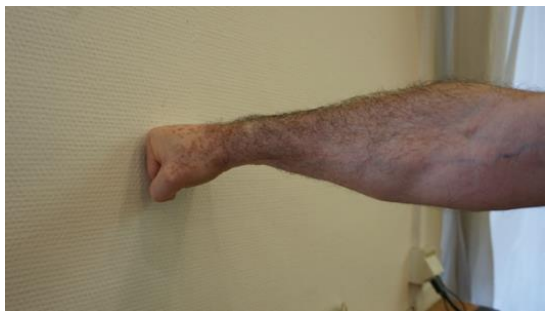
A kézi szerszámokkal végzett munka során alapvető fontosságú, hogy a kéz és kar ízületei egy vonalban legyenek, egymásra támaszkodjanak, se vízszintesen, se függőlegesen ne legyenek kitéve feszítő, vagy csavaró hatásnak. Az elsődleges cél a kar, ízületek és a kézfej helyzete a szerszám és a munkavégzés tárgya, vagyis erőkifejtés iránya vonatkozásában.

Kinyújtott kézzel végzett erőkifejtés esetén a felkar és az alkar egyik csontja egy vonalba esik, és vagy a kéztő csontjain, inain és izmain, vagy az ujjak alapízületein, az öklön érintkezünk a munkavégzés tárgyával. Az 1. számú képen a kéztő csontjaira nehezedik az erőkifejtés, mintha a tenyerünkön támaszkodnánk, az erő vonala egyenesen halad végig a felkaron, az alkar orsócsontján keresztül a kéztőcsontokig és onnan a nyélen keresztül a csavarhúzó fejéig.

1. sz. kép. saját kép.

Pontosan úgy, mint mikor ököllel megütünk valamit, vagy valakit. A japán harcművészetekben külön neve is van ennek a kéztartásnak, KENTO amit öklön támaszkodó fekvőtámaszok végzésével gyakorolnak. Ennek során a SEIKEN-nek nevezett ütőfelület edzése történik a mutató és középső ujj alapízületén, vagy a TATE-nek nevezett ütőfelületé, amikor a mutató-, gyűrűs- és kisujj alapízületén támaszkodik a gyakorlatot végző. A kézfej csontjai – pontosabban a kéztőcsontok és kézközépcsontok – egyik esetben a singcsont, másik esetben az orsócsont vonalát – a 2. és 3. számú képen – követik, annak a meghosszabbításában végeznek munkát.

2. sz. kép. saját kép



3. sz. kép. saját kép

Ha kinyújtott mutatóujjal „bökünk” meg valamit, ugyanezt az elvet követjük, mint azt a 4. számú képen láthatjuk.

4.sz. kép, saját kép.

Ha a kinyújtott karral ütés helyett szúró fegyvert használunk, a fegyver hegye, szintén a kar csontjaival egy vonalban, annak meghosszabbításaként kell működjön. hajlított kéz esetén az orsócsont, nyújtott kéz esetén a felkar- és az orsócsont meghosszabbításában. Ehhez olyan, a tenyérbe simuló nyél, vagy markolat szükséges, mely lehetővé teszi, hogy erősen lehessen megragadni, és használat közben ne csavarodjon ki a csukló, ne feszítse meg a kart, vagy az ujjakat az eszköz indokolatlan mértékben.

A főemlősökre jellemző a többi ujjal szembe fordítható hüvelykujj, amit már Brehm az Állatok Világa című művében is leírt 1863-ban. *„Itt néhány szót kell szólanunk a szembe helyezhető hüvelykujjal bíró kézről, arról a kézről, amelyről az elfogulatlan laikusnak az az érzése, hogy ezáltal lesz az ember második teremtővé, mert ez teszi őt képessé arra, hogy a természetet alkotóan utánozza."* [12] A Főemlősök alcím alatt megjegyzi a szerző, az emberre jellemző erős hüvelykujj kifejezetten megkülönböztető jegy a majomféléknél tapasztalható, jellemzően elcsökevényesedett változattól. Éppen ezért az emberi kéz, és a tenyér, sajátságai miatt külön vizsgálatot igényel a kéziszerszámok és minden kézzel is végzett munka tekintetében.

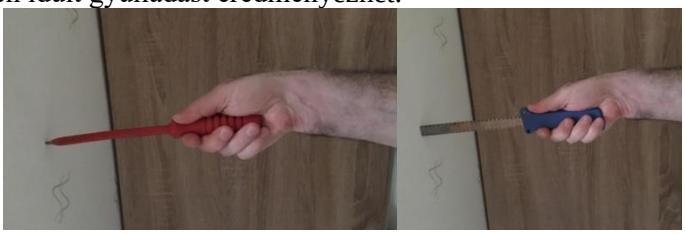
Az ember tenyerében található legnagyobb izom, a hüvelykujj hajlító izma. Mivel a tárgyakat erősen megragadni kizárólag az ujjak és a tenyér izmaival lehet, nagyon fontos, hogy a fogásnál ez a – többihez képest – hatalmas izom ne legyen gátolt, a megfogott tárgy a hüvelyk és mutató ujjak közötti térrészbe kerüljön, mivel itt lehet a legnagyobb erőt kifejteni.

Ennek az említett nagy izomnak a peremén alakul ki az a bőrredő, melyet a tenyérjósok „életvonal" néven emlegetnek, Ez a vonal körülbelül általgosan 20-25 fokos szögben indul a kinyújtott mutatóujjunkhoz képest. Ez egy speciális érték, ami antropometrikus, vagyis az emberekre jellemző adat, mint azt a továbbiakban igazolni is fogom. 5. számú kép. Amikor a hüvelykujjat behajlítjuk – vagyis ráfogunk valamire – a hajlat szöge egyre inkább a 25-35 fokos szög irányába tolódik el.

5. sz. kép saját kép.

Kétkezes, egyenes nyelű szerszámok esetén, mint például az ásó, lándzsa, , míg a támasztást, irányítást végző kéz igyekszik tartani az egyenes irányt az alkar és kézfej vonalában.

Egykezes, egyenes nyelű szerszámok esetén, mint például az egyenes nyelű csavarhúzó, fűrész, a munkát végző csuklóban kisé megtörik a kisujj irányában és feszülés jön létre a csuklóban a hüvelykujj mögött, a kézfej feszített kényszeres tartásban marad. A 6. és 7. számú képen jól látható, hogy a kézfej kényszeresen billentett tartásban van, a csukló a hüvelykujj mögött erősen feszített, ami erőltetés esetén akut, huzamosabb ilyen alkalmazás esetén idült gyulladást eredményezhet.

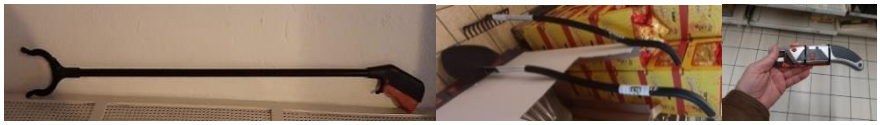


6. és 7. sz. kép saját kép.

Ha kialakítunk egy ívet a szerszám munkavégző egyenes vonalához képest egy ferde, 20 fokos ívben kezdődő és a végén 30-35 fokban végződő nyelet, akkor a szerszám egyenes, az erőt a munka tárgyára átvivő részén egyrészt maximális erőkifejtés érhető el, másrészt a szerszámot működtető kézfej, csukló nem feszül meg. Megfelel a Szabó Gyula által leírt, „*Igénybevétel csökkentése"* követelményének.

Számtalan ilyen kéziszerszámmal találkozhatunk, mivel a kéziszerszámok készítői okkal, szem előtt tartják a fentebb leírt elvnek az alkalmazását. Fel sem lehet sorolni, hogy a tudományos alapossággal megtervezett és antropometrikus és ergonomikus nyél-típus hányféle szerszámnál fordul elő.

A fűrészektől a lombvágóig, a nagyítóktól a zuhanyfejig, számtalan eszköz alkalmazkodik ehhez a hajlathoz. Közös jellemzőjük, hogy a használatuk közben, a csukló feszülése helyett, szinte egyenes csuklóval dolgozunk.



8. 9. 10. sz. képek saját képek

11. sz. kép saját kép

12. 13. sz. kép saját képek

14.15. sz. kép saját képek

16.-17 sz. kép saját képek

Nem csak a kéziszerszámoknál kerül elő ez a kifejezetten emberi tenyérre alakított nyél. Már a legkorábbi repülőgépek botkormányának markolatát is megdöntötték, és ugyanezt az ívet igyekeztek létrehozni. Ezt követték a helikopterek botkormányai, ahol már evidenciaként következett be a hüvelykujjal kényelmesen kezelhető irányítógombok elhelyezése. Mindenki pontosan tudja, akinek valamilyen számítógépes játékhoz erre az eszközre van szüksége, hogy az egyszerű, egyenes joystick kényelmetlen, bár olcsó. A kényelmesebb és ezért hatékonyabb munkát a döntött markolatú és könnyen elérhető, kezelhető gombokkal szerelt eszközzel lehet elvégezni.

Nincs olyan munkagép-kezelő, aki ne ismerné a kényelmes, ergonomikus, tenyérbe simuló, kezelőgombokkal ellátott joysticket. Az összes modern daru, markológépek, homlokrakodók, bontógépek sőt a mezőgazdasági munkagépek jelentős része is ezekkel a praktikus és ergonomikus kezelőszervekkel irányítható

A XX. században kifejlesztett személyi számítógépek fontos eleme, tartozéka az egér néven közismert eszköz, aminek jellemzője a tenyér közepén elhelyezkedő hajlatot követő domborulatba simuló íves felső kiképzés. Néhány esetben a fejlesztők tovább mentek. Annak érdekében, hogy a csukló ne törjön meg és egyenes vonalban helyezkedjen el a kézfej, kifejlesztették például a „hanyatt egér” néven ismeretes változatot, ahol a hüvelykujj közelítő izom és a hüvelykujj hajlatát követő irányító „szarvat” alakítottak ki, csakúgy, mint a joystick típusú irányító karok esetében.

De honnan származik ez a nyél típus?

A SZABLYA ÉS A SZABLYAMARKOLAT

Lehet, hogy többeknek a képek során „beugrott" a szablyamarkolat kifejezés, de tapasztalataim szerint nem olyan közismert, hogy mindenkinek eszébe jusson. Ráadásul, a szablyák sokfélesége miatt csak kevesen tudják azonosítani azt a tipikus íves hajlatot, mely az úgynevezett „honfoglalás-kori" szablyáink markolatán felismerhető. A 18. számú képen egy kézzel kovácsolt honfoglalás-kori magyar szablya replika látható. A 19. képen a markolatvég és a szíjfűző fül – a szablyát a harcos szíjjal a csuklójához rögzíthette, hogy ha a fogásból ki is szakad a markolat, legyen még egy esélye megtartani a fegyverét – látható nagyításban.

18. sz. kép. Kovácsolt, honfoglalás kori magyar szablya replika saját kép

19. sz. kép. Kovácsolt, honfoglalás kori magyar szablya replika markolat nagyítva saját kép

A szakértő olvasó számára azonnal feltűnik a markolat elnagyolt kivitelezése, hiszen a gomb nem olyan szépen gömbölyített, mint a legtöbb leleten látható és hiányoznak az ujjtámasz-veretek is. Itt, a markolat hajlatának bemutatása a cél, amire az eszköz alkalmas.

Egy olyan fegyverről van szó, amit kifejezetten a sztyeppei nomád könnyűlovasság számára fejlesztettek ki. Ez a szablya típus, hajlított markolattal, a markolatvégen gombban végződő verettel és szíjfűző füllel, ujjat támasztó veretekkel a markolaton, vagy markolatgyűrűkkel, a penge irányába előreívelő, gombokban végződő keresztvassal, a markolattal ellentétesen ívelő pengével és fokéllel rendelkezik.

Nem véletlenül írom le ilyen aprólékos részletességgel mindazokat a jellemzőket, amivel a honfoglaláskori magyar szablyák megkülönböztethetőek más korok, sőt más népek szablyáitól. A magyar szablyák markolata például fokozatosan kiegyenesedett a honfoglalást követően, csak a markolat maradt egy enyhe hajlat a kisujj felé a XIV-XV. századra, igaz, a penge íve megmaradt, de a fokél fokozatosan csökkent.

Arról, hogy pontosan mikor alakult ki ez a szablya, csak közelítő adatokkal rendelkezünk. Csiky Gergely doktori értekezésében a nem végleges, általa „protoszablya”-nak hívott fegyverekről így ír: „*A típusba tartozó pengék egyélűek, hátuk egyenes, a penge hegyénél visszaköszörüléssel egy második vágóélet alakítottak ki. Egyenes fokéles pengékkel keresztvassal ellátott és anélküli vágófegyverek egyaránt megtalálhatóak.*

Ez a típus sajátos szerepet kapott az avar kor fegyvertörténeti kutatásaiban, ugyanis az egyenes egyélű kard és a szablya közötti átmeneti típusként tartották számon. Először Szabó János Győző figyelt fel a meglétére, majd Simon László fogalmazta meg ennek a jellegzetességnek a szablya felé mutató átmeneti voltát, végül Bálint Csanád helyezte azt általános steppetörténeti keretek közé.” [13]

Azzal azonban, hogy az értekezésben, a Szablyák címszó alatt Hampel, Bóna és Bálint kutatásainak eredményeit veti össze, egy nagyon fontos információ kerül elő, az, hogy a szablyák végleges kialakulása a 7. század végére tehető.

Mint Simon László is írja az *„Adatok a szablyák kialakulásáról”* című munkájában: *„Mai tudásunk szerint az ívelt pengéjű fokéles szablyák a korai avar kori fejlődést lezáró 670/680-as újabb sztyeppéi eredetű bevándorlók kezén kerültek először a Kárpát-medencébe”* [14] Látható, hogy sok kutató egybehangzó módon jelenti ki, hogy azok a szablyák, melyek minden jellemzője megegyezik a honfoglaláskori szablyákkal, ***legalább 1200-1300 évesek!***

A Nyelv és Tudomány című internetes folyóirat 2011. március 11.-én közölt cikke „*A kaukázusi magyarokról: A honfoglalás körüli idők”* [15] címmel közöl egy képet „Szablyák innen-onnan” címmel. A közölt kép nem tartalmazza a képen látható szablyák eredetére vonatkozó adatokat, de a Torontói Cserkészek honlapján, a Lovasnépek oldalon [16] ott van a magyarázó szöveggel ellátott ábra, 19. számú kép.

20. sz. kép Szablyák innen-onnan

A kaukázusi alán és kárpátmedencei magyar néven megjelölt szablya markolata nagyon hasonló. A szaltovói alánnál, a markolattüske még egyenes, de a rátét gomb és a két ujjtüske a markolaton egyértelműen annak a jele, hogy fejlesztették a markolatot, de **CSAK** a kárpátmedencei néven jelöltnél íves a markolat!

A szaltovói és kaukázusi alán leleteket nem túl sok idő választja el egymástól, de ha csak a VIII. században készült el az első ilyen markolatú szablya, akkor is legalább

1200 éves a találmány. Egy kivételesen régi találmányról van szó! Nagy a valószínűsége annak, hogy más, ilyen régi idők óta, szinte változatlan formában használt találmány nem nagyon akad.

A Magyar Nemzeti Múzeum Honfoglaláskori gyűjteménye egyik ékessége egy Tarcalon talált aranyozott ezüst szerelékes szablya 19. számú kép.

21. sz. kép Honfoglaláskori szablya Tarcalról, Nemzeti Múzeum

A szablya egyedi, soha sehol másutt fel nem fedezett, ki nem fejlesztett kard-típus, minden változata ezekből az eredeti fejlesztésekből származik, legyen az európai, török, perzsa, indiai, vagy arab, vagy kínai. Ahogy Nagy Kálmán meghatározza a honfoglalás-kori magyar szablyát: *„A közelharc legfontosabb támadó fegyvere a 70-80 cm hosszú, ívelt, kissé hajlított szablya volt, amelynek a hegyénél a foka is élesítve volt, hogy a kardvágás utáni visszahúzásnál is sebezzen. Egyenes keresztvassal, a markolata enyhén, mintegy 20°-ra, a kard éle felé volt megdűtve”* [17]

Megállapításom szerint, a honfoglalás kori szablya különlegessége abból fakad, hogy;

a) az ergonomikus markolat eredményeképpen a lovon ülő harcos, miközben lesújtott a szablyával, mindvégig úgy tarthatta a kezében a kardot, hogy a csuklója nem feszült a kisujj irányában, mint az egyenes markolatú kardoknál,

b) az ívelt – a csukló irányába hajló – penge kétharmad részben fokkal ellátott, ami merevíti a pengét, biztos vágást lehetővé téve, míg a durván egy harmad részben kialakított úgynevezett fokél nagyobb tömeget helyezve a kard végére, növeli az ütés erejét,

c) az esetlegesen a sebzés után beszoruló penge, a fokél segítségével abban a pillanatban, hogy a lovas továbbhalad, kihasítja a sebet, a fokél irányában és kiszakad a testből. Nem rántja le a lovast, vagy rántja ki a kezéből a szablyát.

Azon ritka esetekben pedig, amikor gyalogos harcban használják, a döfés esetén szintén nem feszül meg a csukló.

A bécsi szépművészeti múzeumban elhelyezett, aranyozott és ékkövekkel díszített kovács- és ötvösművészeti műremek szablya több szempontból is különleges. Több szerző egybehangzó kutatásai arra mutatnak, hogy ez a szablya az Aba nemzetségtől származhatott, I. Endre királyunk özvegye, Anasztázia által, Ottó Bajor hercegnek ajándékba adott, és később Bécsbe került, a Kunsthistoriches Múzeumban kiállított lelet.

Az éles szemű kritikusok, mint a Lemil-blog egyik szerzője [18] azt is kifogásolják, hogy kard-ként emlegetik, holott nem is kard, hanem szablya. Nyilvánvaló, hogy egy szakértő pontos megnevezéssel szablyaként, sőt korát is pontosan megjelölve, honfoglalás-kori szablyaként azonosítja a fegyvert, hiszen egy olyan kard-típusról van szó, mely saját névvel és jellemzőkkel rendelkezik, ami megkülönbözteti minden más kardtól, mint azt tudományos munka [19], doktori értekezés [20] is leírja. A Bécsben őrzött szablyamarkolaton látható a szablya egyik leglátványosabb része, az ékkövekkel díszített mar-

kolatgyűrűk 21.sz. kép. Ezek nem öncélú díszek, hanem az ujjak támaszául szolgáltak, mint a 19. sz. képeken az ujjtüskék.

22. sz. kép. Honfoglalás kori aranyozott dísz szablya

Nagy valószínűséggel ezek a gyűrűk hordozták annak a markolat-típusnak a kezdeményét, ahol, mint a későbbi huszár-szablyák, kardok esetében, az egyenes markolattüskére épített markolat tenyér felé eső részen fém, vagy fa borítást kapott, az ujjak felé eső részen bőr, vagy textil borítást, amit vékony dróthurkokkal rögzítettek a markolathoz oly módon, hogy a drótok egy hullámos, könnyen megragadható felületet hoztak létre. A 20. sz. képen egy nehézlovassági kard markolata látható.

23. sz. kép nehézlovassági kard markolata, saját kép.

Több filmben is előkerül a szablyamarkolat. Kardként mindössze két szereplő használja a StarWars filmek egyes epizódjaiban, de aki közismertebb az Dooku gróf, az ő fénykardjának markolata a honfoglalás kori szablya markolatának mása.

Egy másik filmben, a Harry Potter több részében, Bellatrix Lestrange használ egy olyan varázspálcát, aminek szablyamarkolata van. Így egyszerűbben tudja a pálcájának a hegyét a célra irányozni, mint az egyenes markolatú varázspálcát használó mágusok. Mint látható, az ergonomikus varázspálca tökéletesen követi a tenyér hajlatait és pontosan egy irányba esik a kinyújtott, célra mutató mutatóujjal. 22. és 23. számú képek.

24.sz. kép Bökés ujjal és és 25. sz.kép bökés pálcával saját képek

A Gyűrűk Ura filmekből ismert „tünde kardok” szintén szablyamarkolatúak.

26. sz. kép a szablya és a pálca íve Pergel Áron képe

27. sz. kép a magyar szablya és Arwen kardja Pergel Áron képe

A szablyamarkolat lehetővé teszi, hogy a legtermészetesebb módon a célra tudjuk irányítani a kézben tartott eszközt. Minden bizonnyal ennek köszönhető, hogy a szablyamarkolat a lőfegyverek esetében is folytatta diadalútját. Az első pisztolyok szablyamarkolattal készültek, 28. kép.

28. sz. kép kovás pisztoly markolat, saját kép

A lőfegyverek esetében ez a gyakorlat átterjedt a korai puskákra is. A válltámasz – tusa – kifejlesztése előtti időkben a pontos célzás elősegítése érdekében ugyanolyan markolata volt a puskáknak, mint a pisztolyoknak, 29.kép.

27. sz. kép kovás puska markolat saját kép

A tusa kifejlesztése után is megmaradt a kezdeti szablya-markolatú ív ott, a tusa előtti részen, ahol a puskát megragadjuk azzal a kézzel, mely az elsütés műveletét végzi. a szablyamarkolatnak köszönhetően, a puskacső pont a mutatóujjunkkal megegyező irányba mutat, 30. és 31. számú kép.

28. sz. kép. és 29. sz. kép, szablyamarkolat a puska tusa előtt. saját kép

Tehát a korai, első lőfegyverek átvették a hidegfegyver markolatát azért, mert nyilvánvaló előnye volt a célzás érdekében. Mind a mai napig ott van a tusa előtt, hiszen ez a speciális, a kéz és a tenyér ergonómiáját figyelembe veszi. Azoknál a lőfegyvertípusoknál, melyeknél nem fontos a nagyon pontos célzás, mint a sörétes rövid csövű puskák – shotgun, lupara – jellemzően csak szablyamarkolattal rendelkeznek tusa nélkül. A szablyamarkolat tehát a mai napig használatban van, szúró-vágó, lő- és tűzfegyverek, valamint különféle szerszámok markolatán.

A szablyamarkolatok sokasága bizonyítja, évezredes múltjával igazolja létjogosultságát. Ergonomikus, atropometrikus, évezredeken átívelő találmány!

A kutatók éjszakája előadásain bemutatott szablyamarkolatú eszközök esetén a hallgatóság átélte az „Aha!” élményt. Végezetül, utoljára bemutatom, hogy szinte nincs olyan porszívó, melynek a csövéhez illesztett hajlékony cső végén ne egy szablyamarkolatú átmenet biztosítaná, hogy mindvégig kényelmes tartásban maradjon a csuklónk.

32. sz. kép szablyamarkolat a porszívón

A SZABLYA KAPCSOLATA AZ ALÁNOKKAL ÉS A MAGYAROKKAL

Az, előzőekben megemlítettem, hogy a szablya első használói az alánok és a magyarok. A két nép évszázadokon keresztül közös szállásterületeken élt, kapcsolatukra a legősibb eredetmondáink is rávilágítanak, mint Hunor és Magor története, melyben a két testvér Alán királylányokat rabol el és vesz feleségül. Erről Váczy Péter is ír tanulmányában; *„Ebben a kérdésben kizárólag Kézai és a XIV. századi krónikák szolgálnak felvilágosítással. A magyar krónikaíró…büszkén írja le a két mitikus testvér, Hunor és Mogor történetét, akiktől minden hun és magyar eredt. Egy szarvasünő vezeti őket a Maeotis mocsaraiba, itt aztán új hazát alapítanak, majd elrabolva Dula alán fejedelem két leányát, idővel annyira megsokasodtak, hogy végül ez a haza se tudta eltartani őket”*. [21]

Természetesen nem lehet egy eredetlegendára alapozni tudományos megállapításokat. A fenti tanulmányon kívül az alánokkal való kapcsolatot a történettudomány is ismeri, mint például Kovács Vilmos [22], Haramza Márk [23]vagy Türk Attila Antal [24].

Az egymás mellett élő, néha egymással csatázó, néha egymással keveredő népek milyen szinten keveredtek jó példa rá az alábbi idézet Türk Attila doktori értekezéséből: *„Az antropológiai vizsgálatok is a lakosság összetételének heterogén jellegét erősítették meg. A nagy része helyi származású volt, a szarmaták, bolgárok és alánok közvetlen leszármazottai, a többiek betelepültek voltak: főleg szlávok,…illetve az Ázsia távoli részéről ide került nomád úzok és besenyők is idővel a lakosság részét alkották.”*

A magyarok, alánokkal való kapcsolatáról megállapítást tesz Al-Maszúdi, a Murug al-Dahab c. munkájában, mint azt Nagy Kálmán idézi; *„A magyarság helyére, helyzetére vonatkozóan megállapítható, hogy a nép ismert önálló története azzal kezdődött a 830-as években, hogy a kazár birodalommal való, közel három évszázadon át tartó együttműködés, alárendelés vagy gyengülő szövetségi viszony után különváltak, majd a Maeotis, Volga, Don körüli területről, az attól nyugatra eső folyóközbe, valószínűleg a Don és a Dnyeszter, Al-Duna közötti területre költöztek át…A kazár birodalomból való kiválásuk után is megtartották a jószomszédi viszonyt a környező népekkel, mint azt Al-Maszúdi a Murug al-Dahab c. munkájában lejegyezte: Békében élnek a kazár királlyal és ugyanúgy az alán fejedelemmel is”*. [17. 14. o.]

Ez azt jelenti, hogy keveredésük, egymás kultúrájának, eszközeinek, technológiájuknak cseréje nem ütközhetett akadályokba. Az alánokkal kapcsolatban ismeretes, hogy törzseik sokfelé letelepedtek a honfoglaló magyarok előtt és velük együtt is, mint azt Sárközy Miklós írja tanulmányában; *„Az alánság hosszú történelme során több részre sza-*

kadt, Galliától Észak-Afrikán át Mongóliáig követhetjük különböző korszakokban megjelenő csoportjaikat." [25]

Nagyon sok néppel keveredtek és amint azt Al-Maszúdi írta békében éltek a „Türkökkel" vagyis a magyarokkal 830 után. A honfoglalás után sokuk velünk együtt telepedett le, azóta teljesen a magyar nemzet részévé váltak, ők a jászok. A már előbb idézett Sárközy Miklós tanulmánya leírja, hogy kik is a jászok, és mi közük az alánokhoz; „*Az ókori és középkori forrásokban szereplő elnevezések – alán, al-lān, aorsos, róxolan(ruχs-alān), r(d)ukhs-ās, ṭuwal-ās, aš-tigor – számos esetben az egész népre vonatkoztatva jelentek meg, míg máskor valószínűleg csak egyes törzsekre utalhatott az adott kifejezés. A rendelkezésünkre álló források alapján elmondható, hogy az alán népnév nagyjából a 13. századi mongol hódításig domináns szerepet játszott az összalánság megjelölésére. Ezt követően az addig csak bizonyos alán csoportokat, törzseket jelölő, máig tisztázatlan etimológiájú ās (amely a keleti szláv ясы alakon keresztül honosodott meg a magyarban jász formában, és amely ettől függetlenül a mai oszét név előzménye is) a 13. századi mongol hódítást követően vált általános és az alánt felváltó népelnevezéssé forrásainkban.*" [25]

A magyar nyelv gazdagodott ezzel a testvéri – nyugodtan mondhatjuk, hiszen nemzetalkotó népünk a jász – együttéléssel, mint Sárközy írja; *„…érdemes röviden utalni a magyar nyelv alán…jövevényszavaira.…ezek a szavak kivétel nélkül a honfoglalás előtti időszakban kerültek a magyar nyelvbe. Ilyen jövevényszavaink például a vért, híd, ezüst, legény, nép, méreg, asszony, kard, vám, részeg, gazdag, tölgy, húg, üveg, egész, keszeg, mély, mén, zöld, gond, édes, fizet,…"* [25] Az alapos tanulmány szerint, a szavak jóval a honfoglalás előtt beépültek a magyar nyelvbe, így több minden más is közös a két népnél. Köztük a kovácsmesterség, technológiák, szavak is. Miért érdekes ez a szablya tekintetében?

A 19. sz. képen Kakukázusi alán és Szaltovói alán néven bemutatott markolat az, ami ugyanazon a képen a honfoglalás kori magyar szablya markolatára hasonlít. A jellegzetesség, mely egybe kapcsolja ezeket, a markolat speciális íve. Azt, hogy mi adta az ötletet ehhez a hajlat kialakításhoz, szinte bizonyosan sosem tudjuk meg. Mint ahogy a legfrissebb tudományos értekezés, Haramza Márk doktori disszertációjában írja, a szablya kifejlesztésével kapcsolatban sem tisztázható, mely néphez köthető az eredete; *„A szablya kialakulása, és a 10. századig történő fejlődése (az idő- és térbeli kiterjedtség az egyes változatok vonatkozásában, valamint a köztük fennálló kapcsolat kérdésessége) mind a hazai, mind a nemzetközi szakirodalomban vitatott"*.

László Gyula … kifejti véleményét, miszerint egy olyan nép hozhatta be e fegyvert 670 után a Kárpát-medencébe, amely előtte a Kaukázus előterében élt. Kovács László … rámutat, hogy a szablya kialakulását nem lehet egy konkrét etnikumhoz kötni.

A „szaltovó-majaki" hatást Erdélyi István már az avar szablyák esetében is valószínűsítette, amellyel együtt a fegyver ázsiai eredetét is hangsúlyozta. … Türk Attila a szablyák 7. századi kelet-európai megjelenését a kazárokhoz köti." [23, 20. o.]

Mindezen megállapítások ellenére, maga a szablya kifejezés nagyon sok nyelvbe változatlanul, vagy valamilyen torzítás útján épült be. Ezt többen is leírják, mint például Kalmár János egy munkájában; *„Mindenesetre tőlünk származott a szláv nyelvekbe. Az ószlovének, új-szlovének és oroszok sabljának, a bolgárok sabjának, a szerbek sabja-nak, a csehek sable-nak, lengyelek sablya-nak, románok sabiu-nak, albánok sablye-nek, az olaszok sciabala-nak, sdabola-nak, a franciák sabre-nak, a spanyolok sable-nak, a portugá-*

lok sabre-nak, a németek sabel-nek, a hollandok sabel-nek, végül a dánok sabel-nek nevezik." [26].

Az Arcanum Kézikönyvtárban található - Magyar etimológiai szótár- Szablya címszó alatt a következőket írja: „Szablya-*egyélű görbe kard'.Sok európai nyelvben élő vándorszó: német Säbel, francia sabre, olasz sciabola, lengyel szabla, szerb-horvát sablja stb. Ezek közül több is bizonyíthatóan a magyarból kölcsönözte a szót mint a* ***szab*** *vélt származékát. Ez utóbbi vélekedés azonban, amely sokáig nálunk is tartotta magát, kétséges, főleg azért, mert az ige 'vág' jelentése jóval később bukkan fel, mint a ~ első adatai, továbbá nincs nyoma olyan *szabol igének, amelyből a ~ mint melléknévi igenévi származék levezethető volna. A ~ szót tehát tisztázatlan eredetűnek kell tekintenünk."* [27] Ugyanitt megtaláljuk a szab szó leírását is; ***„szab*** *– '‹lapszerű anyagot› méretre és formára vág': bőrt, kelmét szab; 'meghatároz, előír, kijelöl': ... Ismeretlen eredetű szó."* [28]

Bármennyire is ismeretlen eredetű a szab és a szablya szavak eredete, az semmiképpen sem vonható kétségbe, hogy a szablya, mint erre a speciális kard-típusra alkalmazott kifejezés a magyar nyelvből – mint ahogy azt az előzőekben olvasható idézetek is bizonyítják - került át az Európai nyelvekbe.

MEGÁLLAPÍTÁSOK

A kutatásom eredményeit meglehetősen röviden össze lehet foglalni.

1. A szablya, ezen belül a honfoglalás-kori magyar szablya és az alán szablyák jellegzetessége a döntött markolat.
2. A különleges kard típus elnevezése ugyan ismeretlen eredetű szóból ered, de egyértelműen a magyar nyelv közvetítésével vált ismertté az európai nyelvekben, ide értve a szláv nyelveket is.
3. A markolat kialakítása ergonomikus és antropometrikus is.
4. A markolat fennmaradt több mint egy évezreden keresztül, és mind a mai napig használatos vágó-szúró sportfegyverek, tűzfegyverek (lőfegyverek), valamint különféle kézi szerszámok nyelén, markolatán.
5. Eddig ergonómiai szempontú kutatás nem született még a témában.

Meglehetősen széles körben kutattam, és arra a megállapításra jutottam, hogy valamely okból a kutatók sem az ergonómia tudományának térnyerése előtt, sem az után sem foglalkoztak a szablyamarkolat eredetével, méretezésével, annak feltárásával, miért alakult ki.

A markolattal kapcsolatos kutatásom egy véletlennek köszönhető. Néhány éve felkértek egy előadás megtartására, lőfegyverek témakörében. A felkészülés során szemet szúrt a korai lőfegyverek markolata és a honfoglalás-kori magyar szablyák markolatívének egyezése, sőt, díszítésük, mint például a markolatgomb egyezése is. Ha tanulmányaim során nem találkozom a munkavédelemmel, mint tantárggyal és ezen belül az ergonómiával, nem lehettek volna meg azok az alapok, melyekre támaszkodva a kutatást és elemzéseket elvégezhettem volna.

Nem várható el a történettudomány művelőitől, hogy a szakterületüktől igen távol eső ergonómia szempontjait beillesszék kutatási szempontjaik közé. Akkor meg különösen nehéz, ha a téma nagy tudású és alapos művelői mind a mai napig első sorban az eredet

kérdésével, vagy a népcsoportok meghatározásával is vitában állnak sok esetben egy-egy lelet kapcsán. Mindenesetre szeretném, ha munkám lökést adhatna bármely területen dolgozó kutatók számára ehhez hasonló interdiszciplináris kutatások megkezdésére.

FELHASZNÁLT FORRÁSOK

[1] Az ergonómia története című cikk A Japán Emberi Tényezők és Ergonómiai Társaság gondozásában lévő honlapon. https://www.ergonomics.jp/e_index/e_outline/e_ergono-history.html
[2] Az 1997-es könyv borítólapjának fényképe alatti képaláírás, Az ergonómia története című cikkben A Japán Emberi Tényezők és Ergonómiai Társaság gondozásában lévő honlapon. https://www.ergonomics.jp/e_index/e_outline/e_ergono-history.html
[3] British Medical Journal april 29.1950. 1009. oldal, Levelezés rovat. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2037509/pdf/brmedj03596-0041b.pdf
[4] COEH: A New Way to Solve Old Problems: The History of Ergonomics. https://www.coeh.berkeley.edu/post/history-of-ergonomics
[5] ERGOWEB: History of ergonomics. szerkesztői cikk Editor 28th March, 2017. https://ergoweb.com/history-of-ergonomics/
[6] Typotex kiadó: Ergonómia Hercegfi Károly – Izsó Lajos (szerk.) Budapest 2008 ISBN**:** 978-963-2790-95-4
[7] Szabó Gyula: Munkahelyek ergonómiai ellenőrzése 2014. https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/12133/2011-0054_munkahelyek_ergonomiai_ellenorzese.pdf?sequence=2&isAllowed=y
[8] Szabó Gy.: Az ergonómia fogalma, története, területei és szemléleti kerete. előadás prezentáció https://docplayer.hu/682203-Az-ergonomia-fogalma-tortenete-teruletei-es-szemleleti-kerete.html
[9] Szabó Gy. Testméretek mozgástartományok. előadás prezentáció https://docplayer.hu/41514195-Testmeretek-mozgastartomanyok-szabo-gyula.html
[10] Wikiwand szócikk: Adolphe Quetelet, https://www.wikiwand.com/hu/Adolphe_Quetelet
[11] Szabó Gy.: Az ergonómia fogalma, története, területei és szemléleti kerete. előadás prezentáció 4.1. sz. dia http://mtk.bme.hu/anyag/ora/MV_1_w.pdf
[12] Brehm A. F.: Az állatok világa 65. oldal https://mek.oszk.hu/03400/03408/html/index.html
[13] Csiky G.: Az avar kori szúró- és vágófegyverek. Osztályozás – tipológia – kronológia – technológia. Doktori értekezés Eötvös Loránd Tudományegyetem Bölcsészettudományi Kar Történelemtudományi Doktori Iskola, Budapest 2009. 125. oldal Szablyák fejezet http://doktori.btk.elte.hu/hist/csikygergely/diss.pdf
[14] Simon L.: Adatok a szablyák kialakulásáról A Herman Ottó Múzeum Évkönyve 30-31/2. (1993) 196. o. https://epa.oszk.hu/02000/02030/00026/pdf/HOM_Evkonyv_30-31_2_171-196.pdf
[15] Nyelv és Tudomány: A kaukázusi magyarokról: A honfoglalás körüli idők zegernyei(szerzői álnév) 2011. március 11. https://m.nyest.hu/renhirek/a-kaukazusi-magyarokrol-1
[16] Torontói cserkészek honlapja https://www.sites.google.com/site/torontoicserkeszek/honfoglalas/lovasnepek

[17] Nagy K.: A honfoglalás hadtörténete Acta historica hungarica turiciensa XXXIV. évfolyam 5. szám 44. oldal. A Zürichi magyar történelmi egyesület 118. sz. kiadványa Sorozatszerkesztő / Editor: Csihák György ISSN 2297-7538 Acta Historica Hungarica Turiciensia - 34. évf. 4. sz. (2019.)
[18] Lemil blog:Kultikus kardok krónikája I. 2014.10.09. 15:00 Titus Pullo Urbino álnevű szerző https://lemil.blog.hu/2014/10/09/kultikus_kardok_kronikaja
[19] Kovács L.: Szablya-kard fegyverváltás: a kétélű kardos 10-11. századi magyar sírok keltezéséhez Archaeologiai Értesítő, 117 - 1990.
[21] Váczy P.: Anonymus és Justinus kivonat. Turul a Magyar Heraldikai és Genealogiai Társaság közlönye az igazgató-választmány megbízásából szerkeszti Bottló Béla titkár Budapest kiadja a Magyar Heraldikai és Genealogiai Társaság MCMXLVII. szerkesztőség és kiadó hivatal Budapest I. Vár, Bécsikapu -tér 4. Országos Levéltár A szerkesztésért és kiadásért felelős: DR Bottló Béla
[22] Kovács V.: Uráli népek és a honfoglaló konglomerátum (befejezés) 4. A konglomerátum kavar csoportja. Együtt, A Magyar Írószövetség kárpátaljai írócsoportjának folyóirata, 2007. 4. szám. 110-116. oldalak.
[23] Haramza M.: A 9–10. Századi kárpát-medencei szablyák archeometallurgiai és hadtörténeti vonatkozása. Doktori disszertáció Szövegkötet Pázmány Péter Katolikus Egyetem Bölcsészettudományi Kar Történelemtudományi Doktori Iskola Hadtörténeti Műhely Budapest 2019.
[24] Türk A. A.: A Magyar őstörténet és a szaltovói régészeti kultúrkör. Doktori értekezés Szegedi Tudományegyetem Bölcsészettudományi Kar Történettudományi Doktori Iskola Medievisztika Program Szeged 2011.
[25] Sárközy M.: A magyarországi jászok nyelvemlékei – források, problémák, új adatok1. Keletkutatás 2020. tavasz, 89–110. old
http://dx.doi.org/10.24391/KELETKUT.2020.1.89.
[26] Kalmár J.: A magyar kard fejlődése Magyar Szemle 1935. 02. 241. oldal utolsó előtti bekezdés.
https://epa.oszk.hu/03900/03940/00027/pdf/EPA03940_magyarszemle_1935_02_238-245.pdf
[27] Arcanum Etimológiai Szótár, Szablya címszó: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-magyar-etimologiai-szotar-F14D3/sz-F3D93/szablya-F3D9C/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfRjE0RDMiXX0sICJxdWVyeSI6ICJzemFibHlhIn0
[28] Arcanum Etimológiai Szótár, Szab címszó: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-magyar-etimologiai-szotar-F14D3/sz-F3D93/szab-F3D94/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfRjE0RDMiXX0sICJxdWVyeSI6ICJzemFibHlhIn0#Lexikonok%5ESzT-ETIM-szab

KÉPEK ÁBRÁK JEGYZÉKE

6. sz. kép Egyenes nyelű csavarhúzó saját kép
7. sz. kép Egyenes nyelű egykezes fűrész saját kép
8. sz. kép Egronomikus szemétszedő csipesz saját kép
9. sz. kép Ergonomikus snitzer saját kép
10. sz. kép Ergonomikus lapát és gereblye saját kép
11. sz. kép Ergonomikus zuhanyfejek saját kép
12. sz. kép Ergonomikus nagyító saját kép
13. sz. kép Ergonomikus nagyító saját kép
14. sz. kép Ergonomikus kézi porszívó saját kép
15. sz. kép Ergonomikus kézi porszívó saját kép
16. sz. kép Ergonomikus kézi porszívó saját kép
17. sz. kép Ergonomikus láncfűrész saját kép
18. sz. kép. Kovácsolt, honfoglalás kori magyar szablya replika saját kép
19.sz kép. Kovácsolt, honfoglalás kori magyar szablya replika markolat nagyítva saját kép
20. Szablyák innen-onnan című ábra. Forrás Torontói cserkészek honlapja
https://0c7c6594-a-62cb3a1a-s-sites.googlegroups.com/site/torontoicserkeszek/honfoglalas/lovasnepek/6_szablyak-innen-on-nan.png?attachauth=ANoY7cq3VmBEPyy96yFueRorUzHYXI7i3u3fdv1MGZYzoOy0U00TPfyO80WvCr_4VrlYHO0m4iVByRctO-UY3wTtLxHLOb1KwYjnchDn9CqA-0jNnicJnSOtO34zV91jU_5oqpU1yDYzuCM9fxfg-jeFisqvH1wkGSmzmyhsjlXlncUlydNJD5R-WHB41lL07QedNHvu-xXAw4GCx-ma7DuI4r4L77QMf_ucd4HpYOu_95JgKRSI1yPM_K7NeGb6LoN5Fm9OMsIedI2fStxKqPNyozjQ-eL-PQ%3D%3D&attredirects=0
21. sz. kép. Honfoglalás kori magyar szablya Magyar Nemzeti Múzeum
https://mnm.hu/sites/default/files/styles/gallery_item/public/gallery/rt_ho_81.1895.8-10._nr002.jpg?itok=K4yMepjQ
22. sz. kép. Honfoglalás kori aranyozott dísz szablya, Bécsi Művészettörténeti Múzeum
forrás: http://muvtor.btk.ppke.hu/etalon/549.jpg
23. sz. kép Nehézlovassági kard markolata, saját kép.
24. és 25. sz. kép Bökés ujjal és pálcával saját képek
26. sz. kép a Szablya és a pálca íve Pergel Áron képe
27. sz. kép A magyar szablya és Arwen kardja Pergel Áron képe
28. sz. kép Kovás pisztoly markolat, saját kép
29. sz. kép Kovás puska markolat saját kép
30. sz. kép. Szablyamarkolat a puska tusa előtt. saját kép
31. sz. kép, Szablyamarkolat a puska tusa előtt. saját kép
32. sz. kép Szablyamarkolat a porszívón, saját kép

DISPOSABLE LOCKS, SEALS AND THEIR POSITION IN PROPERTY PROTECTION (PART 1)

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

SZABÓ László András[1]

Abstract

I have been developing, manufacturing, and marketing disposable locks for almost twenty years. I confess from the metal industry that this was only ancillary production, at first its low cost and high sales volume proved to be a good cost carrier alongside other products I estimated more at the time. 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 first part, I clarify the concept, take a historical look back and examine development from a Hungarian perspective.

Keywords

disposable locks, property protection, mechanical protection, development, regulation

Absztrakt

Közel húsz éve foglalkozom egyszer használatos zárak (plombák) fejlesztésével, gyártásával és forgalmazásával. Bevallom a fémiparból érkezve ez csak kiegészítő termelés volt eleinte alacsony költsége magas eladási darabszáma jó költséghordozónak bizonyult az általam akkoriban többre becsült egyéb termékek mellett. 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. Első részben a fogalmat tisztázom, történeti visszatekintést teszek és fejlődésüket vizsgálom magyar szempontból.

Kulcsszavak

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

[1] szabolandras.kmo@gmail.com | ORCID: 0000-0001-7957-0724 | PhD Candidate, Óbuda University Doctoral School for Safety and Security Sciences | doktorjelölt, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Tanulmányom az egyszer használatos zárakat járja körül, de tágabb értelemben hiszen a jelek és jelzések régi keletűek továbbá az embert, aki alkotja és használja. Már az első társadalmakban is jelezték, hogy az adott barlang melyik törzsé az állatokat festék jelekkel látták el. Még a határt is megfelelő ijesztő és figyelemfelhívó tárgyakkal látták el. Az írásbeliség megjelenésével a jelek a hieroglifák a figyelmeztetések és átkok nem mindenki számára voltak olvashatóak. De egy-egy kiemelt jel például a fáraó neve mindenki számára egyértelmű volt. Figyelmeztetett és jelezte a következményeket. A római időkben a császári parancsokat jelezte de a hajószállítmányok és termékek sértetlenségét is mint a boros amforák lepecsételése. Később a kínai részen a pecsét megjelenése a császári hatalom kifejeződése és megnyilatkozása lett. Nagyobb ugrás a középkor Szent István pecsétje, az Aranybulla pecsétje vagy az Angol királyi pecsét. (innen jön a seal- pecsét kifejezés) Már az ókorban megjelentek az egyedi pecséthengerek később a pecsétnyomók melyek, a forró lágyviaszba belenyomva nemcsak lezárták az adott dokumentumot, hanem hitelesítették és biztosították sértetlenségét a címzetthez való eljutásig. Tehát a pecsételés nemcsak a tulajdonlást jelezte hanem elszámolás esetén is szerepet játszott. Tehát, aki feltörte a pecsétet egyben a törvényt is „megtörte" és számolhatott annak szigorával. Természetesen a polgári társadalmak és a magántulajdon előretörésével a magánszféra a polgárság és kereskedőség is igényelte a saját pecsét és ezzel a kiváltságok megszerzését. Magyarországon nagyon sok város vagy megyeszékhely a címerében őrzi a pecsétjét. A szállítmányozás fuvarozás fejlődésével az eszközök is változtak. Egységes szállító és tároló helyek kialakításával egy másfajta pecsétre és itt megjelenő plombára volt szükség. Már nem a jelzés volt az elsődleges, hanem megjelent a vagyon védelem és vagyon biztonság igénye. A fa alapanyagú kötél vagy madzag anyagú zárak viasz vagy gyurmás lezárással még mindig csak jelzésre szolgáltak. A fémzárak megjelenése a dróthuzal a végén lágyólom fejjel már komoly műszaki előrelépés mutattak ez az iparosodás a tömeggyártás megjelenése és áruk nagy mennyiségének folyamatos szállításának az időszaka. A beazonosíthatóság megmaradt a plombanyomóval egyedi jelet lehetett a lágyólom fejen elhelyezni. Robbanásszerű növekedésnek indult a zárak fejlődése különböző kivitelű anyagú és biztonsági fokozatú zárak jelentek meg. Az Első és a Második Világháború katonai fejlesztései a tikosítás az őrzés és szállítás magasabb szintre emelték a zárak felé megfogalmazott követelményeket. A műanyag felfedezése és széleskörű használata a technológia fejlődése a magánpiac változó követelményei sokat lendítettek és új területekre terelték a fejlesztéseket. Ezzel párhuzamosan megjelentek a szabályozásra gyártásra felhasználásra és megsemmisítésre irányuló igények, mint a piac mint a gyártók felöl. A 2000-es évek elejére az ISO szabvány is meghatározott egy követelményrendszert. A zárak és felhasználásuk területét alapvetően a jog így a magánjog és a büntetőjog volt, ami meghatározza, és továbbra is ez marad. Mindig is fontos eleme volt a rendszernek az ember, hiszen a leleményessége korlátlan, de nem mindig a jó érdekében használja fel. A legfontosabb fejlődések a zárak műszaki és szabályozási területén a fosztogatások és lopások miatti fejlesztések. Szakdolgozatomban ezen témát és területet járom körbe természetesen a fejezetek külön-külön egy-egy szakdolgozat témája lehetnének, de a terjedelem, illetve az adott szemponton a vagyonvédelem fókuszán át való vizsgálat ezt nem teszi lehetővé. A műszaki fejlődésének szabályozása és kapcsolata a vagyonvédelem komplex rendszerének elemeivel, a többoldalúsága a témának a sokszínűsége és izgalmas aspektusai a vagyonvédelemre. Tudtommal a témát előttem még senki sem dolgozta fel.

A PECSÉTEK KIALAKULÁSA ÉS TÁGABB ÉRTELMEZÉSE

Ebben a fejezetben a történelmi korok áttekintésével a teljesség igénye nélkül példák kiemelésével mutatom be a pecsétek, zárak kialakulását történelmi hátterét.

Őskor

Nincs írásbeliség jelek és képek vannak. Barlangrajzok az ember vágya a világ megismerésére és uralására. Az enyém a miénk megjelenése és a védelem a harc a másik törzzsel vagy törzsekkel . Hogyan lehet jelezni megjelölni, hogy egy adott terület mely törzsé családé? Csak a jelek elhelyezésével. A törzsi jelek megjelennek (mai napig fellelhetők az amerikai indián törzseknél, afrikai bennszülötteknél) és ezzel együtt a törzsi vezetőknél is megjelenik a saját jel. Főképp állatok vagy absztrakt formák geometriai alakzatok mindmind egy célt szolgálnak, jelezni hogy ez a miénk a törzsfő védelme alatt áll és egyértelműen következményeket (szankciókat) von maga után a megsértése. Hogyan választottak maguknak jelképet? A név megjelenése a név jelentése és a név valamilyen ábrázolása. Emlékezzünk nincs még írásbeliség. Nagyon fontosak ezen társadalmak számára a nevek és a nevek mögöttes jelentései, ha a név megóvja viselőjét a névből annak jelképéből születő jel, jelzés szintén óvó védő tulajdonsággal rendelkezik. Tehát, hogyha ezen jelet elhelyezzük, a környezeten a fákon és az állatokon ezzel megóvjuk, megvédjük őket az ártalmas behatásoktól (szellemektől) és az idegen kezektől más törzsbeliek gonosz szándékaitól és tetteitől. Az elhelyezés módja karcolás a belevésés és a festékek használata. Később az állatokba jel beleégetése mivel ez így már eltávolíthatatlanná válik, mely az egyszer használatos zárak (plombák) egyik fő kritériuma. Természetesen a leleményesség már akkor is megvolt a felülfestés vagy az átégetése a jelnek. Tízezer év a technika változik de az ember nem. Bármilyen módszerrel, de a vagyont meg kellett védeni a területet és az állatokat tulajdonképpen akkor és ott született meg a mai napig egyik legfontosabb emberi tevékenység a háború. Tehát a jelek egyre nagyobb szerepet játszottak és rendszerbe álltak. Lassan kezdett megjelenni az írásbeliség a közlés és a gondolat megőrzésének egy új megoldása. Ez már a következő fejezet témája.

Ókor

Az ókor [1] legjelentősebb „*pecsétjeként a Salamon pecsétje néven ismert, két egyenlő oldalú háromszögből összetevődő hatágú csillagot a makrokozmosz jeleként szokták értelmezni. A lefelé álló háromszög az alsó, azaz az anyagi világot, a felfelé álló háromszög a felső, azaz a szellemi spirituális világot jelképezi, összekapcsolódásuk, illetve egymásba hatolásuk pedig a kettő egységét fejezi ki. Ezenkívül a lefelé álló háromszög képviseli az őselemek közül a földet és a vizet, a felfelé álló háromszög a levegőt és a tüzet, egyesülésük pedig magát a tetemtett világot szimbolizálja, amely a négy őselemből tevődik össze. Ebből következik, hogy a Salamon pecsétje talizmánként viselve előmozdítja az alsó és a felső világ, azaz a test és a lélek, illetve szellem harmonikus együttműködését, hozzásegít a belső és ezáltal a külső univerzum békéjéhez. Ezenkívül összeköttetést biztosít a makrokozmosszal, és kaput nyit a természetfölötti világra*.”

A Biblia is több helyen említi a pecsétek használatát így Salamon pecsétjét is. Ez egy közismert tény és jelkép. Miért ezzel kezdem? Összeköti az őskort, ahol a jeleknek természetfölötti jelentést tulajdonítottak az ókorral. Salamon pecsétjében az a különleges, hogy nem egy névből generált jel vagy jelek sorozata, mint a fáraóké. Nagyon sok jelentése van nem lehet egyértelműen az anyagi világhoz kötni.

Egyiptom. Fáraók földje a hieroglifák megjelenése a jelek képírássá való fejlődése összefügg a vallással a túlvilági élettel. Nagyon fontos, hogy megjelenik hisz a vallással összefüggő jelképek már az őskorban is megjelennek, de igazi kultuszuk az ókorban teljesedik ki, megalapozva a következő századokét is. A fáraók hittek a jelek védelmében a név védelmező erejében. Tudjuk, ha valaki nevét kitörölték, olyan mintha a személy soha nem is létezett volna ez egy nagyon súlyos büntetésnek számított. A szarkofákon és elhelyezték a nevet védelmezőn. Sajnos nem sikerült elijeszteniük a sir rablókat hiszen a Királyok Völgyében nagyon sok sírt kifosztottak sokat már a temetést követő éjszakán. Családok, generációk éltek ebből a „foglakozásból" Egyiptomban. Őrizték a sírokat a papok, de így is kijátszották őket. Akit elfogtak kivégezték de a régészek a legtöbb sírt már kifosztva tárták fel. A sír lepecsételése átokkal való védelme eleinte működött később már inkább rejtve temetkeztek titokban és semmilyen jelet nem hagytak úgymond nem reklámozták a sír helyét felhívva a fosztogatók figyelmét arra. A piramisok építésének egyik oka volt a védelem. Áll kamrák elhelyezése az igazi elrejtése. Nagyon fontos felfedezéséhez értünk a történelemnek, mégpedig a papír felfedezéséhez. Tudjuk, hogy állati bőrre agyagtáblára már korábban is írtak, de az egymás közötti kommunikáció a gondolatok, szállítási kimutatások, adók és törvények leírása és így történő kézből kézbe átadása nagy lépés volt az emberiség történetében. Ami a pecsétek kialakulásában egy új feladat funkció megjelenése az a hitelestés! Vagyis az iratot a pecsét elhelyezése hitelesítette anélkül, hogy a címzetten kívül más is elolvasta volna. Nem kellett kinyitni a tekercset, még az írástudatlan számára is jelezte, hogy az adott irat kitől származik hogyan kell vele bánni. Megsértése büntetést von maga után.

Mezopotámiában és Egyiptomban és a Görög városállamokban egyaránt használtak pecséthengereket. Technikailag ugyanaz volt, mint ma lágy anyagba viasz a pecséthenger kidomborodó felét végighengergették mely így nyomot hagyott. A meleg viasz még jobb megoldás volt. Az egyiptomi temetkezési kamrákban sok amforát agyagedényt találtak mely ezzel a módszerrel volt lezárva. Tehát a kereskedelem és a diplomácia, mint záró védő és hitelesítő eszközt használta. Kijelenthetjük, hogy az egyszer használatos zárak (plombák) alapvető kritériumai szerint itt születtek meg.

- Kialakul a pecsétek hármas célja;
- Garantálják a titkosságát a tartalomnak, a külső érintettlenségét;
- Tulajdont bizonyítanak;
- Érvényesítenek, hitelesítenek.

Római Birodalom, a hatalom központosítása miatt itt élték virágkorukat a pecsétek. Minden valamirevaló római nemesnek volt saját pecsétje a császári pecsétek a császár arcmásával közismertek. A birodalmat kormányozni kellett a törvényeket és utasításokat a hadseregnek és provinciáknak el kellett juttatni. Nem lehetett megengedni a hamisítást. Megjelennek a fém plombák ólomból ezüstből aranyból. Ezeket hívjuk latinul bulláknak. A pecsétek el kezdenek tipizálódni egy-egy adott feladatra más-más pecsétet használnak. Természetesen itt a felhasználási kör és pecsétnyomó milyensége a különbség.

Középkor

Mint az előző pontból megismertük a pecsétek és tulajdonságaik az ókorban kialakultak. Tehát a középkor a fejlődés tekintetében nem hozott újat. A középkort alapvetően a

kétpólusság uralta a vallási és a világi hatalmak közötti harc. Ez rányomta bélyegét a pecsétekre is. Pár jellemző kiragadott példa erre. Pápai pecsétek: A hitelesítő pecsét egyik fajtája az ellenőrző pecsét, az úgynevezett nagy pecsét helyek hátlapjára az azt hitelesítő személyek (egyházfők) saját pecsétjüket nyomták. A Pápai rendeleteket törvényeket az aktuális Pápa a saját pecsétjével látta el. Ez a pecsét felszentelésétől egészen a haláláig működött majd eltörték és vele temették el. Királyok, császárok, főurak: Rendeleteiket és törvényeiket pecséttel látták el.

A Bevezetőben említett Aranybulla [2] „*Az Aranybulla szűkebb értelemben II. András magyar király1222-ben kiadott, aranypecséttel ellátott királyi dekrétuma, amelyben helyreállította és kibővítette Szent István alkotmányát. Tágabb értelemben az aranybulla szó azt az arany pecsétet jelenti, mellyel a magyar királyok – II. Bélától kezdődően – megerősítették fontosabb okmányaikat."* Természetesen megjelennek a városok a polgárosodás és követelik a jogot maguknak melyhez pecsét és így törvényalkotás is jár. A városi polgárság és kereskedő réteg mely a késő középkorban elkezdi pecsételni szerződéseit, szállítmányait és áruit. A nemesség által használt ezüst és arany pecsétek túl drágák, de van egy anyag mely hasonlóan lágy formálható és megfelelően olcsó. Ez az ólom. A madzag és a rányomott ólomplomba már mindannyiunk számára ismert sok helyen még ma is használatban van.

Példaként pár különböző felhasználási területű pecsét melyet szinte a mai napig használnak:

- Idéző

„Idéző pecsétet „*már a rómaiak is használtak lényege, hogy a főúr (bíró) saját képét ábrázoló pecsétjét küldte el a megidézettnek, a pecsétvivő élőszóba közölte, hogy hol, mikor, és miért kell a megidézettnek megjelennie*."

- Záró

„Akkor használták, amikor egy irat titkosságát, zártságát akarták szavatolni. Ilyenkor az oklevelet olyan módon pecsételték le, hogy annak tartalmát csak a pecsét feltörésével lehetett megismerni, a pecsét illetéktelen feltörőjét bűnösként marasztalták el. Például Magyarországon a koronázási jelvényeket tartó ládát a koronaőrök és országnagyok jelenlétében lepecsételték és így tartották a következő koronázásig."[3]

- Hitelesítő

„Ez a pecsét az oklevélben rögzített jogi tény, vagy akaratnyilvánítás bizonyítására szolgált. Elsősorban az örökérvényűség igényével kiállított kiváltságlevelek (privilégiumok) esetében volt fontos, mert itt a pecsét örök időre szólt. Ezeken az okleveleken megfelelő rögzítést kellett alkalmazni a pecsétnek, ugyanis minden nyilvánosnak szánt oklevelet függesztett pecséttel erősítettek meg. Az ilyen pecséteket könnyen el lehetett távolítani, ezért sok visszaélést, hamisítást követtek el velük. „

- Vámpecsét

Mai napig használják az adott országból kimenő és beérkező szállítmányok ellenőrzésére.

Új Kor és az iparosodás

A tömegcikkek és a tömegtermelés megjelenése szükségessé tette új megoldások kialakulását. [4] Megnőtt a szállítmányok mennyisége nagyobb hajók épültek elindult a vasút lecsökkent a szállító személyzet létszáma egy-egy munkásra sokkal nagyobb mennyiségű áru és az azokért vállalt felelősség rakódott, mint előtte. Meg kellett valahogy oldani az áruk beazonosíthatóságát és a tulajdonos felé való könnyebb elszámolást. Mint láttuk, eddig a történelemben a pecsétek mostantól egyszer használatos zárak (plombák) nem voltak a felhelyező tekintetében megkülönböztetve. Hiszen úgysem merték hamísítani másolni őket. De ebben az új helyzetben nem elég a jel elhelyezése valamilyen számozást is kellett, hogy tudjuk ki és hol helyezte fel a zárat épp az áruk megnövekedett mennyisége miatt. El kezdődött a zárak számozása. Vagyis a plombanyomó egyik felén jel a másikon szám szerepelt melyet a lányólomba belenyomva lenyomatott hagyott. Megnőtt az igény az egyszer használatos zárak tömeggyártására.

FEJLŐDÉSÜK ÉS TECHNIKAI VÁLTOZATOSSÁGUK

Az előző fejezetben eljutottunk általában közismert egyszer használatos zárhoz a plombához. Természetesen a fejlődés nem állt meg és mind a mai napig tart.

„Az egyszer használatos zárak (plombák) legpontosabb meghatározása :

275/2000. (XII. 28.) Korm. Rendelet az Egységes Árutovábbítási Eljárás EK-EFTA Vegyes Bizottságának 2000. december 20-i 1/2000. számú határozata kihirdetéséről II. Melléklet [5]

A zárak jellemzői

Az I. Függelék 28. Cikkében megadott zárak legalább az alábbi alapvető jellemzőkkel rendelkeznek, és az alábbi műszaki jellemzőknek felelnek meg:

a) Alapvető jellemzők:

A zárak:

(1) általános használat során biztonságosak maradnak;

(2) könnyen ellenőrizhetők és felismerhetők;

(3) úgy lettek gyártva, hogy mindenfajta feltörés vagy eltávolítás szabad szemmel látható nyomot hagy rajtuk;

(4) egyszeri használatra lettek tervezve, vagy ha többszöri felhasználásra készültek, úgy lettek tervezve, hogy minden újrahasználás alkalmával

világos, egyedi jellel lehessen azokat ellátni;

(5) egyedi azonosító jelet viselnek.

b) Műszaki jellemzők:

(1) A zárak formája és mérete változhat az alkalmazott zárási módszerrel, a méretnek azonban lehetővé kell tennie az azonosító jelek könnyű leolvasását

(2) Lehetetlen kell hogy legyen a zárak azonosító jeleinek hamisítása, és nehéz az utángyártásuk.

(3) A felhasznált anyagnak ellenállónak kell lennie a véletlen sérüléssel szemben, továbbá lehetetlenné kell tennie az észrevehetetlen hamisítást vagy újrafelhasználást. Többfajta szempont szerint lehet vizsgálni a fejlődést én három szempont szerint szeretném körbejárni".

FEJLŐDÉSÜK ANYAGUK SZERINT

Ólomplomba. Mint láttuk a klasszikus madzag vagy drótszál és ólom anyagok kettőse volt a legtovább használatban. Sajnos manipulálható volt a madzag elvékonyítása és áthúzása a drótszál mozgatásával a lágyólom furat megnagyobbítása vagy az ólomfej átmenő furatának tágítása a belenyomott jel átütése illetve megváltoztatása. Továbbá az ólom környezetszennyező volta ezt a kiviteli formát elavulttá tette. Alumínium plomba. Ugyanaz a kivitel, mint az ólomnál csak a fej anyaga alumínium. Előnye nem környezetszennyező. Hátránya ugyanúgy manipulálható, mint az ólom és az alapanyaga miatt drága az előállítása. Műanyag plomba. Az ólomfej helyett kellett valami más, és ez lett a műanyag. A madzag helyett drótkötél, de már a műanyag száll is használatba került. Tehát tisztán műanyag lett az egyszer használatos zár a plomba. A probléma a jelzések elhelyezése a zárra melyet két módon oldottak meg. Vagy előre már feliratozták sorszámozták, vagy az egyik fele lágy műanyag volt és a hagyományos plombafogóval el lehetett helyezni a jelzést. A lezárás is változott a plombafogóhoz képest már nem kellett külső eszköz egyszerű kézi beroppantás vagy egy önzáró csavaros megoldás mely beletört a fejbe és így történt meg a zárás. Műanyag zárak. Jelképes zárnak, házi zárnak és fuvarozási zárnak is nevezik. Megjelent az igény, hogy ne keljen külső eszköz a lezáráshoz úgynevezett önzáró zárak plombák jelentek meg. Itt kell egy nagyon fontos tévedést összetévesztést tisztázni. A kötöző pánt nem plomba! Más az anyag más a feladat és más a műszaki előírás és a nyilvántartása, illetve a kötöző pántoknál van oldható kötésű kivitel. Az egyszer használatos zárak, plombák esetében nincs oldható kivitel! Roppant mód tud dühíteni mikor valaki az mondja zárra – igen ez kötöző pánt! Nem az! Az egyik villamos ipari eszköz, a másik vagyonvédelmi eszköz. Na remélem ezt sikerült tisztázni! A műanyag záraknál két nagyon fontos műszaki probléma merült fel, mégpedig egyik a szélsőséges hőhatásnak való megfelelés +100 °C-tól a -40 °C-ig. Ez különleges anyagok kifejlesztését polipropilén és a poliamid, valamint egyéb anyagok kombinációját jelentette. Két különböző műanyag összeillesztése más a szalag és más a ház. Illetve ugyanígy más műanyaggal vagy fémmel a zárás megerősítése „bebetétezés" módjával. A másik, mint a törvényből is kitűnik a manipuláció vagy a idegenkezűség azonnali jelzése az anyag roncsolódása, sérülése karcolódása útján. Ezt a színezéssel is el lehet érni tehát nyújtás csavarás vagy más erőbehatás hatására az anyag kifehéredik. Vagyis felületileg van festve.

Műanyag és fém keveréke. Az előbb írt „bebetétezésen" túllépve egyik elemet tisztán műanyagból gyártani. Vagy a ház vagy a záró elem. Átmeneti megoldás a jelképes és biztonsági zár között. A Műanyag házat könnyebb feliratozni mint a fémbe belenyomni a feliratot és a sorszámot. Olyan kivitel is van, ahol a drótkötelet teljesen bevonják műanyaggal így képezve a drótkötélen záró elemet. Fémzárak. Biztonsági zárak. Konténerzárnak. Olajos zárak. Minden része fém a szalag, a drótkötél vagy a merev fémrúd más néven a záró csap és a ház is. Nagyon fontos, hogy szép felületet kell a gyártás során létrehozni pontosan azért mert minden egyes manipulációnak nem rendeltetés szerű erőbehatásnak jól látszania

kell. A házat valamilyen jó alakítható anyagból érdemes gyártani, hogy ezen előírásoknak megfeleljen.

FEJLŐDÉSÜK FELADAT (FUNKCIÓ) SZERINT

Alapvetően két nagycsoportra oszthatjuk a zárakat feladat szerint:

Jelképes zárak

Mint a nevükben is benne van az illetéktelen felnyitás jelzésére szolgálnak. Roncsolás mentesen kinyitni és visszazárni ne lehessen a már felhelyezett zárakat. Kézi erővel le lehet őket szakítani, eltávolítani a lezárt felületről. Olyan mértékben roncsolódnak, hogy egyértelműen jelzik az idegenkezűséget. Egyedi azonosítóval rendelkeznek melyet nyom nélkül eltávolítani vagy megváltoztatni nem lehet. Fontos kritérium, hogy a roncsolódás mértéke megakadályozza két vagy több felhasznált zárból egy látszatra ép zár összerakását, kialakítását.

Biztonsági zárak

Nemcsak jelzik a jogtalan felnyitás tényét és roncsolás mentesen nem lehet őket visszazárni. Védelmet is kell, hogy adjanak. Elvárás bizonyos szintű szakítóerő vagyis kézzel vagy egyszerű kézi szerszámmal ne lehessen eltávolítani a zárakat. Amennyiben a lezárt objektum, konténer, vagon közelében felfigyel az élőerős őrség, vagyonőr, biztonsági őr egy illetéktelenül ott tartózkodóra, akinél pajszer, csapszegvágó, drótvágó vagy bármilyen eszköz van, ami alkalmas lehet az esetleges bűncselekmény megelőzésére vagy bizonyítására, megteheti a szükséges intézkedéseket.

FEJLŐDÉSÜK A ZÁRÁS SZABÁLYOZHATÓSÁGA SZERINT

Igazából a felhasználás követelménye miatt alakult ki, hogy szabályozható vagy fix a zárás. Az, hogy jelképes vagy biztonsági zárról beszélünk érdektelen, hiszen mindkettőnél találunk fix és szabályozható kivitelt. Az olyan felhasználási területen, ahol állandó nagyságú a lezárandó felület lehet fix a zárás. Ilyenek például a konténerek és az ott használt úgynevezett bepattintós tengeri zárak. Míg a vagonoknál vagy az olaj tartályoknál ez a távolság szórt. Vagyis csak szabályozható zár használható, például a drótkötél. Érdekes ellentmondás ebben az összefüggésben a 2méter hosszú szabályozható drótköteles zár melyet a konténer ajtók középső két rúdján átfűzve helyeznek fel.

Technikai változatosság

Ahány ház, annyi szokás! Szoktuk mondani. Ez az egyszer használatos zárakra is igaz. Ahány gyártó annyi zárási megoldás és a formaváltozatosság. A feladat adja mindig a zárási megoldás alapját. Már tudjuk, hogy a zárakat lehet a zárás hosszának szabályozhatósága szerint osztályozni. Tapasztalatom szerint ez a kettő a feladat és a zárás hosszának szabályozhatósága adja a zárási mód kialakítását. Minden fejlesztő, gyártó igyekszik védeni a saját zárási módját találmánnyal, szabadlommal forma védelemmel. Rengeteg zárkivitelt, megoldást védenek le. Ez alapvetően a szabadalmi szabályozástól függ. Például az USA szabványoknál már apró módosítás is lehet új megoldás és ezzel együtt védelem alapja A Magyar szabadalmi törvények sokkal szigorúbbak. Hármas kritérium rendszert használnak.

A Használati mintáknál (kis szabadalmom) Négyes rendszer a Szabadalomnál. A forma védelemnél hármas kritérium rendszert használnak.: Vizsgálják az újdonságot, a feltalálói lépést, és az ipari használhatóságot. A negyedik a szabadalmaknál a publikusság, vagyis a szabadalom már a védelem bejelentése előtt megismerhetővé, hozzáférhetővé vált. Az Európai Unióbaba lépés óta folyik a jogharmonizáció és az Európai Unió egyik célrendszere „Európai vívmányok védelme" hozta létre az Európai Szabadalmat. Vagyis az adott bejelentést nem kell minden egyes európai országban bejelenteni, hanem egy bejelentéssel az egész régióra érvényes eljárást lehet indítani. Érdekes módon a formavédelmek a legerősebbek az Európai Unióban-ban. A kis kitérő után nézzük az egyszer használatos záraknál használt zárási módokat részletesebben. Az úgynevezett bepattintós zárak: lehetnek jelképes és biztonsági zárak. Fix zárásúak. A zárás úgy történik, hogy egy záró elem melyen körbefutó vájatot képeztek ki átmegy a házban egy rugalmas lezáró elemen ez lehet műanyagból vagy fémből készült rugalmas patron vagy a házban elhelyezett záró gyűrű, zéger gyűrű szakszóval. Miután a rugalmas záró elem egyik irányba átengedte, helyére pattan és mivel csak egy irányba enged a fej kialakítása miatt megtörténik a zárás. Már csak roncsolással lehet kihúzni. Az egyszer használatos zár szalagrésze lehet kör alakú záró bemélyedéssel, vagy úgynevezett gyöngyös megoldású. Igazából a hagyományos szuronyzárokra hasonlít csak nem oldható. Ezen zárás és kivitelekre jellemző, hogy nincs mozgó elem a fejben. Hátránya erőszakos kinyitás után visszanyomva a záró elemet csapszeget a házba lezárt helyzet látszatát kelti. Másik megoldási forma a szabályozható zárási hosszú műanyag záraknál a szalagtesten kiemelkedések létrehozása és a fejben elhelyezett akadó elemekkel, tüskékkel valósul meg a zárás. Természetesen az akadó elemeknek tüskéknek megfelelően rugalmasnak kell lenniük. Hátránya a hosszú záró felület roncsolja a tüskéket és gyengíti a zárást. Elkopik a záró tüske, akadó elem és így behúzva a lezárt helyzet látszatát kelti. Hasonlóan az elsőhöz műanyag jelképes zár szabályozható hosszal de a záró tüskék, záró elemek fejben egymáshoz képest eltolva vannak elhelyezve ez a zár szalagját megtöri így tehermentesíti a záró tüskéket, elemeket. Műanyag bebetétezett zár, vagyis egy mozgó záró elem van a fejben, ez lehet műanyag vagy fém és megszorulva a fejben végzi a zárást. Hátránya a fémlaposnak, hogy ha nagyon éles a fejben elhelyezett fémpenge a zárás után előírt zárást ellenőrző meghúzásnál elvághatja a szalagot. Biztonsági fémzárak egyik kivitel a golyós vagy kis fogaskerekes lezárás. Lehet a záró elem csapszeg vagy drótkötél. A fejben elhelyezett kúpon mozogva a zárás irányával ellentétesen az ott elhelyezett golyó(k) vagy fogaskerék rászorul a csapszegre vagy drótkötélre és így történik meg a zárás. Biztonsági fémzárak csapszeges vagy drótköteles kivitel a zárást a fejben elhelyezett hasított kúpos záró elem végzi, mely a házban kialakított kúpon a zárással ellentétesen mozogva rászorul a csapszegre vagy a drótkötélre, így valósítva meg a zárást.

Nem esett szó két nagyon fontos kritériumról, elvárásról az egyszer használatos zárak, plombák kapcsán. Pedig nagyon fontosak a tervezés, fejlesztés tekintetében. Ezek pedig a következők:

Egyrészt: Nem sérülhet vagy eshet le, nyílhat a zár a lezárt objektumról, konténerről. vagonról, pénzeszsákról szállítás közben. Ki kell bírnia a szállítással együtt járó mechanikai terheléseket, időjárási körülményeket, a rázkódást az ütődést. Ezek a körülmények nem szabad, hogy befolyásolják a működését, vagy olyan káros nyomokat hagyjanak, amiket össze lehet téveszteni az idegenkezűséggel. Tapasztaltam, hogy a rajtakapott vagy tetten

ért elkövető későbbi egyik védekezése volt, hogy már nyitva találta az objektumot, konténert, a zár már sérült volt. Ilyenkor meg kell állapítani a nyomokból, sérülésekből a tényállást. Tehát biztonsággal kell bírnia a felhasználással együtt járó környezeti ártalmakat.

Másrészt. A Biztonsági záraknál lehet tapasztalni, hogy a gyártók olyan nagy szakító szilárdságot érnek el a biztonsági zár méretezésénél, hogy megnehezedik a zár eltávolítása a végfelhasználónál vagy az ellenőrzésénél. Mely időveszteségen túl a kinyitás miatti sérülést is okozhat a védendő objektumon, konténeren, vagy az eltávolítást végző személyen. A biztonsági zár az objektumot kell, hogy védje nem tehet kárt benne.

PLOMBA. Tisztázni szeretném miért ide került és miért használom a címben zárójelben a szót. Van egy kiviteli forma melyről még egyáltalán nem esett szó. A rendszerváltás előtt illetve az azt követő években milliós számban használták Magyarországon. Egy csemői Termelő Szövetkezet gyártotta alumínium szalagos kivitelben, melybe kézzel ütötték bele a kívánt szöveget és sorszámozták. A lezárás módja pedig egy patent megoldás volt. Ezért is hívták patentzárnak. Hátránya volt az alumínium szalag sérülése, megvágta a felhelyező kezét, a patent összenyomása nagy erőt kívánt lezárás eszközt igényelt, sokszor nem is zárt csak olyannak tetszett egyszerű szemrevételezéssel. Továbbá rozsdásodott.

Viszont megközelítően tíz-tizenöt évvel ezelőtt egy nagy múlti cég kilobbizta Brüsszelben, hogy Európában a plomba, mint plomba csak ez a fenti megoldás lehet, mert már csak ő gyártotta egyedüliként a világon, hiszen mint láttuk elavult. Tehát a PLOMBA kritériumai a fenti paraméterek, minden más egyszer használatos zár NEM PLOMBA. Sajnálatos módon ez első körben bekerült a VÁM szabályozásba is.

Majd tekintettel a nagy felháborodásra ezt követően a felhasználók részéről, melynek oka a nagy raktárkészlet volt, amit le kellett volna selejtezni és csak ilyen kivitelű zárat beszerezni. A Vám és Pénzügyőrség Országos Parancsnoksága (mai nevén a Nemzeti Adó és Vámhivatal) később módosította, bár meghagyta tájékoztatásként a PLOMBA előírásait, de bármilyen másik zárat is elfogadott egy engedélyezési eljárás keretében. Ez az oka, hogy szaktanulmányomban nem használhatom minden egyszer használatos zárra a plomba megnevezést. A köztudatba, annyira beleült a plomba szó, hogy természetesen szóban lehet használni, de írásban, dokumentumban, rendelésben, hivatkozásban, reklámban, és semmilyen más szerzői jogokat sértő szövegben szövegkörnyezetben ezt nem tehetem meg. Felvetődik Önökben, hogy akkor a piac hogyan válaszolt erre a helyzetre. A válasz nagyon egyszerű, a beszerzéseket nem plombákra írják ki, hanem műanyag zár, jelképes zár, kis fémzár, egyszer használatos zár, házi zár, vámzár, belső használatú zár, rendészeti zár, ellenőrzési zár, magánzár, de a kedvencem a biztonsági kötöző pánt, és a biztonsági műanyag kötöző zár és a vagyonvédelmi biztonsági pánt se rossz. Hát itt tartunk, a név az elnevezés eltérő lehet, de a feladat ugyanaz. Ezzel elérkeztünk a szabályozás témaköréhez, mellyel bővebben a tanulmány második részében foglalkozom.

IRODALOMJEGYZÉK

[1] BERTÉNYI, Iván: Pecséttan, In: A Történelem Segédtudományai. Osiris Kiadó 2001.
[2] FIESZT, György: Rövid magyar címertan és pecséttan. Tankönyvkiadó 1986.
[3] KUMOROVITZ l., Bernát :1944: A magyar pecséthasználat története a középkorban. Gödöllő (bővített kiadás: 1993)
[4] TAKÁCS, Imre: Az Árpád-házi királyok pecsétjei (corpus sigillorum hungariae mediaevalis 1. budapest, 2012
[5] 275/2000. (XII. 28.) Kormány rendelet az egységes árutovábbítási eljárás ek-efta vegyes bizottságának 2000. december 20-i 1/2000. számú határozata kihirdetéséről ii. melléklet a zárak jellemzői https://net.jogtar.hu/jogszabaly?docid=a0000275.kor (letöltve: 2022.02.07.)

THE APPLICATION OF ARTIFICAL INTELLIGENCE IN SMART HOMES

A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA AZ OKOSOTTHONOKBAN

MANDIĆ Dorottya[1]

Abstract

The popularity of smart homes has increased in recent years. Perhaps the COVID-19 pandemic has also contributed to this since people started spending more time in their homes. The smart homes not only provide comfort to users, but also have many other useful features like energy saving or security. Nowadays, we can hear more and more about artificial intelligence. It is used in a variety of fields today, including smart homes. Through artificial intelligence smart homes can be provided with many functions. This study presents the application possibilities and benefits of artificial intelligence on smart homes, as well as the meaning and purpose of smart homes and smart devices.

Keywords

artificial intelligence, AI, smart homes, smart devices, domotics

Absztrakt

Az okosotthonok népszerűsége az elmúlt évek során megnőtt. Ehhez talán a COVID-19 járvány is hozzá járult, hiszen az emberek több időt töltöttek az otthonaikban. Az okosotthon nem csak a kényelmet szolgálja a felhasználók számára, hanem számos egyéb hasznos funkcióval is rendelkezik, mint például az energiatakarékosság vagy a biztonság. A mesterséges intelligenciáról manapság már egyre többet lehet hallani. A mesterséges intelligenciát számos területen alkalmazzák, az egyik ilyen terület az okosotthonok. A mesterséges intelligencia által számos funkcióval bővíthetőek ki az okosotthonok. A tanulmány a mesterséges intelligencia alkalmazási lehetőségeit és előnyeit mutatja be az okosotthonokban, ezen kívül a tanulmányban kitérek az okosotthon jelentésére és céljára, valamint a benne található okoseszközökre.

Kulcsszavak

mesterséges intelligencia, AI, okosotthonok, okoseszközök, domotika

[1] mandic.dorottya@uni-obuda.hu | ORCID: 0000-0002-3384-5590 | PhD Student, Óbuda University Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A globális okosotthonok piaca a Zion Market Research elemzői szerint 2016-ban elérte a 24,10 milliárd dollárt, és a becslések szerint 2022 végére már az 53,45 milliárd dollárt fogja elérni az okosotthonok globális piacának az értéke. [1] A Statista jelentése szerint is az okosotthonok globális piacának az értéke 2022-re elérheti az 53,45 milliárd dollárt. [2] Az okosotthonok iránti kereslet az elmúlt évek során megnőtt, talán a COVID-19 járvány is hatással volt erre, hiszen az emberek több időt töltöttek az otthonaikban. A Xiaomi tanulmánya szerint a fogyasztók körülbelül a 70%-a COVID-19 járvány ideje alatt több időt töltött az otthonában, és ennek a következtében okoseszközökkel próbálták az otthonukat jobbá tenni. [3] A fogyasztók 80%-a szerint előnyös, ha az otthonuk okoseszközökkel van felszerelve. [5] A Safewise adatai alapján 2020-ban az amerikaiak 85%-a vásárolt okosotthoni eszközt, és ebből a vásárlóknak a 75%-a 44-éves vagy fiatalabb személy volt. A legnépszerűbb okosotthoni eszközök az okostévé, az okoshangszóró, és az okosvilágítás volt. A felmérésből ezen kívül kiderül az is, hogy az amerikaiak 55%-a vásárolt új okostévét a COVID-19 járvány ideje alatt, és a megkérdezettek 46%-a állította azt, hogy több pénzt költött az otthoni technikára 2020-ban, és csak a megkérdezettek 22%-a állította azt, hogy kevesebb pénzt költött. Ez mellett a biztonságra is figyelmet fordítottak az otthonaikban, hiszen az okoscsengő, okoskamera, és az okos zár is népszerű volt. [4] A Samsung Electronics 2021-ben kutatást végzett Magyarországon az Impetus Research által. A kutatásból kiderült, hogy Magyarországon a COVID-19 járvány ideje alatt a válaszadók közül legtöbben okostelefont, televíziót, és számítógépet vásároltak. A felmérésből az is kiderült, hogy a válaszadók többsége már hamarabb is tervezte az eszköz megvásárlását, de volt olyan válaszadó is, aki a kialakult helyzet miatt vásárolt új eszközt. A válaszadók a COVID-19 járvány ideje alatt legtöbben az okoseszközeiket az otthonukban munkára, tanulásra, kikapcsolódásra és a kapcsolattartásra használta. [35] A mesterséges intelligenciáról egyre többet hallunk napjainkban, és sokan a jövő meghatározó technológiájaként említik meg. A mesterséges intelligenciát napjainkban számos területen alkalmazzák, ezek közöl csak néhányat említenék meg, mint például az épületek, városok, ipar 4.0, robotika, honvédelem, egészségügy, gazdaság, oktatás. [6] A mesterséges intelligenciának a rövidítése az (MI) az angol jelentése pedig az Artificial Intelligence (AI). A mesterséges általános intelligencia egy olyan gépi intelligencia, amely képes megérteni és megtanulni bármilyen szellemi feladat elvégzését, amire úgy mond az ember is képes. [9] A mesterséges intelligencia alkalmazása az okosotthonokban számos lehetőséget kínál az okosotthon tulajdonosai, és az ott lakók számára, amivel a hétköznapi tevékenységeik elvégzését könnyebbé és jobbá tehetik. A Statista jelentése szerint a mesterséges intelligencia (AI) globális piacának az értéke az elkövetkező években gyorsan fog növekedni, és várhatóan 2025-re elérheti a 126 milliárd dollár értéket. [8]

Az okosotthon jelentése és célja

A világon jelenleg 175 millió okosotthon létezik, és ebből 63 millió okosotthon az Egyesült Államokban található meg. A Consumer Technology Association (CTA) statisztikái szerint az amerikai otthonok 69%-ban található legalább egy okoseszköz. [10] Magyarországon a Nemzeti Média és Hírközlési Hatóság 2020-as jelentése szerint a fogyasztóknak csak a 4%-a rendelkezik okosotthon eszközökkel. A megkérdezettek közül

93%-a azt válaszolta, hogy rendelkezik okostelefonnal, még a 63%-a laptoppal, 32%-a tablettel, valamint a megkérdezettek közül a 44%-a rendelkezik okostévével. Ezen kívül a megkérdezettek 18%-a válaszolta azt, hogy rendelkezik játékkonzollal, 20%-a viselhető eszközzel, mint például az okosóra, 4%-a VR-eszközzel, 3%-a drónnal, 2%-a okosautó eszközzel, a válaszadók 1%-a azt válaszolta, hogy rendelkezik ezeken kívül más okoseszközzel. A jelentésből az is kiderül, hogy a magasabb iskola végzetségűek, illetve a jobb anyagi helyzettel rendelkezők körében az okoseszközök használata sokkal népszerűbb. A megkérdezettek közöl, a 70 év feletti személyek, több mint háromnegyede okostelefont használ az internet használatára. Az internetezésre használt eszközök közül az okostelefon került az első helyre, a válaszadók 83%-a az okostelefont használja az internet használatára. [26] Az NRC 2019-ben okosotthon kutatást végzett Magyarországon, és a kutatásból kiderült, hogy az internet használók négyötöde hallott már az okosotthon fogalmáról, és kicsivel több mint a válaszolók fele állította azt, hogy tudja mit is jelent az okosotthon. Ezen kívül az okosotthon eszközismeret szerint a válaszolók 96%-a állította, hogy hallott már róla, 73%-a találkozott már vele, és 41%-a válaszolta azt, hogy rendelkezik is vele. Az okosotthonban található okoseszközök ismeretéről szinte alig volt olyan válaszadó, aki azt állította volna, hogy nem hallott legalább egy ilyen eszközről, és a válaszadók 64%-a szeretne a közeljövőben legalább egy ilyen eszközt vásárolni az otthonában. A vásárlók körében fontos az energiatakarékosság, kényelem, költségcsökkentés, betörésvédelem, vészhelyzetek észlelése és elhárítása, valamint az időmegtakarítás. Manapság az okosotthon kifejezéssel egyre gyakrabban találkozhatunk viszont még mindig sokan nem ismerik az okosotthon jelentését. Az NRC 2019-es kutatása szerint az internetezők egy része, nincs tisztában azzal, hogy mennyi mindent jelenthet az okosotthon fogalma, és az ismereteik a gyártókkal szemben is hiányosak. Sokan nincsenek tisztában azzal sem, hogy milyen eszközök által tudnák otthonukat okossá tenni. A megkérdezettek közül legtöbben okostévével, termosztáttal, és biztonsági kamerarendszerrel rendelkeznek. [30] Mit is értünk okosotthon alatt? Az okosotthon vagy angolul smart home alatt, egy olyan épületet értünk, amely úgy mond magában foglalja azokat a technológiai megoldásokat, amelyek által automatizálni tudjuk az otthonunkat. Az okosotthon esetében az IoT eszközöket is meg kell említeni, amelyeket okoseszközöknek is szoktak hívni. Az Internet of Things (IoT) jelentése magyarul a dolgok internete. [10] Az Internet of Things kifejezést Kevin Ashton használta először 1999-ben. [22] Az Internet of Things (IoT) vagy magyarul a dolgok internete alatt értünk, minden olyan dolgot és használati tárgyat, amelyet egy hálózaton keresztül más gépekhez csatlakozva működnek emberi beavatkozás nélkül is. [34] Lényegében ezek az eszközök képesek arra, hogy emberi beavatkozás nélkül is tudjanak egymással kapcsolatot létre hozni, kommunikáljanak egymással, valamint adatokat gyűjtsenek és továbbítsanak. Az eszközök egymás közötti kommunikációját, ami emberi beavatkozás nélkül történik azt M2M (Machine-to-Machine) vagy gép-gép kommunikációjának nevezünk. [11] Az IoT eszközök az okosotthonban lehetnek például az okostévé, okoshűtő, okosvilágítás. Az IoT eszközök száma napjainkban rohamosan nő, ezért csak felbecsülni tudjuk a pontos számukat. Az IoT Analitycs jelentése szerint az IoT eszközök száma 2015-től 2025-ig elérheti a 30.9 milliárd eszközt. [14] Az okosotthon esetében fontos megemlíteni, hogy többféle képen tudjuk vezérelni az otthonunkat ez lehet például kézi vezérlés alapján, időponthoz kötve, vagy a külső környezeti tényezők hatására. A vezérlést a következő eszközökkel tudjuk biztosítani az okosotthonban például a távirányító, intelligens fali gomb, okostelefon, laptop. [12] Az okosotthonok egyik nagy

előnyeként megemlítendő, hogy a világ bármely pontjáról ellenőrizni tudjuk az okosotthonunkat. [25] Az okosotthon céljaiként meg kell említeni a kényelmet, a biztonságot, és a költségmegtakarítást. [13] Az okosotthonok mondhatjuk azt, hogy elsősorban a kényelmet szolgálják, de ez mellett az energiamegtakarítás is fontos az okosotthonokban. Az okosotthonban az egyik legnagyobb energiamegtakarítást az okosfűtéssel tudjuk elérni. [31]

Az International Data Corporation (IDC) szerint az európai okosotthonok piaca 2021 második negyedévében 29,1%-kal nőtt Közép és Kelet-Európában. [20] A legnépszerűbb öt márka Európában az Amazon, Google, Samsung, LG Elektronics, és a Hisense. Az 1.ábrán láthatjuk, hogy 2020-ban az Amazon 19.4%-ot ért el a többi márkához képest, ezt követi a Google 11.3%-kal, a Samsung 10.6%-kal majd az LG Elektronics 8.8%-kal, és a Hisense 6%-kal az egyéb márkák összesen 43.9%-ot értek el. Ha megnézzük a 2021-es évet, akkor láthatjuk, hogy az Amazon 16%-ot ért el, a Google 12.8%-ot, a Samsung 10.3%-ot, az LG Elektonics 8.7%-ot, és a Hiense márka 5%-ot ért el, az egyéb márkák pedig 47.2%-ot érték el. Ha összehasonlítsuk a 2021-es és a 2020-as évet, akkor láthatjuk, hogy a Google esetében növekedés történt 2021-ben 1.5%-kal.

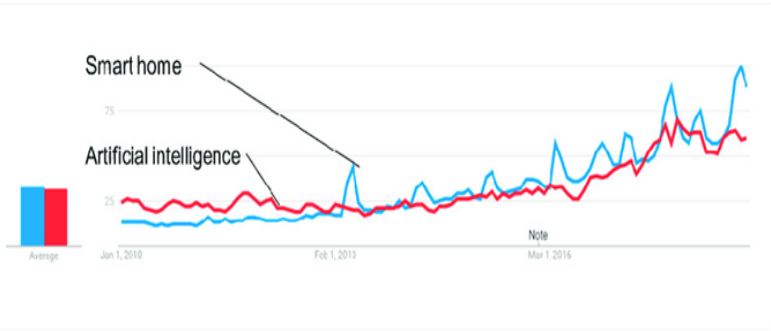
Márka	Év	
	2021	2020
Amazon.com	16 %	19.4%
Google	12.8%	11.3%
Samsung	10.3 %	10.6%
LG Elektonics	8.7%	8.8%
Hisense	5 %	6.0%
Egyéb márkák	47.2%	43.9%
Összesen	100%	100%

1. ábra. A legnépszerűbb öt márka Európában.
Forrás: IDC Worldwide Quarterly Smart Home Device Tracker, September 2021, saját szerkesztés

Az IDC jelentése szerint az okostévékre megnőt a kereslet, valamint az okosotthonban található termékek közül a felhasználók körében igen népszerű volt az okoshangszóró, világítás, otthoni biztonság, valamint a termosztát. [20]

A mesterséges intelligencia az okosotthonokban

Feltehetjük a kérdést, hogy mire alkalmazható az okosotthonokban a mesterséges intelligencia? A mesterséges intelligenciát, ahogy már írtam is a jövő technológiájaként említik meg, és egyre több területen alkalmazzák napjainkban. A mesterséges intelligencia alkalmazásának számos előnye lehet az okosotthonokban.



2.ábra. Az okosotthon és a mesterséges intelligencia iránti érdeklődés. [21]

Az általános mesterséges intelligenciának az a célja, hogy az emberi gondolkodáshoz és cselekvéshez hasonló teljesítményű gépeket próbáljon létre hozni. Az intelligens viselkedés egy része a tanulási képességnek, amire a gépi tanulás területe próbál összpontosítani. A gépi tanulás (Machine learning) a mesterséges intelligencia részterülete. [28] A mély tanulás (Deep Learning) a gépi tanulási technikák egyik alcsoportja, amelynél mesterséges neurális hálózattokat (Neural Networks) használnak. [29] A mesterséges intelligencia által, mint például a beszédfelismerés vagy a virtuális képi azonosítása az okosotthon tulajdonosa számára, illetve az okosotthon lakói számára hasznos megoldásokat nyújthat. Az okosotthonokban a mesterséges intelligenciát csoportokra tudjuk felosztani, mint például a tevékenységfelismerésre, adatfeldolgozásra, hangfelismerésre, képfelismerésre, döntéshozatalra vagy az előrejelzésre. Például a tevékenységfelismerés esetében az okosotthoni eszközök képesek felismerni az emberi tevékenységet a mesterséges intelligencia által. A képfelismerés szempontjából a mesterséges intelligencia az arcfelismerésre vagy az érzelemfelismerésre is tudjuk használni. Ezen kívül például elemezni tudja az emberi viselkedést, valamint a test felépítésének a formáit. De mire is jó ez az okosotthonokban? Például biztonság szempontjából, ha az okosbiztonsági rendszer a kamerán keresztül észleli, hogy egy ismeretlen személy akar az otthonunkba betörni, akkor ebben az esetben elindítsa a riasztást és értesíteni fogja a tulajdonost például az okostelefonjára, ezen kívül automatikusan hívni fogja a rendőrséget. [21] Az okosotthon esetében a mesterséges intelligencia (AI) automatikusan működhet, mint adatgyűjtő és elemző, valamint döntéshozó rendszer. [15] Az okosotthon rendszerek, mint például az Amazon Alexa az Amazon saját fejlesztésű mesterséges intelligenciája, amelyre akár komplett okosotthonos rendszereket, vagy hang alapú vezérlés építhető fel. Ide tartozik az Amazon Echo okoshangszóró, amely képes rögzíteni a hangalapú utasításokat, és a hang alapján a felhasználó irányíthatja az okosotthonban például a világítást vagy a különféle okoseszközöket. A Google Home az egyik legismertebb okosotthon rendszer, amelynél a Google Asszisztens fog a felhasználóknak segíteni az otthon irányításában, valamint a keresésben is. Az előnyeként megemlítendő, hogy a Google Asszisztens folyamatosan tanuló, illetve a felhasználóhoz alkalmazkodó mesterséges intelligencia. Hiszen képes például megtanulni a felhasználó szokásait, vagy ez alapján próbál különféle funkciókat ajánlani a felhasználónak. Az Amazon, és a Google mellett az Apple Home Kit is jelenleg kedvelt a felhasználók körében. Az Apple esetében a Siri nevű mesterséges intelligencia fog segítséget nyújtani a felhasználónak, amivel a HomePod okoshangszórón keresztül fog majd tudni kommunikálni a felhasználó. [16] Az okoshangszórók

iránti érdeklődés megnőtt a felhasználók körében, és egyre elterjedtebbek napjainkban például 2022-re az Egyesült Államokban a háztartások becslések szerint az 55%-a okoshangszóróval fog rendelkezni. A mesterséges intelligenciát ezen kívül az okosotthonokban az adatok, és az információk felhasználásával az otthon teljesítményének a javítására is használható, valamint a felhasználók kényelmének a növelésére. A mesterséges intelligencia az okosotthonokban az összegyűjtött adatok által olyan viselkedést képes kialakítani, amely megfelel a mindennapi életünk számára, mint például megtanulja, hogy ne kapcsolja be a fűtést, ha nem tartózkodunk otthon, ami által például energiát tudunk megtakarítani az okosotthonunkban. [17] A mesterséges intelligencia által a biztonság is magasabb szintre tehető fel, hiszen például az arcfelismerés segítségével az otthonunk riasztórendszere felismeri, hogy például ki áll a bejárati ajtónk előtt. Ha felismeri az adott személyt az arcfelismerés segítségével, akkor kinyithatja neki például az ajtót, ha ismeretlen a személy azt is jelezheti a tulajdonosnak. [7] Lényegében mondhatjuk azt, hogy a mesterséges intelligencia az okosotthonokban segíti az ott lakók tevékenységeinek az elvégzését, valamint megkönnyíti, és próbálja jobbá tenni az ott lakók életét, valamint biztonságot is javítja. Az LG márka például kifejlesztette a DeepThinQ 1.0 platformot, amely olyan mesterséges intelligencia funkciókat tartalmaz, mint például a hang, videó, szenzorfelismerés. A DeepThinQ platformon a fejlesztett termékek a felhőalapú szervereken keresztül önmagukat tanítják, ami által az idő elteltével egyre okosabbak fognak lenni. Ez a tanulási tulajdonság a DeepThinQ technológia alapja, amely által az LG AI-termékei nem csak a környezetüket, hanem a tulajdonosuk viselkedési mintáit is értelmezni tudják. [18] [19]

ÖSSZEGZÉS

Az összegzésként elmondhatjuk, hogy a mesterséges intelligencia használata az okosotthonokban igen hasznos, ami által az okosotthonok tulajdonosai, és az ott lakók kényelme a hétköznapi tevékenységeik elvégzése egyszerűbb és könnyebb lesz, ezen kívül az okosotthon biztonsága is javítható a mesterséges intelligencia által. A tanulmányban megpróbáltam bemutatni a mesterséges intelligencia egyes alkalmazási lehetőségeit, és előnyeit az okosotthonokban. A mesterséges intelligencia által az okosotthonok még jobbá, és energiahatékonyabbá tehetők. [24] Láthatjuk, hogy a mesterséges intelligencia alkalmazása számos előnnyel jár az okosotthonokban. Várhatóan a jövőben az okosotthonok iránti érdeklődés még nagyobb növekedést fog mutatni, hiszen az okosotthonok használata számos előnnyel jár. Az okosotthon előnyei mellett nem szabad megfeledkeznünk a biztonságról sem, hiszen az okosotthonok különféle biztonsági kihívásoknak lehetnek kitéve, mint például a lehallgatás, megfigyelés vagy az adatlopás. [32] Egy felmérés szerint az Európa Unió lakosságának az 55%-a fél attól, hogy a személyes adatai bűnözők kezébe fog kerülni. [33] Ezen kívül a mesterséges intelligencia terjedése szintén nem csak pozitív hatással lehet az életünkre, akár negatív következményei is lehetnek. Az európai lakosság 61%-a pozitív véleménnyel van az MI, és a robotok által kínált lehetőségekre, viszont fontosnak tartsák a technológia megfelelő kezelését. [36] Az Európai parlement külön bizottságot hozott lére, hogy a mesterséges intelligencia hatását vizsgálja. A mesterséges intelligenciának számos előnye van, viszont jogosan feltehetjük azt a kérdést ki felel azért, ha például a mesterséges intelligenciával működtetett eszköz vagy szolgáltatás valamilyen kárt okoz. [23] A jövőben várhatóan a mesterséges intelligencia igen nagy változásokat fog előidézni a társadalomban

és a gazdaság működésében. [27] Fontos lenne, hogy a mesterséges intelligencia előnyei mellett a kihívásokra még nagyobb hangsúlyt fektessünk.

FELHASZNÁLT FORRÁSOK

[1] Global Smart Home Market Increasing At A Good Pace To Reach USD 137.9 billion by 2026, [Online]. Elérhető: https://www.zionmarketresearch.com/news/smart-home-market (Letöltve: 2021. 11. 01.)
[2] Forecast market size of the global smart home market from 2016 to 2022 (in billion U.S. dollars), [Online]. Elérhető: https://www.statista.com/statistics/682204/global-smart-home-market-size/ (Letöltve: 2021. 11. 01.)
[3] Mit jelent a COVID-19 az intelligens otthoni technológiához? [Online]. Elérhető: https://hu.denizatm.com/pages/48116-what-covid-19-has-meant-for-smart-home-technology (Letöltve: 2021. 11. 01.)
[4] Smart Home Spending Increased since Start of Pandemic, [Online]. Elérhető: https://www.safewise.com/blog/smart-home-tech-spending/ (Letöltve: 2021. 11. 03.)
[5] New Xiaomi survey explores how Covid-19 is driving the new smart home, and what it means for 2021 and beyond, [Online]. Elérhető: https://techcrunch.com/sponsor/ xiaomi/new-xiaomi-survey-explores-how-covid-19-is-driving-the-new-smart-home-and-what-it-means-for-2021-and-beyond/ (Letöltve: 2021. 11. 05.)
[6] Kollár, Csaba: A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 47-61., 15 p
[7] Mesterséges intelligencia az IoT könnyebbé tételére, [Online]. Elérhető: https://www.magyar-elektronika.hu/10005-tartalom/2876-mesterseges-intelligencia-az-iot-konnyebbe-tetelere (Letöltve: 2021. 11. 08.)
[8] Artificial intelligence software market revenue worldwide 2018-2025, [Online]. Elérhető: https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-mar ket-revenues/ (Letöltve: 2021. 11. 08.)
[9] Mesterséges intelligencia: A negyedik ipari forradalom, [Online]. Elérhető: https://books.google.rs/books?id=tx3NDwAAQBAJ&printsec=frontcover&hl=sr#v=one page &q&f=false (Letöltve: 2021. 11. 15.)
[10] Hogy működik, mennyibe kerül és egyáltalán mi az az okosotthon? [Online]. Elérhető: https://xiaomishop.hu/hogy-mukodik-mennyibe-kerul-es-egyaltalan-mi-az-okos otthon (Letöltve: 2021. 11. 15.)
[11] Kovács László: A kibertér védelme, Dialóg Campus Kiadó, Budapest, 2018
[12] Minden, amit az okosotthonokról tudni kell, [Online]. Elérhető: https://www.intelligensotthon-tudastar.hu/ (Letöltve: 2021. 11. 17.)
[13] Mi az okosotthon? [Online]. Elérhető: https://www.okosotthonok.com/hu/mi-az-okosotthon-mob (Letöltve: 2021. 11. 18.)
[14] State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time, [Online]. Elérhető: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-conn ections-surpassing-non-iot-for-the-first-time/ (Letöltve: 2021. 11. 20.)
[15] Toth, Andras. (2018). A mesterséges intelligencia és az IoT összekapcsolásának lehetőségei, [Online]. Elérhető: https://www.researchgate.net/publication/349946778_A_me

sterseges_intelligencia_es_az_IoT_osszekapcsolasanak_lehetosegei (Letöltve: 2021. 11. 21.)
[16] A legjobb okosotthon rendszerek, [Online]. Elérhető: https://chameleon-smart_home.com/blog/cikk/a-legjobb-okosotthon-rendszerek (Letöltve: 2021. 11. 23.)
[17] The Helpful Future of Smart Home Automation Is Sooner Than You Think [Online]. Elérhető: https://ambiq.com/the-helpful-future-of-smart-home-automation-is-sooner-than-you-think/ (Letöltve: 2021. 11. 26.)
[18] Smart Homes: Impact of Artificial Intelligence in Connected Home [Online]. Elérhető:https://www.futurebridge.com/blog/smart-homes-impact-of-artificial-intelligence -in-connected-home/ (Letöltve: 2021. 11. 26.)
[19] DeepThinQ technológia az LG termékekben, [Online]. Elérhető: http://www.audi ovideo-trend.hu/multimedia/deepthinq+technologia+az+lg+termekekbe n. html (Letöltve: 2021. 11. 27.)
[20] Amazon Regains the Number 1 Spot in Another Successful Quarter for the European Smart Home Market, Says IDC, [Online]. Elérhető: https://www.idc.com/get doc.jsp? containerId=prEUR148282621(Letöltve: 2021. 11. 28.)
[21] Guo, Xiao, Zhenjiang Shen, Yajing Zhang, and Teng Wu. 2019. "Review on the Application of Artificial Intelligence in Smart Homes" Smart Cities 2, no. 3: 402-420. https://doi.org/10.3390/smartcities2030025
[22] Why the Internet of Things is called Internet of Things: Definition, history, disambiguation, [Online]. Elérhető: https://iot-analytics.com/internet-of-things-definition/ (Letöltve: 2021. 11. 29.)
[23] A mesterséges intelligencia használata és veszélyei, [Online]. Elérhető: https://www.europarl.europa.eu/news/hu/headlines/society/20200918STO87404/a-mesterseges-intelligencia-hasznalata-es-veszelyei (Letöltve: 2021. 11. 29.)
[24] A mesterséges intelligencia is betör az otthonokba, [Online]. Elérhető: https://iotzona.hu/szorakozas/a-mesterseges-intelligencia-is-betor-az-otthonokba (Letöltve: 2021. 11. 29.)
[25] Teljes körű távoli hozzáférés,[Online]. Elérhető: https://www.okosotthon. me/teljeskoru-tavoli-hozzaferes/ (Letöltve: 2021. 11. 30.)
[26] Az elektronikus hírközlési piac fogyasztóinak vizsgálata, [Online]. Elérhető: https://nmhh.hu/dokumentum/218531/internetes_felmeres_2020.pdf (Letöltve: 2021. 11. 30.)
[27] Kollár Csaba: A mesterséges intelligencia kapcsolata a humán biztonsággal. *Nemzetbiztonsági Szemle*, MMXVIII évf. I. szám, pp. 5-23. 2018.
[28] Gépi tanulás, [Online]. Elérhető: https://www.inf.u-szeged.hu/~rfarkas/ML20 /M_L intro.html (Letöltve: 2021. 11. 30.)
[29] Mély gépi tanulás (Deep learning), [Online]. Elérhető: https://www.inf.u-szeged.hu/~rfarkas/ML20/deep_learning.html (Letöltve: 2021. 11. 30.)
[30] Okosotthon kutatás 2019, [Online]. Elérhető: https://nrc.hu/nrc-hirek/okosotthon-kutatas/ (Letöltve: 2021. 12. 03.)
[31] Energiamegtakarítás egyszerűen, [Online]. Elérhető: https://www.okosotthon. me/energiamegtakaritas/ (Letöltve: 2021. 12. 05.)
[32] Csepeli György: Ember 2.0: A mesterséges intelligencia gazdasági és társadalmi hatásai, [Online]. https://books.google.rs/books?id=9mz1DwAAQB AJ&printsec= frontcover&redir_esc=y#v=onepage&q&f=false (Letöltve: 2021. 12. 05.)

[33] A biztonsági unióra vonatkozó uniós stratégia, [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0605&from=EN (Letöltve: 2021. 12. 06.)
[34] A tárgyak internete-IoT, [Online]. Elérhető: https://hu.rs-online.com/web/gener alDisplay.html?id=i/iot-internet-of-things (Letöltve: 2021. 12. 07.)
[35] Sok az új okoseszköz a magyar háztartásokban, de a bevásárlólista még nem üres, [Online]. Elérhető: https://www.samsung.com/hu/news/local/sok-az-uj-okoseszkoz-a-magyar-haztartasokban-de-a-bevasarlolista-meg-nem-ures/ (Letöltve: 2022. 03. 03.)
[36] Mi a mesterséges intelligencia és mire használják? [Online]. Elérhető: https://www.europarl.europa.eu/news/hu/headlines/society/20200827STO85804/mi-az-a-mesterseges-intelligencia-es-mire-hasznaljak (Letöltve: 2022. 03. 04.)

INTEGRATED RISK MANAGEMENT | **INTEGRÁLT KOCKÁZATKEZELÉS**

KEMENDI Ágnes[1]

Abstract

In order to maintain a long-term successful operation, complex security challenges need to be managed by companies. With the proliferation of information and communication technologies (ICTs), more and more risks are emerging. The quality of the risk management process is crucial. Integrated risk management includes the management of ICT risks at a strategic level. The publication examines the role of risk management and discusses risk management systems, methods, and potential ways of working. The publication focuses on the sales process and reviews corporate risks and possible controls; and it builds the risk matrix of a fictitious company in the form of a case study on ICT risks. The risk management process must be continuously operated as part of the company's strategic considerations, and risks must be assessed and managed on a cycle basis. Managing the risks associated with particularly large-scale projects is essential for successful corporate operations. Risk management contributes to the successful and secure operation of companies in the long run, which requires significant resources to be considered.

Keywords

integrated risk management; risk matrix; ICT; control; sales

Absztrakt

A vállalatok komplex biztonsági kihívásait a hosszú távú sikeres vállalati működés érdekében kezelni kell. Az információs és kommunikációs technológiák (IKT) intenzív térnyerésével újabb és újabb kockázatok merülnek fel. A kockázatkezelési folyamat minősége meghatározó. A kockázatok stratégiai szinten történő integrált kezelése magában foglalja az IKT kockázatok stratégiai szinten történő kezelését is. A publikáció a kockázatkezelés szerepét vizsgálja, a vállalati kockázatokból kiindulva tárgyalja a kockázatkezelési rendszereket, módszereket és lehetőségeket, továbbá az értékesítési folyamatra fókuszálva áttekinti a vállalati kockázatokat, és lehetséges kontrollokat, és az IKT kockázatokra vonatkozóan esettanulmány jelleggel felépíti egy fiktív vállalat kockázati mátrixát. A kockázatkezelési folyamatot körfolyamat jelleggel a vállalati stratégiai megfontolások részeként folyamatosan kell működtetni. A jelentős volumenű projektekkel járó kockázatok kezelése a sikeres vállalati működéshez elengedhetetlen. A kockázatkezelési folyamat a hosszú távon sikeres és biztonságos vállalati működéshez járul hozzá, amely mögötti számottevő erőforrás-ráfordítást mérlegelni szükséges.

Kulcsszavak

integrált kockázatkezelés; kockázati mátrix; IKT; kontroll; értékesítés

[1] kemendi.agnes@@uni-obuda.hu | ORCID: 0000-0002-6452-8563| PhD. Student Óbuda University Doctoral School on Safety and Security Sciences | PhD. hallgató Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A sikeres vállalati működés szempontjából meghatározó a vállalati kockázatkezelés szerepe, a kockázatok feltárásának folyamata, a várható valószínűségek azonosítása, és a még elfogadható kockázat mértékének meghatározása. A vállalatok folyamat-szervezésével kapcsolatos kockázatok átfogó, szisztematikus áttekintésével a szervezeti kockázati tényezőkről nyerhető információ. Az érintett területek, kockázatok, és hibaforrások feltárása, valamint a kockázatkezelési eszközök alkalmazása a hosszú távú sikeres vállalati működéshez elengedhetetlen. Az általános vállalati kockázatkezelés rendszerén belül az informatikai kockázatok értékelése kulcsfontosságú. Az IKT-k a vállalati folyamatok szerves részévé váltak. Az IKT technológiák alkalmazása vállalati értéknövelő tényezőként jelenhet meg, hozzájárulva a piaci versenyképességhez, és naprakészséghez. A rendszer, ill. szoftver-implementáció mögötti beruházási döntések megfigyelése képet ad a vállalati stratégiai megfontolásokról is. A publikáció célja az integrált kockázatkezelési megközelítésen alapulóan ismertetni a vállalati kockázatokat, keretrendszert teremteni a vállalati kockázatok strukturálásához és értékeléséhez. A publikáció középpontba helyezi az IKT-k (információs – és kommunikációs technológiák) szerepét az integrált kockázatkezelés keretei között. A publikáció a vállalati kockázatok áttekintésén keresztül vezeti fel a tématerületet, és vizsgálja a kockázatkezelési keretrendszereket és szabványokat, azok eszköztárait, és megjelenését a vállalati gyakorlatban. A publikáció a vállalati kockázatokat integrált megközelítéssel mutatja be; a vállalati értékesítési folyamat példáján keresztül ismerteti a főbb kockázatokat és lehetséges kontrollokat, valamint esettanulmány jelleggel levezeti egy elektronikus kereskedelmi (e-kereskedelmi) piacra lépési projektben érintett fiktív vállalat IKT kockázati mátrixának elkészítésének folyamatát, és lehetséges kockázatkezelési megoldásokat azonosít.

VÁLLALATI KOCKÁZATOK ÁTTEKINTÉSE

A kockázatok elleni védelem az egész szervezet működését áthatja, ebből kifolyólag a szükséges és elégséges védelmi háló több szinten is megjelenik a kapcsolódó kockázatokhoz kötődően. A védelem kérdésköre stratégiai jelentőségű, ennek részterületei: személy- és vagyonvédelem, az adat-, információ- és információtechnológiai védelem, az integritási, korrupciós és egyéb humán kockázatok kezelése, az üzletbiztonság, az üzletmenet-folytonosság és a váratlan havária események (kockázatok) kezelése, illetve azok elhárítása [1].

A potenciális kockázatok belső -, és külső kockázatok formájában vannak jelen. Külső kockázatok a jogszabályi kockázatok, országkockázat, hitel-/kamat-/árfolyamkockázatok, beszállítói/partner kockázat, ügyfélkockázatok, természeti-, környezeti kockázat, biztosítási kockázatok [1]. A belső kockázatok a szervezeti működésre vezethetőek vissza, melynek részei a berendezések meghibásodásával kapcsolatos technológiai kockázatok, vagyoni-, gazdálkodási-, likviditási- és adósságkockázatok, reputációs kockázatok, informatikai kibertér és információs technológia, HR, valamint az etikai és korrupciós kockázatok is [1]. A vállalati életben az IKT-hoz kapcsolódó projektek a szervezeti változás motorjaiként jelennek meg. Ezek a projektek - a kapcsolódó bizonytalanság, illetőleg a szervezetre, annak eredményességére gyakorolt hatásai miatt - megfelelő kockázatkezelést tesznek szükségessé. A biztonság az alkalmazásfejlesztők számára a fejlesztés során sokszor nem elsődleges prioritás, így az alkalmazások jóváhagyása és bevezetése során erre különös tekintettel kell

lenni. A technológiai fejlesztésekkel párhuzamosan biztonsági kérdések folyamatos kezelése is szükségessé válik.

Az ipar 4.0. kontextusában az információbiztonság, és vele együtt az IKT biztonság szerepe nő, és meghatározó a hosszú távú sikeres vállalati működés szempontjából. Az IKT technológiák biztonságtechnikai szempontból számos „rést" hagynak nyitva, melyek támadási célpontok lehetnek. Az IKT biztonság a vállalatok számára stratégiai kérdéssé, illetőleg céllá vált, melyhez kötődően megfelelő „védelmi" terv készítése, és működtetése vált szükségessé a kockázatkezelési folyamat részeként. IKT projektekhez kapcsolódóan a reális projektterv, a projekt kezdetén különösen alapos kockázatelemzés, és - kezelés, a bizonytalansági tényezők alapos feltárása és számbavétele, gyökérokok feltárása, valamint a folyamatos visszacsatolások (monitoring) a siker kulcstényezőiként jelennek meg.

A rendszerek és folyamatok működtetése során információ-biztonsági elvek követése és kontrollok működtetése szükséges. A megfelelően kontrollált folyamatok a vállalatbiztonság megteremtését segítik. Ehhez azonban jól kiépített támogató infrastruktúra kiépítése, működtetése és monitorozása szükséges. Fontos a teljesség, teljeskörűség, valamennyi érintett vállalati folyamat feltérképezése és lefedése, mely megvalósítása szétaprózott, fragmentált folyamatok esetében nem várt nehézségekbe ütközhet, és különös odafigyelést kíván.

KOCKÁZATKEZELÉSI KERETRENDSZEREK ÉS SZABVÁNYOK

A kockázatkezelés hagyományos és vállalati szintű kezelése között határozott különbség van [2]. A két kockázatkezelési megközelítés közötti alapvető különbségeket a KPMG LLP. cég foglalta össze, és bemutatja, hogy a hagyományos kockázatkezelési megközelítés leginkább a kockázatok kezelésének folyamatos és reaktív rendszere [3]. A vállalati kockázatkezelés célja, hogy egy olyan keretrendszert teremtsen, amely képes biztosítani, hogy a vállalat a kockázatokat, és bizonytalanságokat kezelni tudja [4].

A kockázatkezelés folyamata a vállalatok stratégiai fejlesztésének része, és azt a legmagasabb szinten kell meghatározni. Az integrált kockázatkezelés értelmében valamennyi kockázatot értékelni, kontrollálni, és monitorozni kell a vállalat kitettségének megfelelően [4]. Az ISO 31000 kockázatkezelési szabvány a kockázatot a bizonytalanság vállalati célokra való hatásaként értelmezi [5; 6], mindez rámutat arra, hogy a kockázatkezelés a vállalati stratégiai célok szintjén integráltan kezelendő. A vállalati szintű kockázatkezelés során a kockázatok az üzleti stratégia kontextusába vannak helyezve, és „a kockázat mindenki felelőssége", mellyel szigorúan elhatárolódik a megközelítés attól, hogy a szervezet tagjai arra hivatkozhassanak, hogy mindez nem tartozik az ő felelősségi körükbe [3]. A kockázatkezelés integrált keretrendszere azt a lényegi összefüggést mutatja be, amely a vállalati stratégiai célok megvalósítása és az IKT rendszerek szerepe - vállalati üzleti célok -, vezetői döntéshozatal -, valamint a stratégiai versenyelőny támogatása [7] – között húzódik.

A szabványok, pl. ISO 31000 kockázatkezelési szabvány erőteljesen befolyásolják a kockázat, és biztonság területet, annak ellenére, hogy erőteljes kritikai hangok kérdőjelezik meg a minőségüket [8]. Az ISO 31000 szabvány értelmében a kockázatkezelés célja értékteremtés és annak védelme. Az integrált kockázatkezelés ISO 31000 szerinti megvalósítása segíti a vállalatot céljai elérésében, és a reziliencia megteremtésében negatív hatások esetén [9]. A szabványok elősegítik a transzparenciát, az összehasonlíthatóságot, és ezáltal a költséghatékonyabb ellenőrzést is. A szabványokban a hatályuk alá tartozó terület pontosan le

van fektetve, ezáltal beazonosítható, hogy mire vonatkozik, és mire nem. Nem elvárható, hogy taxatív megoldást kínáló lexikont keressünk benne, hanem inkább egy jógyakorlatokat tartalmazó keretrendszerként érdemes rájuk tekinteni, amit adaptálni kell.

A COSO keretrendszer a vállalati célokat stratégiai, operatív, riporting és megfelelési célok szerint értelmezi. A COSO keretrendszer a belső kontrollrendszer integritását mutatja be, és szemlélteti, hogy az üzleti célok - stratégiai, operatív, riporting és megfelelési célok – érdekében milyen kontrollfolyamatok valósulnak meg a különféle szervezeti szinteken [10]. A COSO vállalati kockázatkezelés integrált keretrendszere (COSO Enterprise Risk Management – Integrated Framework) fókuszba helyezi a kockázatkezelést. A COSO ERM keretrendszer a kontrollkörnyezet, célok felállítása, események azonosítása, kockázatértékelés, kockázati válaszok, kontrolltevékenységek, információ és kommunikáció, és monitoring elemeket tartalmazza [10].

Az informatikai biztonság a vállalati biztonság része. Az informatikai rendszerek a vállalati folyamatokról adnak állapotjelentést, és a vállalati stratégia mindennapi megnyilvánulásaként is értelmezhetőek. Az IKT technológiák hatékony alkalmazása értéket állít elő, hozzájárul az üzleti célokhoz, és ezáltal a hosszú távú vállalati sikerességhez. Az informatikai kockázatok kulcskockázatok a vállalati biztonság szempontjából, melyek kezeléséhez speciális kockázatkezelési keretrendszerek nyújtanak támaszt.

A COSO keretrendszernek is része az információ és kommunikáció, azonban mint IT folyamatspecifikus funkcionális területre vonatkozóan több szabvány és ajánlás is alkalmazható, mint a CObIT 5.0 az IT irányítás- és menedzsment keretrendszere és a NIST 800-53-as amerikai biztonsági és adatvédelmi ellenőrzések dokumentum [11; 12].

Az információbiztonsági irányítási rendszer az átfogó irányítási rendszernek az információvédelmet biztosító része, amely figyelembe veszi a működési kockázatokat [13]. Az információbiztonság területére vonatkoznak az ISO/IEC 2700x információbiztonság-irányítás szabványai. Az információbiztonság kockázatmenedzsmenttel foglalkozó szabványa az ISO/IEC 27005 szabvány, mely információbiztonsági kockázatokra vonatkozik, pl. IT vagyonelemek, fenyegetések, meglévő folyamatszabályozások, sérülékenységek, következmények [14].

A CObIT (Control Objectives for Information and related Technology) alkalmazása többek között az IT kockázatkezelés megvalósítását segíti.

A CObIT 5 alapelvek és annak megvalósítását segítő tényezői lehetővé teszik a szervezet számára, hogy IT beruházásait a céljaival összhangba hozza, hogy a beruházásokon keresztül realizálni tudja azok értékét. Az alapelvek – az érintettek igényeinek kielégítése; a vállalat teljes körű lefedése; egyetlen integrált keretrendszer alkalmazása; holisztikus megközelítést lehetővé tétele, és az irányítás (governance) és menedzsment szeparálása – lehetővé teszik az irányítás és menedzsment holisztikus keretrendszerének megteremtését, mely megvalósulását az elvek, szabályok és keretrendszerek; folyamatok; szervezeti struktúrák; vállalati kultúra, etika és viselkedés; információ, szolgáltatások, infrastruktúra és alkalmazások, valamint humán erőforrás, képességek és készségek teszik lehetővé [11].

A CObIT 5 frissített változata, a CObIT 2019 hat alapelve átstruktúrálva és pontosítva jeleníti meg az eredeti öt alapelvet: értékteremtés az érintettek számára; holisztikus megközelítés, dinamikus irányítási rendszer, az irányítás és menedzsment külön funkciók; vállalati igényekre szabott, és teljes körű (end-to-end) irányítási rendszer [15]. Az irányítási rendszer jelenti az integrált keretrendszert.

A COSO és CObIT keretrendszerek folyamatleírásai az ISO/IEC 15504-2 Információs technológia – folyamatképesség-felmérés (Software Process Improvement and Capability dEtermination (SPICE)) szabvány követelményeinek megfelelő folyamat referencia modellek felállítására is alkalmasak [16; 17].

A keretrendszerek megjelenítik azt, hogy a vállalati kockázatkezelési folyamatok egyes elemei összekapcsolódnak, azok integráltan kezelendők, beleértve az IKT folyamatokat.

Kockázatértékelés [18]

A kockázatértékelés során az események hatásának és valószínűségének alapján hozzárendelt értékeket kockázati mátrixon lehet táblázatba foglalni, ill. kockázati térképen lehet ábrázolni. A kockázati mátrix egy táblázat. A kockázati térkép egy ábra, ahol az egyes kockázatok helyét a tengelyeken hozzárendelt értékek határozzák meg.

A kockázati mátrix és a kockázati térkép esetében is a két tengely ugyanaz, valószínűség és súlyosság. Az egyes események kockázata általában (bekövetkezés valószínűsége) x (bekövetkezés hatása) [19].

A kockázati tűréshatároknak megfelelően a kockázatok lehetnek:

- Lehetőség – alacsony kockázat, ahol egyes kontrollok „elengedésével" költségcsökkentésre nyílik lehetőség, ill. kockázatosabb területekre lehet fókuszálni.
- Normál, elfogadható kockázat – ahol jellemzően semmi extra tevékenységre nincs szükség, a jelenlegi kontrollokon, ill. folyamatokon felül.
    - Nem elfogadható kockázat – emelkedett kockázat, amely az elfogadható kockázat szintjét meghaladja, és mitigációt, ill. egyéb adekvát választ követel meg szoros határidőn belül.
    - Egyáltalán nem elfogadható kockázat – jóval meghaladja az elfogadható kockázat szintjét, és azonnali kockázatra adott választ követel meg.

Az azonosított kockázatokhoz kapcsolódóan meg kell határozni a kockázati választ, melyet számos tényező befolyásol. Ilyen tényezők:

- társuló költségvonzat, pl.: biztosítási költség kockázatmegosztás esetén, vagy a kontrollok bevezetésének költsége mitigáció esetén;
- kockázat pozíciója a kockázati térképen, azaz milyen a gyakorisága és nagyságrendje;
- társaság kockázatmenedzsment folyamatának érettsége (minél érettebb, annál szofisztikáltabb megoldás lehet célravezető);
- kockázati válasz eredményessége, azaz mennyire képes csökkenteni a kockázat gyakoriságát, ill. mértékét;
- kockázati válasz hatékonysága, azaz a kockázati válasz relatív előnyei más IT-val kapcsolatos beruházásokhoz, ill. más kockázati válaszokhoz képest.

A vállalat által alkalmazott kockázatkezelési stratégia összefügg a vállalat általános stratégiájával [20]. A különféle kockázatokhoz eltérő kockázati válaszok szükségesek (kockázatkerülés, kockázatcsökkentés/mitigáció, kockázatmegosztás / átruházás, kockázat elfogadása) [18; 20; 21; 22; 23; 24]. Az egyes kockázati válaszok adott körülmények esetén megfelelőek (ld. 1. Táblázat: Kockázatra adott válaszok).

Kockázatra adott válasz	Alkalmazási terület
Kockázatkerülés	a kockázatot jelentő tevékenység megszakítása, ill. a kockázatot jelentő körülményekből való kilépés. Jellemzően magas, v. extrém kockázatok, amelyek nem könnyen mitigálhatóak. Alkalmazása: amikor más kockázati válasz nem megfelelő pl.: elutasítani egy olyan projektben való részvételt, aminél jelentős a kudarc kockázata; elkerülni az ingatlanvásárlással járó kockázatokat, ahelyett bérelni; terrorizmussal sújtott régió elkerülése; jogi, vagy szabályozói kockázatok, amik a kockázatelkerülést teszik szükségessé
Kockázatcsökkentés/ Mitigáció	a kockázat felderítését követően a kockázat gyakoriságának és/ vagy hatásának csökkentésére intézkedéseket tesznek pl.: hatáskörök elkülönítésével (Segregation of duties) kapcsolatos „konfliktusok" mitigálása, amennyiben a feladatkörök elkülönítése nem valósítható meg; biztonsági intézkedések; szabályzatok
Kockázatmegosztás/ Átruházás	a kockázat gyakoriságának vagy hatásának csökkentését jelenti a kockázat egy részének átruházása vagy más módon történő megosztása, mely nem mentesíti a vállalatot a kockázatoktól, de bevonja másik fél készségeit a kockázat kezelésébe és csökkentheti a kockázatok esetleges pénzügyi következményeit, pl.: IT-val kapcsolatos biztonsági eseményekre vonatkozó biztosítás megkötése; az informatikai tevékenység egy részének kiszervezése vagy IT projektkockázat megosztása a szolgáltatóval rögzített áru megállapodások révén; szerződéses klauzúrák, ill. egyéb formális megállapodások; szakértő alkalmazása
Kockázat elfogadása	nem történik ilyenkor intézkedés a kockázathoz kapcsolódóan, az esetleges nem kívánatos esemény felmerülésekor történik könyveli el a vállalat a veszteséget. IT-val kapcsolatos kockázatot csak a menedzsment, és üzleti folyamatok tulajdonosai fogadhatnak el az IT funkcióval együttműködve, ill. az IT funkció által támogatva. Az álláspontot kommunikálni kell az szenior menedzsment és az igazgatóság felé.

Táblázat: Kockázatra adott válaszok, Saját szerkesztés, készült: [18; 20; 21;22;23;24] alapján

Az erőforrás-korlátok miatt a kockázati válaszok priorizálása válik szükségessé. A kockázati válaszokat ezért kategorizáljuk aszerint, hogy

- „gyors győzelem" (hatékony és eredményes kockázati válasz magas kockázatra)
- üzleti hatástanulmány készítése (alapos elemzést és vezetői döntést kívánó kockázati válasz esetén, pl.: költségesebb vagy komplikáltabb kockázati válasz magas kockázat esetén vagy hatékony és eredményes kockázati válasz alacsony kockázat esetén)
- késleltetés (költséges válasz alacsony kockázatra).

VÁLLALATI KOCKÁZATOK INTEGRÁLT MEGKÖZELÍTÉSŰ BEMUTATÁSA

COSO ERM fókuszú kockázati modell

A COSO ERM fókuszú kockázati modell (2. Táblázat: COSO ERM fókuszú kockázati modell) a stratégiai, megfelelési, riporting és operatív kockázatok szerint kategorizálva mutatja be a kockázatokat, melyek a COSO kocka vertikális oszlopain jelennek meg. A besorolások mentén további alkategóriák képezhetőek [3]. A modell átfogóan kezeli a vállalati kockázatokat, és egyben rámutat arra, hogy a vállalati folyamatok összefüggő rendszert képeznek. A stratégiai szemlélet a vállalati működést meghatározza. A kontrollkörnyezet hatással van a vállalati működésre.

Kockázatok

Stratégiai	Megfelelési	Riporting	
Külső	Külső megfelelés	Külső jelentések	
- változás a törvényekben és rendeletekben	- jogszabályi megfelelés - szerződéses megfelelés	- számviteli, - és pénzügyi jelentések	
- kormányváltás		- belső kontrollok - szabályozói jelentéstételi kötelezettségek	
- versenytársak	- adósságmegfelelés	- adózás	
- koncentráció	- peres ügyek		Információ
- gazdasági	- engedélyek		- hozzáférések
- hírnév	- etc.		- adatintegritás
- ipari			- infrastruktúra
- technológia			- elérhetőség
- politika			- etc.
Belső	Belső megfelelés	Belső jelentések	
- szövetségek kialakítása	- etika - csalás, jogellenes tevékenységek	- pénzügyi tervezés és előrejelzés - menedzsment jelentések	
- márka/ márkanév	- szabályzatok	- teljesítménymérés	
- üzleti stratégia		- etc.	
- vevőelégedettség			
- célmeghatározás/ összeghangolás			
- irányítás			
- piackoncentráció			
- árazás			
- termék			
- erőforrásallokáció			

(megjegyzés: a táblázat a következő oldalon folytatódik)

Operatív kockázatok			
Általános	Kereskedelmi	Pénzügyi	Emberi erőforrás
- beszerzés, és elidegenítés	- üzleti folyamatok	- tőke rendelkezésre állása	- jogosultsági szintek
- üzemszünet	- szállítás	- tőke költsége	- változási hajlandóság
- üzletmenet-folytonosság	- emissziós kreditek	- cash flow/ likviditás	- kollektív tárgyalások
- kapacitás	- üzemanyag árak	- készpénzkezelés	- kommunikáció
- katasztrófa események	- üzemanyag beszerzés	- partnerkockázat, hitelkockázat	- emberi erőforrás elosztás
- környezeti kockázatok	- piaci likviditás	- hitelminősítés	- vezetőség/kulcs munkavállalók
- egészség - és biztonság	- portfolió optimalizáció	- árfolyamkockázat	- emberi erőforrások toborzása
- elavulás	- elszámolás és számlázás	- pénzügyi piacok	- szervezeti struktúra
- üzemi hatékonyság	-kereskedelmi ügylet befogadása és végrehajtása	- kamatláb	- kiszervezés
- ellátási lánc kezelése	- átadás nehézségei	- nyugdíjfinanszírozás	- teljesítményösztönzők
- terrorista támadás		- kockázatáthárítás	
- időjárás			

2. Táblázat: COSO ERM fókuszú kockázati modell, Forrás: [3], p8.
(Risk model example, Institute of Internal Auditors)

Az értékesítési folyamat kockázatainak integrált szemléletű áttekintése

A vevői elégedettség stratégiai cél. Az ipar 4.0. és pandémia világában a kereskedelmi csatornák átrendeződése meghatározó hatással bír a vállalatok értékesítési folyamataira. Az IKT megoldások szerepe és az e-kereskedelem szerepe nő [25]. „A megújulásra való képesség előfeltétele a gazdasági szereplők életképességének [26].”

A vállalati működés elsődleges folyamata a „bevételszerzési”, azaz értékesítési folyamat, melynek kockázatait a következőkben átfogóan tekintem át teljes körű (end-to-end) szemlélettel. A vállalati bizalmi kultúra hozzájárul a gördülékeny folyamatokhoz, a folyamatok sebessége nő, a költségek csökkennek [27]. Kontroll szempontból a sikeres működést jellemzi a „bízz, de ellenőrizz” szemlélet, ahol a jól működő folyamatok mellett jelen vannak a megfelelő kontrollok és ellenőrzések. Kontroll alatt azokat a tevékenységeket értem, melyek biztosítják, hogy a folyamat hibamentesen, ill. adott elfogadható tűréshatáron belüli hibaszázalékkal következik be.

A bevételszerzési folyamat során a vállalati stratégia valósul meg. A stratégiai szinten azonosított kockázatok meghatározóak a bevételszerzési/értékesítési folyamat szempontjából (ld. 2. Táblázat: COSO ERM fókuszú kockázati modell). Úgyszintén igaz ez az integrált kockázatkezelési modell további vetületeire, azaz a megfelelési, riporting és operatív kockázatokra. A rendszerek a vállalati folyamatok működését biztosítják, ebből kifolyólag a folyamatban lévő kockázatok összekapcsolódnak a mögöttes IKT kockázatokkal.

Az értékesítési folyamat kapcsán tipikus kockázatok, ill. kockázatos területek: fiktív ügyfél létrehozása; törzsadatok módosítása; a megrendelések nem rendelkeznek megfelelő jóváhagyással; alkalmazott árazás nem megfelelő, nem jóváhagyott, jogosulatlan engedmények, kenőpénz elfogadása; értékesítési csoport teljesítményértékelése; tranzakciók nem a megfelelő periódusra lettek könyvelve; ügyfélminősítési folyamat, új, ill. meglévő ügyfelek

minősítése; esedékességet meghaladó vevői követelések; egyedi tranzakciók kezelése; visszáru kezelése; jogosultsági szintek; hozzáférés-kezelés és hatáskör-átlépések.

Az azonosított kockázatokhoz kapcsolódóan meg kell határozni azok hatásait, és a bekövetkezés gyakoriságát. A kockázati mátrix kétdimenziós táblázatban szemlélteti az azonosított kockázat következményét, ill. a kockázat bekövetkezési valószínűségét, gyakoriságát. A kockázati mátrix felosztása általában 3x3 és 7x7 között változik [19]. Egy lehetséges kockázati mátrixot mutat be a 3. Táblázat: Kockázati mátrix példa.

Valószínűség	Következmény				
[0; 1]	jelentéktelen [0; 1)	mérsékelt [1; 2)	közepes [2; 3)	súlyos [3; 4)	kritikus [4; 5]
elhanyagolható [0]					
csekély (0; 0,1)					
alacsony, nem valószínű [0,1; 0,4)					
valószínű [0,4; 0,6)					
nagyon valószínű [0,6; 0,9)					
majdnem biztos [0,9; 1]					

Jelölések:
elhanyagolható kockázat, lehetőség kontrollerőforrás átcsoportosítására
alacsony, elfogadható kockázat - jellemzően nincs szükség a jelenlegi kontrollokon, folyamatokon felül extratevékenységre, a kockázat felvállalható
normál, elfogadható kockázat - megfelelő folyamatkontrollok, kontrolltevékenységek szükségesek, intézkedés egyéni mérlegelés alapján
magas, nem elfogadható kockázat - kockázatkezelési eszközök szükségesek szoros határidőn belül
kritikus, egyáltalán nem elfogadható - azonnali kockázati választ követel meg

3. Táblázat: Kockázati mátrix példa, Saját szerkesztés, készült [18; 19; 28; 29] felhasználásával

A folyamatlépések elválaszthatatlan részét jelentik a technológiai megoldások, ebből eredően az IKT kockázatok az értékesítési folyamatokhoz szorosan kapcsolódnak. A folyamat megfelelő működéséhez a kockázatok kezeléséhez kontrolltevékenységek szükségesek. Ugyanaz a kontrolltevékenység több kockázat kezelését is biztosíthatja. A kontrollelemek a „tudatos", „biztonságos" szervezet folyamatain keresztül jelennek meg. A kontrollok hatékony érvényesülése akkor valósul meg, ha az rutin jellegű, és működése véletlenül sem marad el.

Az ipar 4.0 fejlesztéseivel lépést tartó innovációra nyitott vállalatok esetében a kockázatkezelési megoldások a vállalati folyamatok transzformációján keresztül valósulnak meg, mely ideális feltételeket teremt jól működő, hatékony kockázatkezelési folyamatok megvalósítására. Az 1. Melléklet: Értékesítési folyamat kockázatai és kontrolltevékenységei c. az értékesítési folyamat főbb területeire vonatkozóan mutat be egy-egy kockázati területet, és tipikus kontrolltevékenységeket, valamint jógyakorlatokat [30].

Esettanulmány vállalati IKT kockázati mátrix készítéséhez
OTC vállalat e-kereskedelmi piacra lépési projekt – IKT kockázati mátrix

Az esettanulmány célja a kockázati mátrix készítésének lépéseinek egyszerűsített bemutatása. OTC vállalat egy fiktív, stabil bevétellel rendelkező kiskereskedelmi hálózat, mely a pandémia idején lépést tartva a vevői igények átrendeződésével az e-kereskedelmi csatornájának fejlesztésére fókuszált. OTC vállalat korábban aktívan nem volt jelen az e-kereskedelmi piacon a pandémiát megelőzően. Kezdetleges jelleggel csak webes felületről indított e-mailes megrendeléseket fogadtak. Vevői köre széles spektrumot lefed, azonban direkt értékesítési ügyfélköre jellemzően a 30-60 éves korosztály, akik vásárlásaik során jellemzően 50-50%-ban készpénzes, ill. bankkártyás fizetést választottak. OTC vállalat számára a pandémia hatására a bevételek direkt értékesítés során olyan mértékben csökkentek, hogy megkérdőjeleződött az üzletmenet-folytonosság elvének biztosítása. A vállalati vezetés stratégiai célként tűzte ki az erőforrások e-kereskedelmi piacra történő átcsoportosítását, és elsődlegesen az e-kereskedelmi csatornából történő jövedelemszerzést.

Az új stratégiához kapcsolódóan IKT beruházások történtek. A projekt célja, hogy az online értékesítés megfelelő keretei biztosítva legyenek. A rendelkezésre álló költségvetés korlátozott volt. A beruházás a legszükségesebbek területekre korlátozódott. A beruházások és fejlesztések rövid időn belül lezajlottak, és a vállalat megkezdte az e-kereskedelmi tevékenységet.

A vállalat tapasztalt szereplőként volt jelen a piacon.

A munkavállalók elkötelezettek. Az ún. Pulse survey alapján a munkavállalói elégedettség szint magas. A jogszabályi környezet ismerete és a megfelelési prioritás mindig fontos prioritás volt a vállalat számára. Jogszabályi megfelelés területén felkészült volt és megfelelt a vállalat az e-kereskedelmi kívánalmaknak. A személyes adatok védelme (GDPR) területén GDPR 30. cikk szerinti adatkezelési nyilvántartással, valamint adatvédelmi szabályzattal rendelkezik. A kiépített adatvédelmi rendszer megfelelőnek tekinthető. Jellemző az adatvédelmi, ill. általános biztonsági tudatosság.

A vállalat az üzembe helyezett új e-kereskedelmi rendszer működése során biztonságot veszélyeztető hatásokkal, fenyegetésekkel, ill. biztonsági incidensekkel találta szembe magát. A gyors beruházási - és üzembe helyezési folyamat következtében biztonsági rések keletkeztek. A vállalat vezetősége a belső vizsgálatok gyökérok elemzése során megállapította, hogy egyes bekövetkezett biztonsági események a biztonsági rendszer sebezhetőségére, annak hiányosságaira, ill. gyengeségeire utalnak, azokat a meglévő biztonsági szabályzatok és folyamatok már nem fedték le. Továbbá több biztonsági hiányosság együttes bekövetkezése fokozott problémát okozhatott, ahogy azt a Reason által ismertetett svájci sajt modell példája is illusztrálja [31; 32]. Megállapítást nyert, hogy a projektkockázatok kezelése során nem került valamennyi érintett kockázat feltárásra, és kezelésre, ebből kifolyólag a biztonsági rendszert erősíteni kell. A biztonsági terv részeként a vállalat az aktuális kockázatok alapján új IKT kockázati mátrixot készített, és meghatározta a lehetséges kockázatkezelési lehetőségeket.

A 4. Táblázat: IKT kockázatok áttekintése – OTC vállalat tartalmazza az azonosított kockázati területeket, a kockázat bekövetkezésének becsült valószínűségével és hatásával. (A hatás-, és valószínűség értékek szubjektív értékek az esettanulmány kockázati mátrixának felvázolásához.)

Jel	Kockázat	Kockázathoz kapcsolódó megjegyzések	Hatás valószínűsége (0,1,2,3,4,5)	Hatás (1,2.3,4,5)
A	**adatbiztonsági kockázatok (A)** - nem jogosult egyén hozzáférése, - nem jogosult felhasználó módosítja, - nem hozzáférhető a szükséges időpontban és szükséges időtartam alatt	Az információbiztonság megteremtését a bizalmasság, sértetlenség és elérhetőség elvei (CIA) határozzák meg.	3	5
B	**adatvesztés (B)**	Adatbiztonsági kockázat. Az üzletmenethez szükséges, és annak során keletkező adatok rendelkezésre állásának kockázata. Az adatok tárolásának, adott törvényi határidőn belüli visszakereshetőségének, ill. auditálhatóságának biztosítása sérülhet. Az adatvesztés elkerülésének fontossága.	2	5
C	**adatszivárgás (data leakage) (C)**	Adatbiztonségi kockázat. Annak a kockázata, hogy az adatok illetéktelen kezekbe kerülnek, és azáltal anyagi kár, reputáció vesztés következik be. A fokozódó online jelenlét miatt Kapcsolódik az emberi erőforrás kockázathoz is.	1	5
D	**emberi erőforrás (D)**	A biztonsági események bekövetkezése sokszor az emberi tényezőhöz köthető, mely lehet egyszeri véletlen hiba, szándékos mulasztás vagy tudatos manipuláció (social engineering) következménye is.	2	4
E	**jogszabályi nem megfelelés (E)**	A jogszabályi környezet ismeretének és a megfelelésnek követelménye. E-kereskedelmi tevékenységhez kapcsolódóan biztosítani kell, hogy a vállalat az online értékesítés felületénaz EU szintű online vitarendezési platformhoz, az Online Dispute Resolution, azaz ODR-hez linket tartalmazzon és email címe rendelkezésre álljon (Kemendi, 2021).	2	5

Jel	Kockázat	Kockázathoz kapcsolódó megjegyzések	Hatás valószínűsége (0,1,2,3,4,5)	Hatás (1,2.3,4,5)
F	**GDPR nem megfelelés, büntetések, hírnévkockázat (F)**	A személyes adatok védelme (GDPR, EU General Data Protection Regulation 2016/679) területén jelentős adatvédelmi követelményeknek kell megfelelni.	2	5
G	**bankkártyaadatokkal és szenzitív azonosító adatokkal kapcsolatos kockázatok /PCI DSS/, bankkártya csalások (G)**	A bankkártya-adatok biztonságos kezelését globális adatbiztonsági sztenderd követeli meg (PCI DSS – Payment Card Industry Data Security Standard).	2	5
H	**IKT kitettségek (H)**	A vállalati üzletmenet folyamatai információs és kommunikációs technológia (IKT) rendszerekben mennek végbe.	3	5
I	**IoT-vel kapcsolatos adatvédelmi és biztonsági kockázatok, kiber kockázatok (I)**	Az Internet of things (IoT) nagyfokú térnyerése és alkalmazása biztonsági kockázatokat rejt. Az internet vezérelt eszközök fejlesztése során a biztonsági kérdések gyakran háttérbe szorulnak, így a technológiai innovációk alkalmazásán keresztül létrejövő biztonsági rések kockázata magas.	2	5
J	**hálózati biztonság (J)**	A hálózati biztonság az IKT biztonság kritikus eleme. A hirtelen megnövekedett API adatforgalom következtében az API-n keresztüli adatforgalom biztonsága prioritás.	3	5
K	**biztonsági incidensek (K)**	A fenyegetések a vállalat sebezhetőségét kihasználva biztonsági eseményhez vezethetnek. A kockázat valós eseménnyé válik, és tényleges hatása tesz.	2	4
L	**üzletviteli zavarok pl. hardware hiba, tűzeset, árvíz, emberi erőforrás elvesztésének kockázata (L)**	A vállalati üzletmenet-folytonosságra váratlan, vis major esetek veszélyt rejthetnek. Ritka, azonban nagy hatású események.	1	5

4. Táblázat: IKT kockázatok áttekintése – OTC vállalat, Saját szerkesztés

A fenti kockázatokat (Jel=A, B,…,.L) a vállalat az alábbi kockázati mátrixban ábrázolta (5. Táblázat: IKT kockázati mátrix – OTC vállalat).

Valószínűség [0; 1]	Következmény jelentéktelen [1]	mérsékelt [2]	közepes [3]	súlyos [4]	kritikus [5]
elhanyagolható [0]					
csekély (0; 0,2)					C, L
alacsony [0,2; 0,4)				D, K	B, E, F, G, I
közepes [0,4; 0,6)					A, H, J
valószínű [0,6; 0,8)					
nagyon valószínű, gyakori [0,8; 1]					

Jelölések:

elhanyagolható kockázat, lehetőség kontrollerőforrás átcsoportosítására

alacsony, elfogadható kockázat - jellemzően nincs szükség a jelenlegi kontrollokon, folyamatokon felül extratevékenységre, a kockázat felvállalható

normál, elfogadható kockázat - megfelelő folyamatkontrollok, kontrolltevékenységek szükségesek, intézkedés egyéni mérlegelés alapján

magas, nem elfogadható kockázat - kockázatkezelési eszközök szükségesek szoros határidőn belül

kritikus, egyáltalán nem elfogadható - azonnali kockázati választ követel meg

5. Táblázat: IKT kockázati mátrix – OTC vállalat, Saját szerkesztés

Valamennyi kockázat a vállalat kockázati mátrixában súlyos, nem elfogadható, ill. kritikus, egyáltalán nem elfogadható következménnyel jár. A vállalat kockázatkezelési csoportja az azonosított IKT kockázatokhoz kapcsolódóan jellemző jógyakorlatokat határozott meg, amelyeket lehetséges kockázatkezelési javaslatként fognak értékelni, és a kockázatkezelési terv részeként bevezetni (6. Táblázat: IKT kockázatok és kockázatkezelési megoldások). A bevezetésre kerülő intézkedések eredményeként a vállalati vezetőség a kockázati szint csökkenését várja. Kockázatokkal arányos védelem kiépítése a cél.

Jel	Kockázat	Lehetséges kockázatkezelési javaslat
A	**adatbiztonsági kockázatok (A)** - nem jogosult egyén hozzáférése, - nem jogosult felhasználó módosítja, - nem hozzáférhető a szükséges időpontban és szükséges időtartam alatt	„zárt védelem” /IT-, fizikai-, és személyi biztonság/, hozzáférések minimalizálása, minimum funkció elve, négy szem elve, szabályzatok adekvát működtetése, technológiai megoldások adekvát beépítése /kockázatokkal arányos védelem/
B	**adatvesztés (B)**	biztonsági mentések/back up-ok, legutolsó biztonsági másolat visszatöltése, archiválás, hozzáférés-kezelés, logging
C	**adatszivárgás (data leakage) (C)**	„tiszta asztal” politika, IT eszközök- és adathordozók védelme, tréning, átvilágítás

Jel	Kockázat	Lehetséges kockázatkezelési javaslat
D	**emberi erőforrás (D)**	kiválasztás (HR kompetencia), átvilágítás, tréning, megfigyelés/monitorozás, elbocsátás, jelszó használat, titkosítás, limitált hozzáférés, felelősségi körök kialakítása, szabályzatok, folyamatok, munkafolyamatba épített kontrollok, változáskezelés, tudásmenedzsment, a tudás védelme, etikai kódex, etikai nagykövetek, a „vezetőség hangja”, példamutatás
E	**jogszabályi nem megfelelés (E)**	megfelelés ellenőrzése és tesztelése, auditok, belső folyamatok vizsgálata, „akció tervek” készítése, GRC szoftverek adekvát működtetése
F	**GDPR nem megfelelés, büntetések, hírnévkockázat (F)**	GDPR folyamatok, GDPR felelős
G	**bankkártyaadatokkal és szenzitív azonosító adatokkal kapcsolatos kockázatok /PCI DSS/, bankkártya csalások (G)**	biztonsági folyamatok, kontrollok, információbiztonsági szabályok, hálózatok és rendszerek biztonsága, tárolt kártyaadatok védelme, nyilvános hálózaton keresztüli adatforgalom titkosítása
H	**IKT kitettségek (H)**	kockázatkezelési terv, és kockázatok értékelése, szabályzatok, intézkedési tervek, monitorozás
I	**IoT-vel kapcsolatos adatvédelmi és biztonsági kockázatok, kiber kockázatok (I)**	hálózati adatforgalom kontrollja pl. biztonsági router, felhasználó azonosítás stb.
J	**hálózati biztonság (J)**	biztonsági átjárók, tűzfalak, vírusvédelem, API biztonság
K	**biztonsági incidensek (K)**	incidens kezelési folyamat, gyökérokok feltárása (teljes körű), intézkedési terv, monitorozás, folyamatdokumentáció-, és szabályzatok frissítése, kockázatkezelés (korai azonosítás, felismerés, ill. megelőzés)
L	**üzletviteli zavarok pl. hardware hiba, tűzeset, árvíz, emberi erőforrás elvesztésének kockázata (L)**	Üzletmenet-folytonosság menedzsment (BCM), Üzletimenet folytonossági – (BCP), és Katasztrófaelhárítási terv (DRP); erőforrás-tervezés, IT erőforrás-helyreállítási terv, tesztelés, folyamatos monitoring, incidens – és vészhelyzet szimuláció, hatástanulmány készítése, helyreállítási idő meghatározása

6. Táblázat: IKT kockázatok és kockázatkezelési megoldások, Saját szerkesztés [33] alapján

KÖVETKEZTETÉSEK

A kockázatkezelési folyamat alapvetően egy folyamatosan működtetett körfolyamat. Egyes események direkt indukálják azt. A projektkockázatok integrált szemléletű kezelése szükséges. A vállalati stratégiai tervekhez kapcsolódóan a kockázatokat értékelni, és kezelni kell. Az ipar 4.0. dinamikusan változó világában a vállalatok alkalmazkodási képessége fontos sikerkritérium. A változó környezethez való alkalmazkodásra, – ahol szinte csak a válto-

zás állandó – valamennyi üzleti-, ill. támogató funkciónak fel kell készülnie. Az üzleti stratégia változása - pl. erőforrás-átcsoportosítás egy új értékesítési csatornára - a sikeres projektmegvalósítás részeként adekvát kockázatkezelést követel meg. Az egyes kockázatkezelési lehetőségek erőforrás-ráfordításokkal járnak, melyet a vállalati vezetőségnek mérlegelni kell. A kockázatarányos védelem elve segíti a döntéshozatalt. A kívánt biztonsági szint megteremtését segíti a vállalati folyamatok leírása és szabályozása. A kockázatokat teljes körű (end-to-end) szemlélettel kell kezelni ahhoz, hogy valamennyi érintett terület feltárásra kerüljön, ezáltal csökkenthető annak a valószínűsége, hogy több hiba, ill. nem várt negatív esemény együttes bekövetkezése azok egyéni bekövetkezési valószínűségéhez képest jóval nagyobb kárt okozzon, pl. teljes rendszer, ill. folyamatleálláshoz vezet. A sikeres kockázatkezelés eredménye a kívánt biztonsági szint elérése.

ÖSSZEGZÉS

A publikációban bemutattam a főbb vállalati kockázatokat, és kockázatkezelési keretrendszereket, ill. a releváns szabványok funkcióját. A publikációban tárgyaltam a kockázatkezelési folyamat egyes elemeit, bemutattam az értékesítési folyamat specifikumait kockázatkezelési szempontból, és jógyakorlatokat fogalmaztam meg a kontrollkörnyezet kiépítésével kapcsolatban. Esettanulmány jelleggel bemutattam egy fiktív vállalat e-kereskedelmi piacra lépési projektjéhez kapcsolódó IKT területre fókuszáló kockázati mátrix készítését, és lehetséges kockázatkezelési megoldásokat ismertettem.

A hosszú távú vállalati sikeresség, és a biztonságos vállalati működés szorosan összekapcsolódik. Az ipar 4.0. világában a reziliencia, az alkalmazkodás képessége központi szerepet kap. A vállalat relatív biztonsága a sikeres működés alapja. A vállalat biztonságának kérdése stratégiai jelentőségű, összefonódik a kockázatkezeléssel, és kontrolltudatossággal. Az informatikai biztonság, és vele párhuzamosan az emberi tényező által generált kockázatok kezelése a szervezeti biztonsági rendszerében kiemelt jelentőséggel bírnak.

A kockázatkezelési folyamat a kockázatok azonosításán, értékelésén, és kockázatkezelési eszközök meghatározásán alapul. A sikeres kockázatkezelés értéket jelent a vállalat számára, a vállalat ezáltal eléri a kívánt biztonsági szintet. Az IKT kockázatok kezelését a vállalati stratégiával összhangban kell megvalósítani. A kockázatok integrált kezelése a vállalati stratégiához illeszkedik.

HIVATKOZÁSOK

[1] Kocziszky G., & Kardkovács K. (2020). *A compliance szerepe a közösségi értékek és érdekek védelmében.* Akadémiai Kiadó

[2] Banham, R. 2004. Enterprising views of risk management. *Journal of Accountancy 197* (6), 65-71.

[3] Hall, J. (2007). Internal Auditing and ERM: Fitting in and Adding Value, *The Institute of Internal Auditors Research Foundation,* https://global.theiia.org/about/about-the-iia/Public%20Documents/Sawyer_Award_2007.pdf

[4] Dionne, Georges: *Corporate Risk Management: Theories and Applications,* John Wiley & Sons, Incorporated, 2019. ProQuest Ebook Central, ISBN 9781119583172

[5] ISO 31000: 2018 Risk management – Guidelines https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[6] Trusted Business Partners Kft. (in Eds. Iványos János). (2014). *Kockázatkezelési kézikönyv.* 2014. http://www.trusted.hu/attachments/article/91/Kock%C3%A1zatkezel%C3%A9si%20K%C3%A9zik%C3%B6nyv%20v2.pdf
[7] Ahlan, A. R., & Arshad, Y. (2012). Understanding Components of IT Risks and Enterprise Risk Management, *Risk Management for the Future - Theory and Cases*, Jan Emblemsvag, IntechOpen, https://doi.org 10.5772/32023. Available from: https://www.intechopen.com/chapters/36108
[8] Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?, *Reliability Engineering & System Safety, 189*, pp. 279-286, https://doi.org/10.1016/j.ress.2019.04.035, https://www.sciencedirect.com/science/article/pii/S0951832018312250
[9] IWA 31:2020 (en) Risk management — Guidelines on using ISO 31000 in management systems, https://www.iso.org/obp/ui/fr/#iso:std:iso:iwa:31:ed-1:v1:en
[10] COSO. (2004). *Enterprise Risk Management – Integrated Framework*
[11] ISACA. (2012). *CObIT5. A Business Framework for the Governance and Management of Enterprise IT.*
[12] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations
[13] Fogarasi, A., & Szűcs. E. (2021). A szabványos irányítási rendszerek fejlődése, integrációja, *Biztonságtudományi Szemle, 3*(2), pp. 1-13
[14] Michelberger, P. (2018). *Információ-, folyamat- és vállalatbiztonság*, Óbudai Egyetem, Keleti Károly Gazdasági Kar
[15] De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, Springer Nature Switzerland AG.
[16] ISO/IEC 15504-2:2003(en)
Information technology — Process assessment — Part 2: Performing an assessment, https://www.iso.org/obp/ui/#iso:std:iso-iec:15504:-2:ed-1:v1:en
[17] Iványos, J., Roóz, J., & Messnarz, R. (2010). *Governance Capability Assessment. Using ISO/IEC 15504 for Internal Finacial Controls and IT management*. Proceedings of the MONTIFIC Project at the Conference of "The Current Financial Crisis and Competences to Address Problems on the European Market", pp.17-47., https://www.researchgate.net/publication/294428037_Governance_Capability_Assessment_Using_ISOIEC_15504_for_Internal_Financial_Controls_and_IT_Management
[18] ISACA. (2009). *The RiskIT Framework*, https://www.hci- itil.com/ITIL_v3/docs/RiskIT_FW_30June2010_Research.pdf
[19] Csordás, E. (2012). Fogalmi és értelmezési zavarok a kockázati mátrixok és kockázati térképek körül, *Hitelintézeti Szemle*, https://www.bankszovetseg.hu/Content/Hitelintezeti/254-271-csordas1.pdf
[20] Farkas, Sz., & Szabó, J. (2010). *A vállalati kockázatkezelés kézikönyve.* Dialog Campus
[21] Conrad, E., Misenar, S., Feldman, J. (2016). Chapter 2 - Domain 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity), In Conrad, E., Misenar, S., & Feldman, J. (Eds.), *CISSP Study Guide* (3rd Edition, pp. 11-79). Syngress, https://doi.org/10.1016/B978-0-12-802437-9.00002-3

[22] Fennelly, L.J., & Perry, M. A. (2017). Assessing Risk and Vulnerabilities. in Fennelly, L.J., Perry, M. A. (Eds.). *Physical Security: 150 Things You Should Know* (2nd ed.)
[23] Peterson, K. E. (2010). Security Risk Management. *International Foundation for Protection Officers (IFPO): The Professional Protection Officer: Security Strategies, Tactics and Trends,* (2nd ed.), Butterworth-Heinemann, https://doi.org/10.1016/C2009-0-19898-7
[24] Purpura, P. P. (2013). Resilience, Risk Management, Business Continuity, and Emergency Management. *Security and Loss Prevention* (6th ed.)
[25] Kemendi, A. (2021). E-commerce safety and security in the industry 4.0 era, *National Security Review*, *2021(*1), https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_1_NSR.pdf
[26] Takácsné György, K. (2017). Kihívások, esélyek, alternatívák (és a nem-növekedés tóriája – „degrowth"), in Takács, I. (Ed.), *Az együttműködési attitűdök gazdasági társadalmi hatótényezői az északmagyarországi régióban működő kkv-kban*. http://real.mtak.hu/54108/1/Tanulmanykotet_OTKA_K109026_u.pdf
[27] Takácsné György, K. & Benedek, A. (2016). Bizalmon alapuló együttműködés vizsgálata a kis- és középvállalatok körében, In Csiszárik-Kocsir, A. (Ed.), *Vállalkozásfejlesztés a XXI. században VI.*, pp. 379-390, Óbuda University, Keleti Faculty of Business and Management. http://kgk.uni-obuda.hu/sites/default/files/27_Benedek-Takacsne.pdf
[28] Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach, *Safety Science*, *48*(10), pp. 1269-1278, https://doi.org/10.1016/j.ssci.2010.04.005, https://www.sciencedirect.com/science/article/pii/S0925753510001049
[29] MIL-STD-882E. System Safety. Department of Defense (USA). Standard Practice.
[30] Rao, S. R. (2014). Perspective SOX Controls - Driving Transformation of the Order-to-Cash Value Chain, Infosys Limited External Document, https://www.infosysbpm.com/offerings/functions/sales-fulfillment/white-papers/Documents/SOX-controls.pdf
[31] Reason, J. (1999). The 'Swiss Cheese' model
[32] Reason, J. (2000). Human error: models and management, *BMJ*, *320*(7237): 768–770. https://doi.org/10.1136/bmj.320.7237.768, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/
[33] Michelberger, P. & Kemendi, A. (2020). DATA, INFORMATION AND IT SECURITY - SOFTWARE SUPPORT FOR SECURITY ACTIVITIES, *PROBLEMS OF MANAGEMENT IN THE 21ST CENTURY, 15* (2), pp. 108-124. https://www.scientiasocialis.lt/pmc/files/pdf/108-124.Michelberger_Vol.15-2_pmc.pdf

TÁBLÁZATOK

1. Táblázat: Kockázatra adott válaszok
2. Táblázat: COSO ERM fókuszú kockázati modell
3. Táblázat: Kockázati mátrix példa
4. Táblázat: IKT kockázatok áttekintése – OTC vállalat
5. Táblázat: IKT kockázati mátrix – OTC vállalat
6. Táblázat: IKT kockázatok és kockázatkezelési megoldások

MELLÉKLETEK

1. Melléklet: Értékesítési folyamat kockázatai és kontrolltevékenységei

1. Rendelésfelvétel		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nem teljes vagy nem pontos rendelési adatok	a hiányzó adatok pótlása, korrigálása	- a rendeléskezelési rendszer a vevő-, ár-, és termék törzsadatokkal összeköttetésben van; - a rendelési nyomtatvány kötelező mezők kitöltése hiányában nem küldhető el; - vevők tájékoztatása a rendelés során a várható feldolgozási időről - érvényes rendelési szám nélkül a rendelés nem kerül feldolgozásra
rendelés duplikált felvétele	a rendszer figyelmeztető üzenetet küld a duplikált rendelésfelvétel megelőzése érdekében	- a rendelések egymást követően számozottak, mely ellenőrzésre is kerül
rendelések feldolgozása a jóváhagyott hitelkereten felül (magasabb vevői kintlévőségek, -és leírások kockázata)	- rendelések automatikus blokkolása, a hitelkeret átlépése esetén - a blokkolt rendelések feloldására jóváhagyási folyamat	- rendelések jóváhagyása a minimális rendelési szabályzat, hitelkeret, termékre-és szolgáltatásra való jogosultság, beszerzés -és készlet rendelkezésre állás, átfutási idő és árazás, ügyfélpolitika szerint - új ügyfél esetén először a törzsadatok létrehozása szükséges, új rendelések ezt követően vehetők fel
magasabb diszkontráták alkalmazása az értékesítési csoport ad hoc kérései szerint	független verifikáció alkalmazása magasabb diszkontráták alkalmazása esetén	sztenderd diszkontráta beállítása, és alkalmazása a rendszerben különböző vevő-, és termék szegmensekre; valamennyi eltérő ráta esetében jóváhagyás szükséges

2. Számlázás		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nem, vagy késve generálódik számla a szállítmányokhoz	- szállítmány jóváhagyott kiadása alapján a raktárból, a rendszer automatikusan generálja a számlát azonos dátummal - szállítási dátum nem módosítható megfelelő szintű vezetői jóváhagyás nélkül	- előzetes szállítási értesítés küldése a vevőnek - szállítási konfirmációs dokumentumok scannelni és archiválni - manuális számlák megfelelő jóváhagyással készülhetnek - alacsony összegű készpénztranzakciókat vállalati hitelkártyás, vagy direkt debit-es tranzakcióval helyettesíteni - összevont számlázás a vevőknek - összevont csoportos fizetés lehetősége a vevőknek automatikus pénzallokációval a könyvelésben, ahol lehetséges
nem megfelelő ár, mennyiség, és egyéb információ feltüntetése a számlán	- rendszerbeállítás alapján a számlaadatok ellenőrzése a törzsadatok és a megrendelésadatok alapján. Nem érvényes adatok elutasításra kerülnek vagy egy függő tételeket tartalmazó file-ba, mely később korrigálható	workflow megoldás a vevővel való vitás tételek gyors rendezésére

3. Pénzbeszedés		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nincs nyomonkövetés az esedékességet meghaladó vevőkre	- vezető ellenőrzi a koros követeléseket, és összehasonlítja a beérkezett kintlévőségeket a periódus elején nyitott követelésekkel	- fizetési ígéretek rögzítése és nyomon követése,- jelentősebb vevőket ösztönözni arra, hogy fizessenek a termék kézhezvételekor a megrendelő alapján, ahelyett, hogy a számlára várnak, - amennyiben nem a számla teljes összege kerül kiegyenlítésre, azt azonnal eszkalálni kell, - elektronikus átutalási utasításokkal ellátott elektronikus fizetések feltöltése az értékesítési főkönyvbe, amelyek lehetővé teszik az automatikus párosítást
a beérkező pénz nem kapcsolódik az értékesítéshez, vagy nem megfelelő ügyfélszámlára lett könyvelve	- a beérkező pénz ügyfélszámlához rendelése az ügyfélnév, az ügyfélszám, és a számlaszám alapján történik, és csak nyitott számlákkal szemben	- Vevők menedzser felülvizsgálja valamennyi azonosítatlan banki befizetést - amennyiben a beazonosítás nem sikeres, átmenetileg az azonosítatlan/felosztatlan befizetések számlára kerül - a beszedési csoport felelőssége az azonosítatlan/felosztatlan befizetések számla "tisztítása"

4. Visszaküldések		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
a visszaküldések nincsenek jóváhagyva, vagy azok nem felelnek meg a vállalati szabályzatnak	- a visszaküldött áru fizikai ellenőrzése, felülvizsgálata és a visszáru engedély (RMA - return merchandise authorization) jóváhagyása szükséges	- a jóváhagyási folyamat felgyorsítása valós idejű információk biztosításával a jóváhagyók részére - csak jóváhagyott visszatérítések kerülnek feldolgozásra - magas összegű kérelmek jóváhagyása jóváhagyási limittel rendelkező ügyfélmenedzser által, ill. alacsony összegű kérelmek automatikus jóváhagyása
a készpénzbevételek nem kapcsolódnak az értékesítéshez, vagy nem a megfelelő ügyfélszámlára lettek könyvelve	- a beérkező pénz ügyfélszámlához rendelése az ügyfélnév, az ügyfélszám, és a számlaszám alapján történik, és csak nyitott számlákkal szemben	Rendszer kiépítése a vevői igények és levonások nyilvántartására

Forrás: [30]

CIVIL-MILITARY COOPERATION CAPABILITIES IN COMPLEX OPERATIONAL ENVIRONMENT

A CIVIL-KATONAI EGYÜTTMŰKÖDÉS KÉPESSÉGÉNEK ALKALMAZÁSA A KOMPLEX HADMŰVELETI KÖRNYEZETBEN

VARGA Zsófi[1]

Abstract

The rapidly changing security environment of the 21st century has brought to the fore the management of conflicts in the place where they emerge and the importance of peace support, peacekeeping operations and humanitarian activities, in addition to war operations. During these operations, the strategic, operational and tactical levels are not sharply separated, and their implementation is characterized by high civil and political sensitivity. The change in the civilian aspects of the operational environment resulted in the horizontal extension of the use of force and required the doctrinal development of new principles and procedures. Following a paradigm shift in warfare, the study examines the application of Information Operations, in particular Civil-Military Cooperation capabilities, in a complex operational environment.

Keywords

Information Operations, Civil-military Cooperation, Joint Operations Area

Absztrakt

A 21. század gyorsan változó biztonsági környezete előtérbe helyezte a konfliktusok helyben történő kezelését, a háborús műveletek mellett a béketámogató, békefenntartó műveletek, a humanitárius tevékenységek jelentőségét. Ezen műveletek során a hadászati, hadműveleti, harcászati szintek nem különülnek el élesen, végrehajtásuk során magas civil és politikai érzékenység jellemző. A hadműveleti környezet polgári aspektusainak változása a haderő alkalmazásának horizontális kiterjesztését eredményezte és új elvek, eljárások doktrinális kidolgozását követelte. A tanulmány a hadviselésben végbement paradigmaváltást követve vizsgálja az Információs Műveletek, részletesen a Civil-katonai együttműködés képességének alkalmazását a komplex műveleti környezetben.

Kulcsszavak

Információs Műveletek, Civil-katonai együttműködés, közös műveleti terület

[1] zsofivarga05@gmail.com | ORCID: 0000-0001-6187-6274 | Education and Individual Training Branch, Ministry of Defence | Oktatási és Képzési Osztály, Honvédelmi Minisztérium

BEVEZETÉS

Figyelembe véve a 21. századi hadviselés terén bekövetkezett változásokat, a hadszíntér fizikai dimenziói - szárazföldi, légi, tengeri, űrbeli - mellett megjelenő, földrajzilag nem meghatározható információs hadszínteret, amely lehetőséget ad mind az állami, mind pedig a nem állami szereplők számára, hogy az információs környezetben tevékenykedjenek saját érdekeik érvényesítésére, rávilágít a katonai műveletek előkészítése, tervezése és végrehajtása során az együttműködési képesség növelésének és az összhaderőnemi jelleg megerősítésének a jelentőségére. Az információs hadszíntérben végbemenő technikai és kognitív folyamatok célja az információ megszerzésén túl, annak az ellenséggel szemben történő minél hatékonyabb felhasználására összpontosul.

A válságkezelő, felkelés ellenes (Counterinsurgency – COIN) műveletek során kiemelt szerepet kapnak az információs műveletek (Infromation Operations – INFOOPS), felértékelődtek azon katonai képességek – civil-katonai együttműködés (Civil-military cooperation – CIMIC, pszichológiai műveletek (Psychological operations – PSYOPS) – melyek az információs térben jelennek meg. A hadviselés átalakulása, a műveleti környezet változása következtében, eltérő erőket, eszközöket és eljárásokat alkalmazó katonai erőre van szükség. Mindezek rámutattak a CIMIC képesség fontosságára, annak doktrinális hátterének kidolgozására.

ASZIMMETRIKUS HADVISELÉS

„Ha tehát az ellenséget a háború által saját akaratunk teljesítésére kell szorítanunk, akkor vagy képtelenné kell tegyük a védekezésre, vagy pedig olyan állapotba kell juttassuk, amelyben a védelemre való képtelenség veszélye fenyegeti.” [1]

Szempontok	Vesztfáliai rendszer	4. generációs hadviselés
szuverenitás	korlátlan állami szuverenitás	korlátozott állami szuverenitás
hadviselés	állami monopólium, államok közötti konfliktus	állami monopólium csökkenése, megszűnése állami és nem állami szereplők közötti konfliktus
eszköz	hagyományos	új eszközök, kiszámíthatatlanság
eljárás	összemérhető, hasonló	eltérő
doktrínák	kialakult törvényszerűség harcoló -nem harcoló felek	szabályok megszegése, átfedés a határok között harcoló –nem harcoló, harcoló –semleges felek
néphez való viszonyulás	nép, fegyveres erők és a kormány egysége	nép feletti befolyás háttértámogatás megszerzése
cél meghatározása	konkrét célok győzelem vagy vereség	alkalmi győzelem vagy vereség

Táblázat: A hadviselés átalakulása, Varga Zsófi, Szakdolgozat, 2018.

A HADVISELÉS ÁTALAKULÁSA

A modern nemzetközi kapcsolatokat, illetve a modern hadviselés generációinak megkülönböztetését az 1648-ban a harmincéves háborút lezáró vesztfáliai békétől számítjuk. A vesztfáliai béke a hadtörténelem számára is paradigmaváltást jelentett, hiszen az átalakulás folyamán jelent meg a szuverenitás[2] fogalma, a modern nemzetállamok rendszere. A szuverenitás elméletét átfogóan Jean Bodin közelítette meg, aki szerint *„a szuverenitás egy állam állandó és abszolút hatalma… azaz a parancsolás legfőbb hatalma”*. [2] A paradigmaváltás egyik meghatározó fordulópontja volt, hogy létrejött az állam hadviselési monopóliuma, ennek eredményeképpen a nem állami hadviselők háttérbe szorultak, így a háborúkat már nemzetállamok vagy államszövetségek között, saját fegyveres erőkkel vívták meg. [3] A hadszíntéren kialakultak olyan általánosan elfogadott szabályok, eljárások, amelyek a barbarizmust mérsékelték és fejlődésnek indultak az eszközök és a magatartásformák is. *„barbár módra vérrel, sok vérrel áztassuk a harcteret, de eszünk segítségével oly eszközökhöz nyúljunk, amelyek úgyszólván simán hozzák a sikert.”* [4] Ugyanakkor a háború természeténél fogva, a szemben álló felek gyűlölködéséből ered, ezért a háború megvívásának alapja a nép. Clausewitz az ilyen háború természetének leírására a „*csodálatos háromszöget” alkalmazta,* amelyben a három tényező a nép, a kormány és a fegyveres erők együttese veszi fel a harcot az ellenséggel szemben. *„Nem létezhetik oly művelt nép, mely ha létérdekéről van szó, a háborúban önfeláldozással járó könyörületes emberbaráti indulatot tanúsítson, mert: hiszen az, aki a nyers erőszakot minden melléktekintet nélkül alkalmazza, feltétlenül előnyben van a másik fölött.”* [5]

Az eddigi háborús történelem során kialakult tapasztalatok fokozatosan épültek be az államok katonai doktrináiba, olyan alapelveket fogalmaznak meg a haderő számára, mint az erők összpontosítása, a cél meghatározása és a morál fenntartása. Ezeknek az elveknek az alkalmazása lehetővé teszi a haderő számára, hogy a problémákat koherens módon oldják meg, hogy minél előbb véget vethessenek a konfliktusnak. [6] A háború folyamán az ellenfelek által alkalmazott eszközök nagyrészt azonosak voltak, ugyanúgy, ahogy a célok is, megtörni az ellenfél akaratát és ellenőrzés alá vonni az államot.

Korunkban azonban mindezek a megállapítások kiegészítésre szorulnak, ugyanis a klasszikustól eltérően a nemzetállamok közötti háború mára kiegészült a nem állami szereplők határokon átívelő fenyegetéseivel, melynek következtében az állam szuverenitása korlátozottá válik. Gyakori példa, hogy az állam egyre nagyobb teret ad a nemzetek feletti intézményeknek. A nem állami szereplők lehetnek bűnszervezetek, etnikai vagy vallási alapon szerveződő csoportok, politikai indíttatású mozgalmak. Az általuk folytatott harc leggyakoribb formája a felkelés, melynek következtében az állam hadviselési monopóliuma veszélybe kerül. A negyedik generációs hadviselés során ismét megjelennek megkérdőjelezhető magatartásformák és harceljárások, amelyeket nem tekintünk a hagyományos hadviselés részének. Mivel a nem állami hadviselő az állam erőinek alkalmazhatósági szintje alatt helyezkedik el, magatartását nem korlátozzák az állami törvények, annál inkább meghatározó a társadalomtól kapott tartós támogatás. Ennek a társadalmi hálózatnak köszönhetően tudnak információt szerezni, elvegyülni, és újabb tagokat toborozni. A felkelők figyelmen kívül hagyva a doktrínákat, sajátos eszközöket és módszereket alkalmaznak, amellyel a nép akaratára gyakorolnak nyomást. Támadásaikra a kiszámíthatatlanság és az elhúzódó jelleg a jellemző, minél hosszabb ideje tart a konfliktus, annál inkább felhagy a társadalom az ellenállással.

[2] A fogalom a francia felség (souverain) megszólításából ered.

Az állami hadviselő hierarchikus rendszere teljesen átlátható, mivel a célpontok azonosíthatók, irányított támadással a kormányerők gyenge pontjainak ismeretében könnyen sebezhetővé válik a rendszer, ezzel szemben a hálózati kapcsolati rendszer nem azonosítható, így annak felszámolása hatékony hírszerzési képességet és fejlett felderítő rendszerek használatát teszi szükségessé. A kapcsolatrendszer feltérképezéséhez elkerülhetetlen az ún. humántér viszonyainak és magatartásának az ismerete.

A felkelők elleni műveletek során a győzelem a biztonság több aspektusára gyakorol pozitív és negatív hatást, így kettőség alakult ki az erőfölény és a politikai célok mentén. A felkelők érdekében áll kihasználni a másik fél gyengeségeit, amely által közelebb kerülhetnek saját céljaik megvalósításához, hiszen az általuk folytatott hadviselés nem teszi lehetővé a konfliktus politikai alkuval történő lezárását. Számukra a háborús helyzet fenntartása teremti meg a győzelem alapfeltételét és alkalmi győzelemként könyvelhetik el, ha a másik felet olyan helyzetbe kényszerítik, amelyet már nem képes sem gazdaságilag sem politikailag fenntartani, ezért kénytelen megváltoztatni politikai szándékait. [7]

Aszimmetrikus konfliktusok kezelése

Az aszimmetrikus konfliktusok kezelésében állandó problémát jelent a helyi biztonsági erők alacsony hatékonysága, amely nem a felkelők erejével, hanem a műveleti terület lakosságának arányával áll összefüggésben. Az arányokat a konfliktus jellege mindig befolyásolja, viszont, ha biztonsági erők létszáma nem ér el egy bizonyos szintet, képtelenek a közrend és az adott terület biztosítására, ugyanakkor a magas arány sem feltétlenül jelent garanciát. A biztonsági erők legfontosabb feladata a területi ellenőrzés fenntartása a nép védelme érdekében, ehhez az aszimmetrikus konfliktusok során nem kizárt a biztonsági erőket ideiglenesen különleges jogosítványokkal felruházni. A létszámnövelés a toborzás és mozgósítás mellett megvalósulhat milíciák létrehozásával is. A milícia egyfajta mérce, ami tükrözi, hogy a társadalom mennyire bízik a kormány sikerében. Tagjai saját körzetükön belül, állandó jelenléttel azonnal alkalmazhatók - például közigazgatási épületek vagy kritikus infrastruktúra őrzésére - helyismeretük kompenzálja a katonai képességek hiányát. Ugyanakkor a visszaélések elkerülése érdekében az egyéni megbízhatóság is figyelmet igényel. Mind a két fél számára az információszerzés jelenti a legfontosabb stratégiai előnyt, ezért a biztonsági erőknek óvniuk kell képességeiket. [8] A biztonsági erők mellett a rendőrség is alkalmazható, mint a kormány eszközeként bevethető szerv a felkelés felderítésére. A rendőrség rendelkezhet olyan kapcsolatrendszerrel, ami tartalmazhatja az adott körzet felderítő hálózatának elemeit. A lakosságnak biztonságot szükséges szavatolni annak érdekében, hogy információt osszanak meg akár a biztonsági erőkkel, akár a rendőrséggel, amelyek alapján meg lehet kezdeni a műveletek tervezését, azonban a felkelők gyors alkalmazkodóképessége hosszú távon jelentősen csökkenti az adott információ megbízhatóságát.

A felderítés, hírszerzés szerepe

A felderítési, hírszerzési feladatok két fő erőforrással kerülnek végrehajtásra, az emberi (humán) és technikai eszközökkel. Bár a technika fejlődése következtében a műszaki készülékek számtalan képességgel rendelkeznek, napjaink konfliktusainak a lakosság vált a fő színterévé, ezért felértékelődött az emberi erőforrások által folytatott hírszerzés (Human Intelligence - HUMINT)[3] szerepe. A felderítést a művelet környezetének előkészítése előzi meg, melyet a

[3] Human Intelligence, emberi erőforrásból származó információ megszerzésére szakosodott felderítési ág.

tervező, felderítő és a hadműveleti törzs végez a parancsnok döntéshozatalának elősegítése érdekében, lehetővé téve a műveletre való felkészülést és végrehajtást. Meghatározza a felderítés érdekeltségi körzetét, értékeli a műveleti környezetet és annak hatásait, azonosítja az ellenfelet. Amennyiben rendelkezik harcászati doktrínával előzetes következtetéseket vonhatunk le arról, hogy az abban lefektetett elveket a másik fél hogyan alkalmazza a műveletek során. [9] Az aszimmetrikus műveleti környezet számos tényezője hatással van a felderítésre, a műveletek komplexitása következtében a katonai vezetési szintek – stratégiai, hadműveleti, harcászati - egyre inkább összemosódnak, valamint a nem katonai szereplők megjelenése olyan átfogó megközelítést (Comprehensive Approach) igényel, amely segít megteremteni a hatékony együttműködést a katonai szereplők és a műveleti területen tartózkodó különféle szervezetek között.

CIVIL-KATONAI EGYÜTTMŰKÖDÉS

„Úgy vélem, hagyományos erőink valamennyi vezetőjének és parancsnokának meg kell értenie a különleges műveleti erőket és szorosabban együtt kell működnie azokkal – gondolok itt a különleges műveleti erők hadműveleti különítményeire, a civil-katonai kapcsolattartó és a lélektani műveleti csoportokra. A modern csatatéren nem akarhatunk sikert a fenti elemek közötti együttműködés nélkül." [10]

A CIMIC doktrína fejlődése

Első alkalommal a NATO Katonai Bizottsági dokumentuma (Military Committee document - MC) 411/1 határozta meg a CIMIC fogalmát, ami szerint előmozdítja az együttműködést a NATO parancsnoka és a közös műveleti terület (Joint Operations Area - JOA) civil szereplői között. *„A misszió érdekében történő koordináció, a NATO parancsnok és a polgári szereplők között, beleértve a terület lakosságát és a helyi hatóságokat, továbbá a nemzetközi, nemzeti és nem kormányzati szervezeteket és ügynökségeket."* [11] A Szövetségi Összhaderőnemi Kiadvány (Allied Joint Publication -AJP) első CIMIC doktrínája óta a műveleti tapasztalatok folyamatos feldolgozásra kerültek, de a CIMIC fogalma és feladatrendszere változatlan maradt. „*Koordináció és együttműködés a NATO parancsnok és a civil szereplők között, amely magába foglalja a helyi lakosságot és hatóságokat, valamint a nemzetközi, nem kormányzati és helyi szervezeteket."* [12] Szövetséges Adminisztratív Kiadvány (Allied Administrative Publication -AAP) meghatározása: „A NATO parancsnok és a polgári szereplők -beleértve a nemzeti lakosságot és helyi hatóságokat, nemzetközi, nemzeti és a nem kormányzati szervezeteket és ügynökségeket -közötti együttműködés és koordináció a misszió támogatása érdekében." [13] A Magyar Honvédség Összhaderőnemi Civil-Katonai Együttműködési Doktrína a következő képen fogalmazza meg: „*A CIMIC a katonai és a civil oldal -kormányzati és nem kormányzati szervezetek, nemzeti hatóságok, nemzetközi szervezetek és a helyi lakosság -között kiépített és fenntartott koordináció és együttműködés a támogatott parancsnok küldetésének eredményes végrehajtása érdekében. Közvetlen célja a parancsnok küldetésének végrehajtását elősegítő együttműködés létrehozása és fenntartása a műveleti terület civil szereplőivel. Hosszú távú célja, hogy segítsen kialakítani és fenntartani azokat a feltételeket, amelyek hosszú távon hozzájárulnak a válság jövőbeni rendezéséhez."* [14] Ahogy a definíció is meghatározza a CIMIC, mint NATO képességét a parancsnok munkájának támogatására hozták létre. A Szövetségi Összhaderőnemi Kiadványok (Allied Joint Publication -AJP) kezdetben megfeleltek az akkori elvárásoknak, azonban 2003-tól olyan új kihívások jelentek meg, elsősorban Irakból és

Afganisztánból, amelyek számos NATO, köztük a CIMIC doktrína felülvizsgálatát igényelték. A CIMIC doktrína kibővítésének az volt a célja, hogy meghatározza azt a szilárd elméleti alapot, amely megfelel a megváltozott műveleti környezet követelményeinek. A NATO megfogalmazta, hogy a hatékony válságkezelés politikai, polgári és katonai szempontból egyaránt átfogó megközelítést igényel, ennek a szemléletnek a CIMIC doktrínákban is vissza kell tükröződniük, különösképp a polgári-katonai együttműködés területén. [15] Az aktuális CIMIC-doktrína AJP-3.19 az alapelvek, valamint a technikák, taktikák és eljárások mellett, magába foglalja a CIMIC hatékony megvalósításához szükséges struktúrát. A NATO katonai irányelvei és annak alkalmazása a CIMIC vonatkozásában, közvetlenül a Katonai Bizottság Military Committee MC 411/2 által meghatározott politikából származik. Az AJP-3.19 is harmonizált az AJP-01 és más kapcsolódó szövetséges közös kiadványokkal. A technikákkal, taktikákkal és az eljárásokkal kapcsolatos részleteket a Szövetséges Operációs Kézikönyv (AM 86-1-1) tartalmazza. Ezt egészíti ki a CIMIC Funkcionális Tervezési Útmutató (Functional Planning Guide -FPG), amely részletes információkat nyújt a CIMIC tervezés támogatásáról. [16]

Az AJP-3.19 egy új fejezettel az ún. cross-cutting topics (CCT) cikkellyel bővült. Olyan civil környezetet érintő aspektusokat, problémákat vesz sorra, amelyek kezelése tulajdonképpen nem tartozik a katonai feladatok közé, mégis eltérő módon befolyásolják a katonai végrehajtást. Az alábbi témaköröket határozták meg: civilek védelme (Protection of Civilians -PoC); gyermekek és a fegyveres konfliktusok (Children and Armed Conflict -CAAC); nők, béke és biztonság; kulturális javak védelme (Cultural Property Protection -CPP), illetve az integritás létrehozása. [17]A műveletek során elengedhetetlen az egyes CCT-k jellemzőinek és azok egymásra gyakorolt hatásának elemzése a polgári környezettel összefüggésében, mert a CIMIC a biztonsági környezet teljes spektrumának ismeretében tudja eredményesen végezni feladatát.

A katonai műveletek irányítása

A hadtudományban általánosan elfogadott koncepció szerint, a katonai műveletek irányítása négy szinten valósul meg: szakpolitikai, hadászati, hadműveleti és harcászati szinten. A szakpolitikai célok meghatározása és megvalósítása az állam jogrendjének helyreállítása, a beavatkozás időszakában nehezen kikényszeríthetők. Amennyiben az ország legitim politikai elittel rendelkezik, a célok világosak, a szükséges erőkkel és eljárásokkal garantálható azok elérése. A stratégiai célokat is világosan kell megfogalmazni összhangban a politikai érdekekkel, hiszen a biztonsági erők sem tudják az elhibázott politikai döntések negatív következményeit teljes mértékben ellensúlyozni. Tehát a szakpolitika meghatározása után hadászati szinten történik döntés a rendelkezésre álló erőforrások alkalmazásáról. Az Összhaderőnemi Doktrína szerint *„a hadműveleti szint alkotja a kapcsolatot a katonai stratégiai cél elérése és az erők harcászati szintű alkalmazása között."* [18] Itt kell felmérni az ellenség képességeit, megtalálni a sebezhetőségét. Az ellenség erőssége és gyengesége egyaránt a nép, emiatt a biztonsági erők számára érzékeny terület a hadműveleti szint, hiszen a rendelkezésre álló képességekkel legyőzhetik az ellenséget, de ha a harcászati siker következtében jelentős a járulékos veszteség, ennek a lélektani hatása felkelők oldalára állítja a népet, ezért a harcászati sikerek nem mindig könyvelhetők el hadműveleti sikereként. Harcászati szinten történik a fegyveres erők tevékenységének végrehajtása, a sikeres tevékenységek biztosítják a hadműveleti és a katonai stratégiai célok elérését. [19]

A CIMIC FELADATRENDSZERÉNEK BEMUTATÁSA

Ahogy Samuel P. Huntington fogalmaz: „A katonáknak, a rend védelmezőinek nagy a felelőssége. A legnagyobb szolgálat, amit tehetnek az, hogy hűek maradnak önmagukhoz és katonás csöndben, bátran szolgálnak. Ha megtagadják a katonaszellemet, először önmagukat, végső soron a nemzetet semmisítik meg." [20] A fegyveres erő feladatát a lakossággal polgári-katonai együttműködés keretében tudja teljesíteni, ezért a kooperációnak minden körülmények között létre kell jönnie. A következőkben a CIMIC feladatrendszerén keresztül ismertetem polgári-katonai együttműködés megjelenését.

A polgári-katonai kapcsolattartás

Az átfogó megközelítés tükrében a NATO szélesebb körű együttműködés megvalósulását szorgalmazza a civil szereplőkkel. A polgári-katonai kapcsolattartás feladata, hogy a megfelelő szinteken biztosítsa a koordinációt, a harmonizációt és az információ megosztását a civil szektorral, a műveletek tervezésének és végrehajtásának támogatása érdekében. A kapcsolatok kialakítása a tervezés kezdeti szakaszának alapvető része és hozzájárul a további két CIMIC funkció kialakulásához. A polgári-katonai összeköttetés a következőket foglalja magába:

- Az érintett nem katonai szereplők időben történő azonosítása;
- összekötő struktúra kialakítása;
- bizalmas és a nyilvános információk kezelése. [21]

A CIMIC tevékenység megkezdése előtt egyeztetni kell a műveleti területen lévő nemzetközi és helyi civil szervezetekkel, megismerni azok feladatrendszerét, hogy a közös feladatok végrehajtása során ne korlátozzák egymás hatáskörét. Az így begyűjtött információkból a felállított, folyamatosan frissített kapcsolati hálót a műveletben résztvevők rendelkezésére kell bocsájtani. [22]

A haderő polgári támogatása

A parancsnokoknak a közös műveleti területen szükségük van a lakosság támogatására, többek között a katonai műveletek megzavarását elkerülendő erőfeszítések összehangolása érdekében. Az erők egyrészt a polgári információforrásoktól, másrészt a polgári erőforrásoktól származó adatoktól függhetnek, ezért a parancsnokoknak törekedniük kell a műveletek legszélesebb körű polgári támogatottságára. A műveletek tervezésében és végrehajtásában a CIMIC proaktív szerepet játszik. A haderő támogatása a következőket foglalja magába:

- A polgári környezetre vonatkozó információk összegyűjtése, értékelése és jelentése;
- kulcsfontosságú személyek és az érzékeny tényezők beazonosítása, amelyek kritikus hatást gyakorolnak a műveletek tervezésére és végrehajtása;
- felmérni a műveletek civil környezetre gyakorolt hatását; a negatív következmények enyhítése;
- elemezni a nem katonai tevékenységek hatását a saját műveletekre;
- az erők elfogadásának támogatása;
- hozzájárulás a civil társadalom tájékoztatásához a stratégiai kommunikáció által meghatározott erőfeszítésekkel összhangban;
- szükség esetén megkönnyíteni a hozzáférést a nem katonai erőforrásokhoz. [23]

A CIMIC közvetlen, de nem harci támogatással vesz részt a műveleti célok elérése érdekében történő tervezésében és végrehajtásban. A műveleti területről begyűjtött civil környezettel kapcsolatos adatok feldolgozást követően kerülnek a parancsnok elé, illetve a döntés előkészítő szintekre, ahol a nyílt források tájékoztatásainak figyelembevételével kerülnek véglegesítésre. A parancsnoknak a saját felelősségi területén folyamatosan tájékozódnia kell a CIMIC és a PSYOPS eszközök által a biztonsági környezetre gyakorolt hatásokról. [24]

A polgári környezet katonai támogatása

Az átfogó megközelítés keretében a nem katonai szereplőknek és a polgári környezetnek nyújtott katonai támogatást általában csak akkor lehet végrehajtani, ha az szükséges feltételként jelentkezik a katonai feladatok megvalósításához. A polgári környezet támogatása a CIMIC tevékenységek széles skáláját felöleli, amely olyan katonai erőforrásokat igényel, mint az információ, személyi állomány, felszerelés, kommunikációs létesítmények, funkcionális szakértők és a kiképzés. A lépcsőzetes megközelítés szerint a támogatást az alábbi sorrendben kell végrehajtani:

- támogatás az erőforrások és az információ megosztás révén
- a katonai eszközökkel történő támogatás csak a legvégső esetben. [25]

Az aktuális civil környezet értékelése és a műveleti területről érkező adatok feldolgozása után kerül meghatározásra a projekttevékenység fő irányvonala. A támogatás irányulhat a kormány megsegítésére, a stratégia kidolgozását megelőzően felmérik a kormányzati rendszer jellegzetességeit, hiányosságait majd funkcionális szakértőkkel együttműködve helyreállító intézkedéseket állapítanak meg. [26] Ugyan így az infrastruktúra fejlesztése és megóvása is fontos spektrum. Amennyiben a műveleti terület, olyan színes földrajzi adottságokkal rendelkezik, mint például Afganisztán, ahol a természeti katasztrófák nagy gyakorisággal fordulnak elő, az eddigi katasztrófákat és azok kezelésének tapasztalatait feldolgozva napra kész tervet kell készteni a különféle katasztrófahelyzetek kiküszöbölésére. Mivel a természeti csapások egy része előre jelezhető, de váratlanul is bekövetkezhetnek, felszámolásuk összetett feladat, gyors és hatékony megoldását követel. Az elvégzendő feladatok megfelelő irányítás alatti koordinációját szakaszosan, kellő szakmai háttérrel és a főbb felelősök kijelölésével lehet hatékonyan végrehajtani. [27]

Összegezve a CIMIC alkalmazását további négy tényező feltételezi:

- A CIMIC munkatársak teljes mértékben integrálva vannak a parancsnok székhelyére (HQ), valamint teljes körű felhatalmazással rendelkeznek a közös műveleti területen (JOA) a CIMIC tevékenységek és projektek koordinációjára;
- A CIMIC képesség a parancsnok tervének szerves részét képezi, hozzájárulnak a stratégia végrehajtásához, a stabil és fenntartható végállapot megvalósításához. Felügyeli a katonai erők polgári szférához fűződő tevékenységét, szükség esetén biztosítja a funkcionális szakértőket;
- A NATO erők arra törekszenek, hogy támogassák a civil szereplők tevékenységét a kívánt végállapot eléréséhez. A műveletek során stratégiai és hadműveleti szinten kellő mértékben bevonja a tervezésbe a megfelelő polgári testületeket;
- Mind a gyors projekteket és a fejlesztési tevékenységeket is azzal a céllal végzik, hogy azokat rövidesen az illetékes civil szervezetekre vagy helyi hatóságokra átruházzák. [28]

Szakasz	Időbeni elhelyezés	Főbb felelősök	Feladatok
Szakterület specifikus munkacsoport megalakítása	Előre prognosztizált eseményt követően folyamatos felkészülés	Kontingens parancsnoka és a hadműveleti törzs	Esetleges katasztrófa bekövetkezésekor azonnali foganatosítandó intézkedések előkészítése
Állomány tájékoztatása az esetlegesen kialakuló fertőzések hatásairól	Esemény bekövetkezése előtt, felszámolás ideje alatt folyamatosan	Kontingens parancsnoka és egészségügyi szakszemélyzet	Tünetekre való felhívás és azok kezelési lehetőségei
Kár felmérése	Esemény bekövetkezését követően, valamint kárfelszámolás alatt folyamatosan	Irányító szerv és végrehajtó alegységek	Teljes körű állapot feltérképezése (épület, utak, elektromos és egyéb hálózatok stb.)
Cselekvési változatok kialakítása a táboron belüli mentesítési és újraépítési feladatok elvégzése érdekében	Esemény típusától függően a legrövidebb időn belül	Kontingens parancsnoka és a hadműveleti törzs, valamint szakterület specifikus tanácsadók	Legoptimálisabb változat kialakítása, figyelemmel a háborús övezet veszélyeire
Műveleti terület, -ekkor már háborús övezet -folyamatos monitorizálása személyi védelem miatt	Folyamatos és további Force Protection erőkkel megerősített	kontingens hadműveleti részleg és felderítő részleg, CIMIC és PSYOPS csoportok	Lakosság és ellenálló elemekről adatszerzés és értékelés, a teljeskörű védelem érdekében
Lakosság folyamatos tájékoztatása, segítése a pánik és lincs hangulat elkerülése érdekében	A prognosztizálható természeti jelenség megjelenésétől a mentesítési feladatok befejezéséig	CIMIC és PSYOPS csoportok	Veszélyre és annak következményeire történő felhívás, segélyek osztásának koordinálása, egészségügy…stb.
Szakasz	**Időbeni elhelyezés**	**Főbb felelősök**	**Feladatok**
Kiküszöbölési terv elkészítése, optimális vezetői döntéshozatal	Vezetői döntéshozatalt követően azonnal	Kontingens parancsnoka és a hadműveleti törzs, valamint szakterület specifikus tanácsadók	Ütemterv elkészítése és a munkálatok előkészítése
Munkálatok végrehajtása	Parancs kiadását követően,	Felkészített erők	Eredeti állapot visszaállítása, teljes körű mentesítési feladatok végrehajtása

2. Táblázat: A feladat végrehajtásának menete, Patyi György: Afganisztáni misszió alatt magyar tábort érő természeti csapás következményeinek felszámolása háborús körülmények között

ÖSSZEGZÉS

Ahogy arra a CIMIC is rávilágít, a humán környezet feltérképezése elengedhetetlen a válságkezelő és az aszimmetrikus konfliktusok katonai műveleteinek minél hatékonyabb előkészítése, tervezése és végrehajtása érdekében. A képesség célja olyan támogató környezet megteremtése és fenntartása, amelyek - főként katonai előnyök (információs fölény) biztosítá-

sával - segítik a parancsnokot feladatainak eredményes végrehajtásában, amelynek megvalósításában az információs műveletek további technikai és kognitív képességei is alkalmazásra kerülnek. A hadműveletek támogatását célzó CIMIC karöltve a PSYOPS műveletek alkalmazásával képes a haderő katonai sikereinek támogatására a pozitív, semleges és negatív befolyásoló, valamint tájékoztató tevékenységek révén.

Annak érdekében, hogy a műveleti környezet szegmenseiben végbemenő változásokat, ok-okozati összefüggéseket megértsük, a társadalomtudományok széles ismereteivel is rendelkeznünk kell, ugyanakkor a műveletek során nélkülözhetetlen a helyi lakosság kulturális aspektusainak megértése, ezért különös jelentőséggel bír a kulturális antropológia alkalmazása. A tapasztalat feldolgozások igazolják a társadalomtudományok és a katonai hírszerzés közötti kapcsolat szükségességét. Ahhoz, hogy ez képességként megjelenjen az amerikai haderő létrehozta a Human Terrain System (HTS) rendszert, amely során katonai egységekbe ágyazott csapatok folytatnak társadalmi tudományi kutatásokat a helyi lakosságról, ezzel támogatva a katonai vezetés döntéseit és segítve a hadszíntéren állomásozó csapatokat. [29]

A folyamatos tapasztalatfeldolgozás, a társadalomtudományok felhasználása és a következtetések interpretálása rendkívül fontos a képesség további fejlődése érdekében és elengedhetetlenek az információs műveletek hatékony alkalmazása érdekében, napjaink konfliktusainak kezelésében.

IRODALOMJEGYZÉK

[1] KARL, von Clausewitz: A háborúról, Budapest, Athenaeum Irodalmi és Nyomdaipari Rt., Második kiadás, 1917., pp. 16.
[2] JEAN, Bodin: Az államról, Budapest, Gondolat Kiadó, 1987., pp. 73.
[3] RESPERGER István - KISS Álmos Péter - SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban, Budapest, Zrínyi Kiadó, 2014., pp. 67.
[4] KARL, von Clausewitz: A háborúról, Budapest, Athenaeum Irodalmi és Nyomdaipari Rt., Második kiadás, 1917., pp. 191.
[5] KARL, von Clausewitz: A háborúról, Budapest, Athenaeum Irodalmi és Nyomdaipari Rt., Második kiadás, 1917., pp. 16.
[6] Allied Joint Doctrine AJP-01 (E), Nato Standardization Office, 2017., 1-13. 1-14.
[7] BAKOS, Csaba Attila: Clausewitz „újratöltve", Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 2015., pp. 101.
[8] KISS, Álmos Péter: Háború a nép között - Esettanulmányok a negyedik generációs hadviselés történetéből, Zrínyi Kiadó, Budapest, 2016., pp. 141 –143.
[9] HOLNDONNER, Hermann: A Magyar Honvédség összhaderőmei felderítő rendszere működésének elemzése, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Budapest 2014., pp. 72.
[10] L., Magruder dandártábornok, Joint Readiness Training Center
[11] MC 411/1 NATO Military Policy on Civil-Military Co-operation (CIMIC), NATO Military Committee, 2001.
[12] AJP-3.4.9 Allied Joint Doctrine for Civil-Military Cooperation (CIMIC), NATO Standardization Agency (NSA), 2013., https://www.cimic-coe.org/wp-content/uploads/2014/06/AJP-3.4.9-EDA-V1-E1.pdf 2-1 (Letöltve: 2018.09.20.)
[13] AAP–6, Allied Administrative Publication, NSA, 2014., 2-C-5, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf (Letöltve: 2022.01.10.)

[14] Magyar Honvédség Összhaderőnemi Civil-Katonai Együttműködési Doktrína. Honvédelmi Minisztérium, Honvéd Vezérkar Hadműveleti és Kiképzési Csoportfőnökség (HM HVK HDMKIKCSF) kiadványa, Budapest, 2004.
[15] HANGYA, Gábor: About NATO CIMIC Doctrine, CIMIC Centre of Excellence (CCOE), 2014., pp. 14.
[16] AJP-3.19, Allied Joint Doctrine For Civil-Military Cooperation, NSO, 2018., pp. 17. https://www.cimic-coe.org/wp-content/uploads/2018/11/AJP-3.19-EDA-V1-E.pdf (Letöltve: 2022.01.22.)
[17] AJP-3.19, Allied Joint Doctrine For Civil-Military Cooperation, NSO, 2018., B-1 https://www.cimic-coe.org/wp-content/uploads/2018/11/AJP-3.19-EDA-V1-E.pdf (Letöltve: 2022.01.22.)
[18] MH Összhaderőnemi Doktrína, pp. 2-20.
[19] KISS, Álmos Péter: Háború a nép között, Budapest, Zrínyi Kiadó, 2016., pp. 160-163.
[20] SAMUEL, P. Huntington: A katona és az állam, Budapest, Zrínyi Kiadó, 1994., pp. 453.
[21] AJP-3.19, Allied Joint Doctrine For Civil-Military Cooperation, NSO, 2018., 2-5 https://www.cimic-coe.org/wp-content/uploads/2018/11/AJP-3.19-EDA-V1-E.pdf (Letöltve: 2022.01.23.)
[22] POLYECSKÓ, László: Az MH PRT civil-katonai együttműködési és a lélektani műveletek tevékenysége in. Boldizsár Gábor, Wagner Péter: A Magyar Honvédség befejezett szárazföldi műveletei Afganisztánban, Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 122-123.
[23] AJP-3.19, Allied Joint Doctrine For Civil-Military Cooperation, NSO, 2018., 2-7 https://www.cimic-coe.org/wp-content/uploads/2018/11/AJP-3.19-EDA-V1-E.pdf (Letöltve: 2022.01.22.)
[24] POLYECSKÓ, László: Az MH PRT civil-katonai együttműködési és a lélektani műveletek tevékenysége in. Boldizsár Gábor, Wagner Péter: A Magyar Honvédség befejezett szárazföldi műveletei Afganisztánban, Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 123.
[25] AJP-3.19, Allied Joint Doctrine For Civil-Military Cooperation, NSO, 2018., pp. https://www.cimic-coe.org/wp-content/uploads/2018/11/AJP-3.19-EDA-V1-E.pdf 2-7 (Letöltve: 2022.01.23.)
[26] PPOLYECSKÓ, László: Az MH PRT civil-katonai együttműködési és a lélektani műveletek tevékenysége in. Boldizsár Gábor, Wagner Péter: A Magyar Honvédség befejezett szárazföldi műveletei Afganisztánban, Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 124.
[27] PATYI, György: Afganisztáni misszió alatt magyar tábort érő természeti csapás következményeinek felszámolása háborús körülmények között, NKE, Budapest, pp. 15.
[28] AJP-3.4.9 Allied Joint Doctrine for Civil-Military Cooperation Edition A Version 1, Nato Standardization (NSA), 2013., pp. 2-1
[29] MONTGOMERY, McFate - Steve Fondacaro: Reflections on the Human Terrain System During the First 4 Years, PRISM, Center fot Complex Operations, 2011., 2. évfolyam, 4 szám, pp. 63-69.

PROTECTION AGAINST LISTENING VS. INFORMATION LEAKAGE CHANNELS

LEHALLGATÁS ELLENI VÉDELEM VS. INFORMÁCIÓSZIVÁRGÁSI-CSATORNÁK

DOMJÁN András [1]

Abstract

Today, the press deals relatively frequently with the subject of interception, which can be approached from various perspectives. On the one hand, the focus was on obtaining information to enforce law enforcement interests, and on the other hand, so-called unauthorized, illegal observations were featured in the media. Protection against eavesdropping interacts with the need to obtain information on an ongoing basis, whether or not it is carried out unlawfully in a manner permitted by law or in the absence thereof. This dynamic phenomenon can be observed in our living environment as well as in the case of corporate, public or government buildings. Interception protection and information leakage channels are fairly closely related concepts that need to be addressed in a same system. In the following, I will describe these two areas based on their interaction.

Keywords

eavesdropping, information leakage channel, information protection, security awareness

Absztrakt

Manapság a sajtó viszonylag sűrűn foglalkozik a lehallgatás témakörével, amelyet különböző aspektusokból közelíthetünk meg. Egyfelől a bűnüldözési érdekek érvényesítése miatt alkalmazott információszerzések kerültek a fókuszba, másfelől pedig az úgynevezett engedély nélküli, illegális megfigyelések szerepeltek a médiában. A lehallgatás elleni védelem folyamatos kölcsönhatásban van az információszerzési igénnyel, függetlenül attól, hogy azt a törvény által engedélyezett módon vagy annak hiányában törvénytelenül végzik. Ez a dinamikus jelenség megfigyelhető a lakókörnyezetünkben ugyan úgy, mint a vállalati-, köz-, vagy kormányzati épületek esetében. A lehallgatás elleni védelem és az információszivárgási csatornák meglehetősen szorosan összefüggő fogalmak, amelyeket egy rendszerben kezelve kell vizsgálnunk. A következőkben ezt a két területet az egymásra gyakorolt hatásuk alapján, a közvetlen környezetünk és az objektumvédelem szemszögéből ismertetem.

Kulcsszavak

lehallgatás, információszivárgási csatorna, információvédelem, biztonságtudatosság

[1] andras.domjan@gmail.com | ORCID: 0000-0002-0178-5263 | head of department, Counter Terrorism Centre Head of Information Protection Department | osztályvezető, Terrorelhárítási Központ Információvédelmi Osztály

INFORMATION PROTECTION IN GENERAL

Nowadays, the acquisition, use, or attack of various "sensitive" information can have an impact on politics, economic actors, or even public administration. These phenomena are closely linked to informing and, where appropriate, influencing the public, freedom of the press itself and, last but not least, human rights issues. The functioning of today's modern social communication and the development of related expression habits can in some cases result in difficult-to-predict consequences. The information-sharing dumping that appears here also provides an opportunity for individuals to disclose sensitive information. There is more and more talk in the economic and industrial fields about the so-called industrial espionage, the acquisition of protected data related to product development and company strategy. As a result of technological advances, more and more professional covert surveillance tools are becoming available to everyone in the market, creating the opportunity to increase the number of secret data mining activities. Although this type of act is legal only under strict legal conditions, its trade has evolved into a fairly thriving industry through online webshops. The possibility of obtaining hidden information is given in the same way in the private sector as in the industrial environment, or even in government areas. Because of the increase in these risks, it is imperative for companies to develop their own security strategy to implement information protection.

Particular emphasis should also be placed on the training and education of individuals in this process. Interception protection and information leakage channels are both part of a larger set called the Information Security field. In the classic sense, telephone tapping is now a controlled connection to a complex infocommunication system, as both the mobile telephone network and landline telephone lines provide connections via digital exchanges.

In terms of industrial and corporate security, there is an increasing emphasis on information security and, in particular, protection against eavesdropping. The importance of the field is also proved by the fact that a separate series of standards deals with the topic under the number MSZ ISO / IEC 27001: 20xx[2]. The 2014 release is currently available with newer modifications. The standard deals with the establishment, implementation, continuous monitoring and definition of development requirements for Information Security Management Systems. It sets standards for government, commercial and non-profit organizations regarding their information systems to increase security, data protection and availability. The information security management system is based on the so-called PDCA[3] model. This allows us to continuously monitor and analyze the risks and then optimize our security system to achieve the appropriate level of protection. [1] After describing the main areas of information security, I present the concept of "eavesdropping", starting from the risks in our everyday life, the challenges and tasks to be solved in the field of corporate and related objects protection.

[2] Information technology — Security techniques — Information security management systems. Requirements MSZ ISO/IEC Hungarian National Standard

[3] Plan-Do-Check-Act

FIELDS OF INFORMATION SECURITY

In order to guarantee confidentiality, integrity and availability, the data or information to be protected shall not be accessed by unauthorized persons, in any form, from personal security to document security to electronic information security. Accordingly, we can distinguish between physical, personal, documentary, and electronic information security based on access to information. [2]

In order to protect the information to be protected and to prevent access to infocommunication systems, it is necessary to develop a complex security measures process, together with the associated technical equipment. Physical security includes all mechanical and security protection solutions, architectural and structural designs that are able to guarantee controlled access to the protected area, the infocommunication system and the data itself. In the case of highly protected objects, great emphasis is placed on adequate physical security, primarily due to the construction of protection against explosion. In addition to the reinforcement of the building, the nearby surroundings must be coordinated with the object in order to maintain the necessary safety distances.

The scope of personal security includes the right to access classified information and to know its content at a certain level. The authorization process for access to confidential data should be preceded by a national security "screening" to identify potential risks. Continuous monitoring and multi-step access can reduce information leakage.

Document security is closely related to personal security, as the data and documents that contain the information to be protected are classified into different levels of classification, which determines the conditions under which they can be accessed and their contents known.

Electronic information security (INFOSEC) represents the infocommunication system (ICT[4]) itself, its network elements, terminals, its operational characteristics, rules, installation requirements and its impact on the environment.

Areas of electronic information security [3]:

- Transmission Security - TRANSEC
- Emanations Security - EMSEC
- Cryptographic Security - CRYPTOSEC
- Computer Security - COMPSEC
- Network Security – NETSEC

It follows from the territorial division that the equipment building the information network, the transmission media and the regulations necessary for their operation are all organized into separate groups, together with the related information protection regulations.

INFORMATION LEAKAGE - CHANNELS

The presentation of the areas of information security is a good example of how complex a system should be built, operated in a coordinated manner, and protected from

[4] Infocommunication technology

possible external "harmful" influences. In this complex system, the information leakage channels represent the set of equipment and other technical solutions that enable the transmission, radiance, connections or display of the data to be obtained. We can identify two forms depending on the type of human behavior required to obtain the information. This can be a targeted activity aimed directly at obtaining information, this is called an act of active or some kind of omission or negligence, which allows access to data, this is called a passive leakage channel. In practice, we can encounter it in the following ways.

Active information leakage channel

In order to obtain the information to be targeted, the perpetrator performs a deliberate act by extracting from the infocommunication system himself the oral speech, the events and the written materials, or the appropriate information obtained in the nearby vicinity of the target person or company and record or transmit without consent. This type of activity is illegal, only allowed to the secret services and the police, subject to strict legal conditions, for a specified period of time. Nevertheless, the industry is booming thanks to e-commerce, with virtually the capabilities of professional eavesdropping devices available for purchase without a license.

I would like to note here that in Hungary these products can be classified as "secret service equipment"[5] and their application falls within the scope of military technical activities. It is also illegal to make a statement or make a false statement about a fact that was not made during the procurement procedure, usually during the customs procedure.

Passive information leakage channel

This category includes all electronic devices, equipment, systems capable of transmitting sound, images and data, which, due to their normal or, where appropriate, different operation, provide an opportunity to get to know some or even all of the information.

In order to maintain an adequate level of information security, it is necessary to detect and continuously monitor information leakage channels and, if possible, to eliminate them. Given the complexity of the process, this type of "countermeasure" necessitates the development of a complex system of protection. Protection against interception (TSCM[6]) and eavesdropping are an integral part of security measures.

EAVESDROPPING PROTECTION

Eavesdropping protection as an activity in the field of information security cannot be linked to a single area, but rather to information leakage channels. Examining the concept literally, eavesdropping as an objective verb according to the interpretive dictionary of the Hungarian language: „*A telephone conversation is listened to and interrogated by a person who is on the line without the knowledge of the speakers."*[7].

[5] 156/2017. (VI. 16.) Government decree on detailed rules for the authorisation of military technical activities and the certification of enterprises, XXVI. Chapter

[6] Technical Surveillance Countermeasure

[7] https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/l-39E16/lehallgat-3AECA/

Protection against eavesdropping is no longer to be taken literally, as the human voice itself is coded in a significant part of infocommunication technologies or as part of an application. The human thought itself can be considered as the starting point of the sound, data and other information that is the subject of the activity. At the present state of the art, it is not yet possible to display this with any equipment. Experiments are already underway in this area and with surprisingly good results, which means that Dutch and German researchers have been able to display the frames imaged by the human brain while watching a movie. This process was solved with a software called Brain2Pix, which put together the image seen from the fMRI[8] signals. [4] We do not yet have to reckon with this type of interception device in terms of information protection, but a similar technological process is taking place, even in the case of converting speech into an electrical signal. This is important for detection because sound, as an acoustic signal, propagates through its environment, even indirectly. Due to the complexity of the infocommunication systems, the interception cannot be handled from a purely human or technical point of view, as the joint involvement of the two areas is necessary for the realization of the act.

In connection with wiretapping, I only deal with illegal acts, I do not cover the collection of hidden audio and video information that falls within the remit of the secret services. The rather varied repository of commercially available "bugs" allows covert observations to be made as described above, creating an active channel for information leakage. In this field, the secret observation and eavesdropping is usually supported by the fact that in our everyday life and environment, technical inspection is not typical as a preventive activity. In addition to the intrusion detection system, a well-established network of cameras can be effective in terms of protection so that no spy devices in our apartment are "forgotten", as they must somehow be introduced first in order to achieve the desired goal. However, the passive information leakage channels created by the equipment we operate can be a much bigger problem in everyday life. Of these, I would mention the breath monitors and the baby monitors, which are audio and video transmission devices designed with wireless transmission, most of which also have a speaker, which is practically suitable for two-way communication. Depending on the method of radio transmission, unauthorized persons have the option of displaying the signal available on the air with a suitable receiver. One such incident occurred in 2013 in Houston, USA, when a couple heard suspicious noises from their 2-year-old girl's room after washing their dishes after a birthday dinner. Entering the room, a man woke their child through the baby monitor with obscene words. As it turned out, the camera device was connected to the internet on the wifi without adequate protection, so the stranger was able to access the camera. [5] In the case of analogue or digital RF cameras, depending on the sensitivity of the receiver, it is possible to obtain information by approaching the residential property.

Cameras installed in homes for security purposes can also pose a threat, as various software vulnerabilities allow hackers to gain access to our private lives as well. This happened in 2020 when a group of hackers claimed to have gained access to 50,000 home cameras and began selling their recordings online. [6]

[8] functional Magnetic Resonance Imaging

POSSIBILITIES OF LISTENING PROTECTION IN THE FIELD OF OBJECT PROTECTION

Protection against eavesdropping as part of information protection already faces serious challenges in business. Based on the risk assessment, the areas and processes of vulnerability can be identified, if possible, the possible channels of information leakage, and then the security measures can be determined. Information security can only be guaranteed by building a complex object protection system. The most critical component of the information protection measures developed as part of the facility insurance can be considered the people working there and the people visiting it, as the lack of appropriate knowledge can pose a serious risk. Unlike privacy, there is already a complex interaction between the human factor and the information security system in the area of corporate security. Personnel operating security equipment must be provided with ongoing training on current risks and their effects on security systems. Complex object protection systems can be basically divided into active and passive components.

Active protection solutions

We need different technical and tactical components to detect and prevent information leakage channels. We can be the first to consider regime measures related to properly controlled and enforced information security. This includes the introduction and use of flash drivers and any wireless equipment at the workplace. As part of our audit of TSCM activity, we are faced with the issue of confidentiality, should the company have its own technical review team if it does not have its own technical review team? This can be a headache in many cases, but it should not be forgotten that the use of instruments in reconnaissance is a rather expensive risk to the use of rather expensive devices, without them or with weaker parameters. The active category includes so-called RF monitor systems that continuously monitor of the radio spectrum. Building this type of protection is quite complicated, but it is the best solution in terms of its effectiveness. The spectrum analysis used as part of the technical review can only provide real frequency data to the operator for a short period of time, for the duration of the TSCM. Monitoring of the continuous frequency range is essential for the detection of "store and forward" type interception devices and should therefore be considered as part of effective information protection systems. In many cases, RF jammers known from military applications are recommended as protection against eavesdropping devices using radio transmission, which is a separately licensed activity.

In my opinion, in our basically crowded radio frequency environment, it is not considered to be the most efficient concept, as digital transmission technology is in many cases optimized for interference protection, so as a positive feedback it means a continuous increase in RF power, practically creating a micro oven around us. Due to the acoustic characteristics mentioned earlier, interfering devices, so-called white noise generators, are also used in the sound range, which can overdrive electroacoustic equipment and make it unsuitable for conversion (digitization). Various vibration generators are recommended for the protection of doors and windows, room partition and space dividers, in order to provide protection against contact microphones.

Passive protection solutions

In this category we can consider primarily the structural designs of the parts of the object to be protected, which are able to reduce the efficiency of the various transmission methods or even make the connection impossible. Examples include the need for RF shielding techniques using the Faraday cage principle and the need to create so-called protected negotiators. In many cases, it is not feasible to implement an "tin box" type office, but various wallpaper-like conductive materials (copper and carbon fiber coverings) and films with significant RF attenuation to protect the windows are available on the market. The combined use of these can provide up to 40 dB attenuation for protection, which can degrade the signal-to-noise ratio under certain power conditions to such an extent that a hidden eavesdropping device with wireless transmission cannot be operated. In some cases, the location of the office, such as being designed for the basement, taking advantage of the "beneficial" effect of reinforced concrete structures, has already significantly increased the security of the room.

In many cases, the security methods and designs described above are not fully implemented in practice, and information security incidents may occur. We have recently witnessed such a case in connection with a data leak in Vigadó, Budapest. In 2017, V4s and Israel held talks on a wave of refugees when, following a private discussion through the interpreter system, the Israeli prime minister shared his personal views. At the same time, members of the press were admitted to the room designated for them, where they also had access to the same interpreting system as the meeting. This was recorded by one of the participants and shared on the international news portal. [7]

IR transmission was used in this situation, but due to the organizational problem, a data leak still occurred. The source of similar problems could be audio equipment using RF connections, or so-called micro ports used for voice transmission if they do not include an encryption algorythm.

INFORMATION PROTECTION IN EVERYDAY LIFE

Due to technical progress, the infocommunication equipment we usually use, due to its complexity, is closely related to our daily activities and habits, and possibly to our interests. The resulting information can be stored in digital form or transmitted in real time via the available communication channel. This is where leaks caused by wearable devices occur, which can indirectly become an operator of an information leakage channel. As a result of uploading data from a fitness class using bluetooth technology to a server, the results of which were shared and made visible on a map, a map of Singapore's secret military base emerged. [8] Our infocommunication equipment, our objects of use, are typically devices supported by continuous software updates, which are provided by the developers at regular intervals. The new version reaches the users after detecting the errors and vulnerabilities of the applications and then fixing them. In the event that someone does not perform these proposed updates, in some cases, there is a serious information security risk, creating an opportunity to establish information leakage channels.

In the spirit of "Connecting World," the explosive spread of IoT[9] technology in our everyday devices and environments provides new opportunities for hackers to discover and exploit information security vulnerabilities. Sensors and data transmitters, built on a myriad of wireless connections, generate traffic in the radio spectrum that can only be detected and filtered out with software with serious analytical capabilities.

SUMMARY

Taking into account the complexity of Information Security, it can be stated that it is only possible to create and operate efficiently functioning security systems in a complex way, taking into account the human factor. In addition to the personnel handling the surveillance systems, the safety-conscious behavior of individuals using electronic infocommunication equipment is also required to achieve the desired result. The average user needs a degree of self-control so that he or she does not have to connect step-by-step to all open Wi-Fi hotspots and keeps his or her software up-to-date. To achieve this, training and education are required at regular intervals for users to maintain an adequate level of protection for their own devices in addition to corporate infocommunication equipment. From the description of eavesdropping protection related to object protection, it can be seen that the classic "bug search" is not a sufficient tactical element to ensure complete security. In addition to the TSCM activity performed by specially trained professionals, a permanent RF monitor system, operated with software with appropriate processing capabilities, can guarantee the desired level of security.

LITERATURE

[1] MSZ ISO IEC 27001, „Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények," MAGYAR SZABVÁNYÜGYI TESTÜLET, 2014.
[2] Dr. Haig Zsolt, „Hadmérnök," 22. November 2006. [Online]. Available: http://www.hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html. [Hozzáférés dátuma: 15. 10. 2018.].
[3] Várhegyi István, Haig Zsolt, Hadviselés az információs hadszíntéren, Budapest: Zrínyi Kiadó, 2005.
[4] „BITPORT," 03. 04. 2021. [Online]. Available: https://bitport.hu/kivetitettek-hogy-mit-lat-az-agy-kelloen-horrorisztikus. [Hozzáférés dátuma: 08. 10. 2021.].
[5] Alana Abramson, „abcnews.go," 13. 08. 2013. [Online]. Available: https://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/. [Hozzáférés dátuma: 11. 10. 2020.].
[6] Szabó Dániel, „napi.hu," 22. 10. 2020. [Online]. Available: https://www.napi.hu/tech/kamera-biztonsagi-kamera-adatlopas-hacker.716124.html. [Hozzáférés dátuma: 14. 02. 2021.].
[7] hvg, „hvg.hu," 19. 07. 2017. [Online]. Available: https://hvg.hu/itthon/20170719_Bekapcsolva_maradt_Netanjahu_mikrofonja_Budapesten_ahogy_az_EUt_szidta. [Hozzáférés dátuma: 21. 07. 2017.].
[8] Rob Cyrill, „telegraph.co.uk," 18. 01. 2018. [Online]. Available: https://www.telegraph.co.uk/news/2018/01/28/fitness-tracker-data-reveal-locations-military-bases-personnel/. [Hozzáférés dátuma: 15. 04. 2019.].

[9] Internet of things

CYBER SECURITY IN 2021 IN THE BANKING SECTOR AND FINANCIAL ORGANIZATIONS

KIBERBIZTONSÁG 2021-BEN A BANKSZEKTORBAN ÉS A PÉNZÜGYI SZERVEZETEKNÉL

GULYÁS Olivér[1], KISS Gábor [2]

Abstract

Every year marks another "worst year ever" for cyber-attacks. In 2021 cybersecurity was again in spotlight. The number of data breaches until September 30, 2021, has already exceeded the total number of events in 2020 by 17 percent [1]. The banking sector was disproportionately affected by the scale of the attacks. In the first half of 2021 blackmail virus attacks increased by 1318 percent on a y-o-y basis [2]. Therefore, in addition to taking advantage of the rapid development of information technology, the potential threat of the attack surface of the banking sector is increased and exposed to more sophisticated cyber threats. With the development of digital technology hackers are also improving their skills, building maximum protection against their malicious attacks is an increasing challenge for professionals. Day by day, more and more businesses are using the digital solutions offered by banks, which is why effective cybersecurity programs have become more important than any other-ever.

Keywords

hacker, banking sector, digital attacks, cyber threats

Absztrakt

A kiberbiztonsággal kapcsolatban minden évben azt gondoljuk, hogy ezt volt az eddigi legrosszabb év. 2021-ben a kiberbiztonság ismét nemvárt rivaldafénybe került. Az adathalász támadások 2021 szeptember 30-ig már 17 százalékkal meghaladták 2020 összes támadásának számát [1]. A bankszektort aránytalanul nagymértékben érintették a kibertámadások, 2021 első félévében 1318%-kal nőtt a zsarolóvírus-támadások száma év-per-év alapon [2]. Éppen ezért, a rohamos információ technológiai fejlődés mellett, a bankszektort érintő veszély potenciális támadási felülete is megnövekedett és napról napra kifinomultabb kiberfenyegetésnek vannak kitéve. A digitális technológia fejlődésével a hackerek is fejlesztik tudásukat, és a rosszindulatú támadásaik ellen maximális védelmet kiépíteni egyre nagyobb kihívást jelent a szakemberek számára. Napról napra egyre több vállalkozás használja a bankok által kínált digitális megoldásokat, éppen ezért a hatékony kiberbiztonsági programok minden eddiginél fontosabbá váltak.

Kulcsszavak

hacker, bankszektor, digitális támadások, kiberfenyegetések

[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbudai University | doktorandusz, Óbudai Egyetem

[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-937 | associated professor, Óbudai University | egyetemi docens, Óbudai Egyetem

BEVEZETÉS

Mára már szinte minden bank bevezette a különböző mobil alkalmazásokat, amelyek új sebezhetőségi pontot kínálnak a kiberbűnözők számára, akik az ügyfelek banki adatait veszek leggyakrabban célba, hiszen a pénzügyi adatok óriási értékkel bírnak.

A banki alkalmazások két oldalról támadhatóak, egyrészt a kliens oldali alkalmazások révén, másrészt pedig szerver oldalról. Ezért a bankoknak biztosítaniuk kell az érzékeny adatok biztonságát az ügyfél eszközéről való hozzáféréskor, valamint a banki szervereken történő tároláskor. A pénzintézetek (is) sokszor külsős vállalkozást bíznak meg a szoftvereik programozásához és azok karbantartásához. A tapasztalatok alapján ők kevésbé tartják magukra nézve kötelezőnek a vállalati biztonsági szabályok betartását – így a hackerek rajtuk keresztül is indíthatnak támadást [3].

A pénzügyi szervezeteknek teljes mértékben át kell látniuk az információ technológiai ökoszisztéma sérülékenységét, és a támadások végrehajtásához használt különböző támadási vektorokat, ahhoz, hogy átfogó kiberbiztonsági programot tudjanak kidolgozni. Fontos, hogy a biztonsági rendszert kiépítők ne csak lépést tartsanak a folyamatosan fejlődő kiberbűnözőkkel, hanem egy lépéssel előttük járjanak.

A cikk célja bemutatni milyen kiberkockázatok merülnek fel a pénzintézeteknél, hogyan lehetne növelni a pénzintézetek hálózatainak biztonságát, ez által megakadályozva a veszteségeket. Ennek érdekében, adaptálhatóak-e a legújabb információ technológiai fejlesztések, azon belül a blokklánc technológia.

TÁMADÁSI VEKTOROK, TÁMADÁSI FELÜLETEK ÉS BIZTONSÁGI RÉSEK

A kiberkockázat kezelési program hatékony felépítéséhez meg kell ismernünk a támadási vektorok, a támadási felületek és a biztonsági rések közötti különbséget.

A támadási vektorok azok az eszközök vagy taktikák, amelyek segítségével a hackerek jogosulatlanul hozzáférhetnek egy hálózathoz.

A szervezet támadási felülete az összes olyan érintkezési pont, amelyeken keresztül a támadók hozzáférhetnek a hálózathoz, manipulálhatják azt, vagy érzékeny adatokat nyerhetnek ki. A támadási felületek lehetnek fizikaiak vagy digitálisak. A fizikai: hardver vagy fizikai eszközök, például számítógépek, táblagépek, útválasztók és szerverek; A digitális támadási felültek magukban foglalják például a szoftvereket, webes és asztali alkalmazásokat, hálózatokat és portokat.

A biztonsági rések digitális vagy fizikai hacker támadásnak adhatnak teret ezért különös figyelemmel szükséges kezelni őket. A legfontosabb azonban az emberi tényező, a csalódott vagy képzetlen, tájékozatlan alkalmazottak. Az emberek kezelik az információt, mint erőforrást, de rajtuk keresztül történhet az adatszivárgás is, melynek következtében illetéktelen felek hozzáférnek, ellopják vagy közzéteszik egy szervezet bizalmas vagy védett információit [3]. Ennek megelőzése érdekében fontos a jogosultsági szintek meghatározása: minden dolgozó csak azokhoz az adatokhoz és munkafolyamatokhoz férjen hozzá, amelyek a feladatköre ellátásához szükségesek. A dolgozókkal meg kell ismertetni a szervezet adatvédelmi és informatikai biztonság politikáját, fel kell hívni a figyelmüket a lehetséges veszélyekre.

TÁMADÁSOK OKAI

A kibertámadásoknak számos különböző oka van, de a leggyakoribb indíték a pénzbeli haszonszerzés. A második leggyakoribb támadás a személyazonosításra alkalmas adatokhoz való hozzáférés megszerzése, mivel ez által üzleti titkokhoz, szabadalmaztatott információkhoz juthatnak hozzá a hackerek. Szintén gyakori ok egy vállalat hírnevének szándékos csorbítása, vagy negatív üzleti pozícióba hozása, ez által ellehetetlenítése. Az információ típusa függvényében a támadók a megszerzett információ megosztásával, szenzitív adatok (cég vagy az adott személyre vonatkozó) világhálóra kerülésével is zsarolhatnak.

A kiberbűnözők két átfogó módon hajthatnak végre támadást. Az egyik a digitális támadás, a másik a fizikai támadás, amely során személyesen próbálnak bejutni egy irodaházba és ily módon adatokhoz jutni [4].

DIGITÁLIS TÁMADÁSOK TÍPUSAI

A leggyakoribb esetek a *ransomware*, azaz a zsarolóprogramok általi támadások, amelyek meggátolhatják a felhasználó hozzáférését az adataikhoz, zárolják a számítógépet, tulajdonképpen túszként tartják fogva a személyes fájljait. A támadók átveszik a számítógép feletti irányítást, és váltságdíjat követelnek a visszaállított hozzáférésért cserébe. A *ransomware* támadások elleni védekezés legfontosabb módja annak biztosítása, hogy minden eszköz és szoftvere folyamatosan naprakész és frissített legyen, folyamatosan készüljön biztonsági mentés, ne nyissanak meg a felhasználók automatikusan e-mail mellékleteket, valamint érdemes felhőszolgáltatásokat használni. A pénzintézetek fokozott veszélynek vannak kitéve e tekintetben, mivel a *ransomware* támadásokkal főleg olyan szervezeteket támadnak, akik érzékeny adatokat őriznek, és gyorsan tudnak váltságdíjat fizetni [5].

A *rootkit* eredetileg olyan eszközök gyűjtő elnevezése volt, amelyek lehetővé tették a rendszergazda szintű hozzáférést a számítógéphez vagy a hálózathoz. Manapság a *rootkit*-eket rosszindulatú szoftverekkel azonosítják, amelyek elrejtik a létezésüket az operációs rendszer és ezáltal a felhasználók elől. A támadó a *rootkit* telepítése után távolról képes lesz a gazdagépen a rendszerkonfigurációkat felülírni, valamint a fájlokon változásokat végrehajtani. Elsődleges céljuk az adathalászat [6].

Az adathalász támadások a támadási vektorok leggyakoribb típusai közé tartoznak, és ez lehet az egyik legnehezebben kezelhető támadási fajta, mivel az elsődleges célpont a képzetlen dolgozó, aki általában nem jártas az információ-technológiában. Az adathalász e-mailek legfőbb jellemzője, hogy pontosan úgy néznek ki, mintha ismert vagy megbízható cégtől érkeztek volna (például: banktól, vagy egy online áruháztól). Ezek az e-mailek azzal próbálnak a címzett bizalmába férkőzni, hogy valamilyen történetet mesélnek el, majd egy melléklet megnyitására, vagy egy linkre kattintásra biztatják a felhasználót. Előfordul, hogy azt állítják, a felhasználó adataival visszaélést vagy harmadik fél által bejelentkezési kísérletet észleletek, esetleg meg kell erősíteni személyes adatokat. Gyakori a nyereményhez jutás ígérete is [7].

Szolgáltatásmegtagadási támadások (*Distributed Denial of Service*, DDoS), az elosztott szolgáltatásmegtagadási támadások a webhely az informatikai rendszer kapacitásának határait feszegetik. Céljuk, hogy azok forgalmát megszakítsák a webhely túlterhelésével és működésképtelenné tételével. Ezeket a támadásokat jellemzően botnetek segítségével hajtják végre, amelyek arra szolgálnak, hogy a kérésekkel túlcsordulást hozzanak létre a webhelyen, melynek következtében a webhely leáll [8].

A gyenge vagy feltört felhasználónevek és jelszavak a biztonsági incidensek egyik fő okai, ezért a felhasználók számára egyértelmű útmutatásokra van szükség, mivel ők a vállalat leggyengébb láncszemei. 2018-ban fél milliárd személyes adatot sikerült hackereknek eltulajdonítania, ami az előző évhez képest 126 százalékkal több esetet jelentett [9]. Az elmúlt évtized öt legnagyobb adathalász eseménye (Yahoo, Alibaba, LinkedIn, Sina Weibo, Facebook) összesen közel 6 milliárd felhasználót érintett [10]. A probléma forrása az, hogy a felhasználóknak saját jelszavakat kell létrehozniuk, ezért nagy a valószínűsége, hogy nem fognak elég biztonságos jelszót kitalálni. Ennek oka az lehet, hogy a felhasználók könnyen megjegyezhető jelszót szeretnének, nem ismerik a bevált jelszóbiztonsági gyakorlatokat, vagy olyan mintákat használnak jelszavaik létrehozásához, mint például a nevüket és/vagy a születési dátumukat [9]. Látható, hogy az alapképzés sem készíti fel a hallgatókat a megfelelő jelszóhasználati szokások kialakítására, ezért mindenképp erre is hangsúlyt kell fektetni – már az oktatás során [11]. Az információbiztonsági oktatásnál is új didaktikai elemre van szükség a jelszóhasználati szokások megváltoztatására, például jelszófejtő programok használata által, ahol a résztvevők megtapasztalhatják a gyenge jelszavak feltörésén keresztül, mennyire rövid idő szükséges azok megfejtéséhez [12] [13].

A bennfentes fenyegetések többféle formában és mértékben fordulhatnak elő. Kiváltó oka lehet pusztán hanyagság, de eredhet bosszúból és rosszindulatból egyaránt. A gondatlanságra jó példa, amikor szenzitív adatokat küldenek véletlenül az arra jogosulatlan felhasználónak, míg rosszindulatú szándék amikor valaki szándékosan, károkozás céljából ad át információkat, vagy kifejezetten anyagi haszonszerzés céljából pénzért. Felmérések szerint a károk 62%-a származik a munkavállalók vagy beszállítók gondatlansága miatt. E támadások mérséklésének egyik módja az, hogy a pontos hozzáférési szinteket biztosítja a felhasználóknak, amelyre a feladatuk ellátásához szükségük van, semmivel sem többet [14].

Harmadik fél szállítók megbízott vállalkozások sok szervezet számára rugalmasságot és nagyobb termelékenységet tesznek lehetővé. De a külső beszállítók kiberbiztonsági helyzetét éppoly komolyan kell venni, mint a sajátot. Harmadik féltől származó adatvédelmi incidensek száma rohamosan növekszik, és mivel egy kutatás szerint a szervezetek több mint 36 százaléka azt állítja, hogy legalább egy harmadik fél által okozott adatvédelmi incidenst átélt, egyértelmű, hogy miért van szükség átfogó, harmadik fél kockázatkezelési programjára [15].

Megfelelő titkosítás nélkül a szervezetek támadások áldozataivá válhatnak, mivel az adatok különböző hálózatokon keresztül kerülnek továbbításra. Amikor a felhasználók kockázatnak kitett hálózatokhoz vagy alkalmazásokhoz csatlakoznak, megnő annak a valószínűsége, hogy az érzékeny információk nyilvánosságra kerülnek egy adatvédelmi incidens során. Proaktív és megelőző intézkedéseket kell hozni annak biztosítására, hogy minden adat biztonságban legyen a felhasználók és az alkalmazások közötti mozgás során. Az adatokat nem csak továbbítás közben, hanem nyugalmi állapotban (tárolás) és az adattal való munka (feldolgozás) közben is titkosítani kell.

A hibás konfiguráció könnyű lehetőségeket teremthet a hackerek számára a sebezhetőségek kihasználására. Az ez ellen való védekezés kulcsa, hogy folyamatosan figyelemmel kell kísérni a szervezet „kiber-higiéniáját", így biztosíthatja, hogy az alkalmazások és eszközök beállításai naprakészek legyenek az iparági szabványoknak és a legjobb gyakorlatoknak megfelelően [16].

FIZIKAI TÁMADÁSOK TÍPUSAI

A fizikai támadások alkalmával a támadó személyesen jelenik meg és avatkozik be az adatok megszerzésének érdekében. Ennél fogva igen komoly előzetes felkészülést, színjátszó képességet és nem utolsó sorban hidegvért igényel a támadó részéről.

Az első lépés ilyenkor, hogy a támadó tervet dolgoz ki az adott objektumba való észrevétlen bejutáshoz. A besurranáshoz felhasználhatja más dolgozó adatait, vagy megpróbálja elhitetni a biztonsági őrrel, hogy otthon hagyta a beléptető kártyáját, vagy keresi a táskája alján, miközben nagy csomagokkal egyensúlyoz. Az ilyen esetekben a segítség nyújtás iránti hajlandóságát igyekszik kihasználni. A bejutás másik bevett módszere, hogy karbantartó munkásként jelenik meg, vagy ilyen csoporthoz csatlakozva surran be munkásruhában. Ezek a módszerek *piggybacking* és *tailgating* néven váltak ismertté [17].

Előfordul olyan eset is, amikor a támadó öltönyben vendégként érkezik egy vállalathoz, és a dolgozók válla fölött átkukucskálva próbál megfigyelni felhasználó neveket és jelszavakat, ezt hívják *shoulder surfing*-nek [18].

Sok támadó kukabúvárként tevékenykedik, vagyis konkrétan a hulladékot nézi át. A szemét sok olyan kidobott levelet is tartalmazhat, amelyekből személyes információkhoz juthat a támadó. Ezért fontos az irodákban iratmegsemmisítőt használni, de mindemellett a dolgozókat is figyelmeztetni kell, az iratkezelési szabályzatok betartására, valamint otthonaikban se dobjanak ki olyan iratokat, számlákat, amelyekből profilt alkothat róluk egy kiberbűnöző [19].

COVID-19-CEL KAPCSOLATOS VÁLTOZÁSOK

A kibertámadások száma és intenzitása minden iparágban folyamatosan növekedett az elmúlt években. Bár egyes kutatók hangsúlyozzák, hogy 2020 óta a támadások növekedése még mindig csak az általános növekvő tendencia része, hajlamosak vagyunk elfogadni, hogy a globális világjárvány miatt a minta megváltozott. Tapasztalatunk és egyre több kutatás is azt bizonyítja, hogy a lezárások miatt a cégeknek át kellett térniük a távmunkára, ezáltal új támadási felületek nyíltak meg. A támadások száma és intenzitása az otthoni vagy távoli elérésű informatikai és internetes infrastruktúra gyengesége miatt tovább emelkedett. A Verizon jelentése szerint például az adathalász támadások gyakorisága 2021-ben 25 százalékról 36 százalékra nőtt, elsősorban a globális kijárási korlátozások miatt növekvő otthoni megrendelések miatt [20].

BLOCKCHAIN NYÚJTOTTA LEHETŐSÉGEK

A pénzügyi ágazat számára a legnagyobb kihívást a jelentős mértékű papírmunka, a veszélyes adatszivárgás és a redundáns folyamatok jelentik, ezek azok a kihívások, amelyek tovább növelik az amúgy is hatalmas működési költségeket és a növelik a fogyasztók bizalmának hiányát. A blokklánc alkalmazása a pénzügyi szolgáltatásokban sokat segíthetne ezeknek a problémáknak a kiküszöbölésében. A blokklánc eddig nem látott biztonságot és átláthatóságot hozhatna a pénzügyi szektorba. A technológia decentralizált, és egy-egy tranzakció hitelesítését több csomóponton végzik, ezért nem módosítható. Mivel minden csomóponton ugyanazok, az adatok fognak szerepelni, ez biztosítja, hogy az adatok visszakövethetőek, biztonságosak és hitelesek maradhatnak. Ugyanakkor adatvédelemi szempontból is megfelelő lehet, mivel a rendszer használatához egy nyilvános és egy privát

kulcsra van szükség a hálózathoz való hozzáférés biztonságának és az egyéni tranzakcióinak titkosságának megőrzése érdekében. Így a pénzintézetek az adatokhoz való hozzáférés nélkül is elvégezhetik a felhasználó-ellenőrzést az adat ellenőrzése el tud válni az adattól magától csökkentve ezzel a jogsértések esélyét [21].

Blokklánc segítségével hatékonyabban lehetne ellenőrizni a pénzügyi tranzakciókat. Mivel a blokkláncon lévő rekordok megváltoztathatatlanok, az auditorok ellenőrizhetik, hogy megfelelnek-e a valóságnak. Egy átlagos pénzügyi elszámolás több oda-vissza váltást foglal magában a bank *front-* és *back office*-a között. Az intelligens szerződések használatával elkerülhetőek ezek a lépések, megkönnyítik a P2P (*peer to peer*) tranzakciókat, és kihagyhatnak több lépcsőfokot a pénzügyi elszámolás felgyorsítása érdekében. A blokklánc közvetítők nélkül képes azonnali, határokon átnyúló fizetéseket is kezelni [21].

A Blockchain technológia használata segíthet a fenti kiberkockázatok egy részének csökkentésében. A legtöbb pénzintézet már vizsgálja a technológiában rejlő lehetőségeket. A technológia alapját adó funkciók, mint az elosztott főkönyvi technológia, nagyon jó kiindulási pont a kibertámadások elleni védekezésben. A különböző pénzügyi intézmények a blokklánc technológiát használják vagy tesztelik tőzsdei kereskedéshez, kereskedelem finanszírozáshoz, hűségprogramokhoz, ahogy korábban írtuk kísérleteznek a technológia felhasználásával a P2P kifizetések és a nemzetközi fizetések elszámolásában [22] [21] [23].

ÖSSZEFOGLALÁS

A cikkben bemutattuk a kritikus támadási pontokat és megnéztük a támadások okait. Összességében elmondhatjuk, hogy a gazdaság különböző szektorait, azon belül a pénzügyi szektort kiemelten, évről évre növekvő mértékben érintik a kibertámadások különböző módszerei. A digitális támadások mellett továbbra sem hanyagolhatjuk el a fizikai támadások jelentőségét. Azt is megállapítottuk, hogy az adatszivárgás kiemelkedő oka továbbra is az emberi tényező: a belső kolléga vagy külső beszállító gondatlansága, nem megfelelő jelszókezelése vagy szélsőséges esetben kifejezetten a rosszindulatú szándéka.

A cikkben vizsgált kibertámadások fő tanulságai összefoglalva:

1. Egyetlen szervezet vagy hálózat sem biztonságos: mérettől vagy az iparágtól függetlenül a cégek nincsenek biztonságban a kibertámadásoktól.
2. Üzletmenet folytonossági programokra, védelmi és biztonsági protokollokra vagy az ügyfélkommunikációra nagyon nagy hangsúlyt kell fektetni: a szervezeteknek elő kell készíteniük a megfelelő szabályzatokat. A szabályzatoknak harmadik feles szolgáltatókra és más szállítókra is vonatkozniuk kell.
3. Fizetni vagy nem fizetni: a szakemberek általában nem javasolják a váltságdíjak kifizetését. Precedenst teremt, felhívja a többi kiberbűnöző figyelmét, hogy az adott szervezet hajlandó fizetni
4. A támadások időzítettek és célzottak: az értékes felhasználói adatok, az áldozat fizetési potenciálja kulcsfontosságú tényezők. Sokszor egy támadást hónapokkal megelőzően már el lettek rejtve a jövőben támadáshoz a bejutást biztosító „trójai falovak”.
5. A kibertámadások akkor a legkártékonyabbak, ha hatással vannak az ügyfelekre: az üzleti működés elleni támadások akkor a leghatásosabbak, ha közvetlenül érintik, megzavarják az ügyfelek működését.

6. Az emberi tűzfal a védelem első vonala: az emberi hiba még mindig a legfontosabb kiberbiztonsági tényező [5] [8] [24] [25] [26].

A pénzügyi szektor esetében kiemelten fontos tényező, hogy a legtöbbször szenzitív adatokat kezelnek. Bár a blokklánc technológia tömeges elterjedése még várat magára, de megfelelő keretek között ez a technológia megoldást nyújthat a kibervédelem bizonyos kihívásaira. Jövőbeni új lehetőség lehet például a dolgok Internetje (*Internet of Things*, IoT) és a blokklánc technológia összekötésével a banki finanszírozás mögötti biztosítékok értékének valós idejű monitorozása is lehetővé válik.

FELHASZNÁLT IRODALOM

[1] M. Henriquez, „Security Magazine," 9 12 2021. [Online]. Available: https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021. [Hozzáférés dátuma: 16 12 2021].

[2] M. Henriquez, „Security Magazin," Reserved BNP Media, 20 10 2021. [Online]. Available: https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021. [Hozzáférés dátuma: 05 12 2021].

[3] P. Dr. Michelberger, Információ-, folyamat- és vállalatbiztonság, Budapest: ÓE-KGK-4086, ISBN 978-963-449-201-8, 2020.

[4] S. Scorecard, „Security Scorecard," Security Scorecard , 25 01 2021. [Online]. Available: https://securityscorecard.com/blog/what-is-an-attack-vector-common-examples. [Hozzáférés dátuma: 05 12 2021].

[5] A. G. Johansen, „Norton," NortonLifeLock, 23 11 2021. [Online]. Available: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html. [Hozzáférés dátuma: 12 12 2021].

[6] Kaspersky, „What is Rootkit – Definition and Explanation," Kaspersky, na na 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit. [Hozzáférés dátuma: 07 12 2021].

[7] KnowBe4, „Phishing," KnowBe4, [Online]. Available: https://www.phishing.org/what-is-phishing. [Hozzáférés dátuma: 12 12 2021].

[8] R. KARTCH, „Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response," Carnegie Mellon University, 21 11 2016. [Online]. Available: https://insights.sei.cmu.edu/blog/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response/. [Hozzáférés dátuma: 10 12 2021].

[9] C. D. Defense, „6 Password Security Risks and How to Avoid Them," Cypress Data Defense, 15 06 2020. [Online]. Available: https://www.cypressdatadefense.com/blog/password-security-risks/. [Hozzáférés dátuma: 08 12 2021].

[10] D. S. Michael Hill, „CSO, IDG Tech Media GmbH," 16 07 2021. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Hozzáférés dátuma: 16 12 2021].

[11] G. Kiss, „The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education," SHS WEB OF CONFERENCES (2261-2424): 66 Paper 01042. 7 p., 2019.

[12] A. Szász, G. Kiss, „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra," INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT (1587-8694): 18 3-4 pp 82-104, 2018.

[13] A. Szász, G. Kiss, „Multimedia password retrieval programs in information security education," JOURNAL OF APPLIED MULTIMEDIA (1789-6967 1789-6967): 13 3 pp 87-96 Paper JAM.2018.3.002., 2018.
[14] Digitrend, „Kiberbiztonság: a leggyengébb láncszem a munkavállaló," Digitrend, 27 02 2020. [Online]. Available: https://digitrendi.hu/kiberbiztonsag-a-leggyengebb-lancszem-a-munkavallalo/. [Hozzáférés dátuma: 05 12 2021].
[15] E. global, „Building trust with your third parties in a technology-driven and disruptive world," EY third-party risk management, 2020. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-trpm-survey-2019-20-update-final.pdf. [Hozzáférés dátuma: 17 12 2021].
[16] C. Brook, „Digital Guardian," 6 10 2020. [Online]. Available: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more. [Hozzáférés dátuma: 17 12 2021].
[17] K. T. P. Ltd., „Tailgating Attack: A Physical Social Engineering Crime," Kratikal Tech Pvt. Ltd., 20 04 2020. [Online]. Available: https://kratikal.medium.com/tailgating-attack-a-physical-social-engineering-crime-f63da4195536. [Hozzáférés dátuma: 10 12 2021].
[18] T. I. Team, „What is shoulder surfing?," Business Tech , 07 05 2021. [Online]. Available: https://www.businesstechweekly.com/cybersecurity/password-security/what-is-shoulder-surfing/. [Hozzáférés dátuma: 05 12 2021].
[19] G. Wright, „Tech Target," 04 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/dumpster-diving. [Hozzáférés dátuma: 17 12 2021].
[20] Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup, 2021 Data Breach Investigations Report, Verizon, 2021.
[21] E. Learning, „Esme Learning," Esme Learning, 24 08 2021. [Online]. Available: https://esmelearning.com/blogs/news/blockchain-solving-financial-sector-problems. [Hozzáférés dátuma: 05 12 2021].
[22] D. Sinha, „Analytics Insight," 07 07 2021. [Online]. Available: https://www.analyticsinsight.net/blockchain-technology-disrupting-banking-sector-worldwide-in-2021/. [Hozzáférés dátuma: 22 02 2022].
[23] Mariano Belinky, Emmet Rennick, Andrew Veitch, „The Fintech 2.0 Paper: rebooting financial services," 2015. [Online]. Available: https://www.oliverwyman.com/our-expertise/insights/2015/jun/the-fintech-2-0-paper.html. [Hozzáférés dátuma: 01 02 2022].
[24] Ronald D. Lee, Michael A. Mancusi, Amber A. Hay, Anthony Raglani, „Arnold&Porter," 11 06 2021. [Online]. Available: https://www.arnoldporter.com/en/perspectives/publications/2021/06/lessons-learned-from-the-solarwinds-cyberattack. [Hozzáférés dátuma: 26 01 2022].
[25] J. p. M. Jr., „TechBeacon," 2020. [Online]. Available: https://techbeacon.com/security/8-lessons-garmin-ransomware-attack. [Hozzáférés dátuma: 26 01 2022].
[26] M. H. ("Heff"), „SecurityMetrics," [Online]. Available: https://www.securitymetrics.com/blog/garmin-ransomware-attack-soc-threat-analysis-and-10-lessons-learned. [Hozzáférés dátuma: 26 01 2022].

THE FUTURE OF EIDAS IN THE LIGHT OF POST-QUANTUM CRYPTOGRAPHY

AZ EIDAS JÖVŐJE A POSZT-KVANTUM KRIPTOGRÁFIA TÜKRÉBEN

NYÁRI Norbert[1]

Abstract

This paper examines the challenges and future of digital signatures, which are widespread today, and the electronic signatures based on them. Several electronic signature schemes have been defined worldwide; the European version is governed by the eIDAS Regulation. Electronic signatures based on public key cryptography currently in use will be compromised by high-performance quantum computers. In my article, the basic operation of electronic signatures is presented, and vulnerable points are identified. I shall furthermore cover the various recommendations to help the transition to the post-quantum era, NIST, ENISA, etc., which provide guidance on how to strengthen systems that are still operating in production environments against quantum attacks as long as standardized, quantum-safe public-key cryptographic primitives are on the way.

Keywords

digital signature, electronic signature, cryptography, post quantum cryptography, IT security

Absztrakt

Jelen cikk a manapság széleskörben elterjedt digitális aláírások, és az azokra épülő, joghatást is kiváltó elektronikus aláírások várható kihívásait és jövőjét vizsgálja. Világszerte több elektronikus aláírási sémát definiáltak, az Európai változatot az eIDAS rendelet szabályozza. A jelenleg alkalmazott nyilvános kulcsú rejtjelezésre épülő elektronikus aláírásokat kompromittálni fogják a nagyteljesítményű kvantumszámítógépek. Cikkemben bemutatásra kerül az elektronikus aláírások alapvető működése, azonosításra kerülnek a sebezhető pontok. Kitérek továbbá a különböző ajánlásokra, amelyek a poszt-kvantum érába való áttérést hivatottak segíteni, a NIST, ENISA stb, melyek irányt mutatnak, hogy hogyan erősíthetők meg a jelenleg is éles környezetben működő rendszerek a kvantum támadásokkal szemben addig, ameddig nem áll rendelkezésünkre szabványosított, kvantumbiztos nyílt kulcsú kriptográfiai primitív.

Kulcsszavak

digitális aláírás, elektronikus aláírás, kriptográfia, posztkvantum kriptográfia, informatikai biztonság

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

INTRODUCTION

This paper examines the expected challenges of the now widespread public-key cryptographic technologies for digital signatures. The trust services and the various electronic signatures defined in the eIDAS framework adopted throughout the EU are based on the above-mentioned public-key cryptographic (PKC) primitives. Large-scale quantum computers with adequate computational capacity shall, over time, compromise all public-key cryptographic algorithms (RSA, DSA, Diffie-Hellman Key Exchange etc.) currently used in production environments.

The so-called quantum apocalypse shall have a great impact on eIDAS and thus the European trust services and electronic signatures as well. Not only that no more secure certificates can be issued, and no more documents can be signed in a secure manner but also already signed documents with today's technologies shall be easily tampered with seriously violating Confidentiality and Integrity IT security principles.

Fortunately, the future does not have to be that dark. Large companies researching quantum computing report new results every year (e.g., the IBM 127-qubit quantum computer November, 2021 [1]), but we still have time until universal quantum supremacy is achieved, notwithstanding, in my humble opinion the time available needs to be spent on conscious preparation and gradual migration. Thankfully, many guides and articles can be of help: security guides proposing methods and techniques for strengthening production systems (and PKI certificates).

Besides, in the meantime mathematicians, cryptographers and other scientists are trying to find new, secure, quantum-proof approaches in cryptography and in parallel, standardization institutes around the world working on new, quantum-safe standards for PKC and digital signatures.

Stressing the difference between "Electronic signature" and "digital signature" is vital. While digital signature is technical phrase including various encryption and hash algorithms, electronic signature is a legal concept, with many different interpretations and implementations. As for implementation, the most basic scenario is a simple name written on the end of an electronic document. An electronic signature can also be a legal application of digital signature technology, making electronic signature a special use case of digital signature. Let us get into the details of electronic signature.

ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE

The concept of electronic signature has a bit of a history: signatures transmitted by telegraph have existed and recognized by law since the mid-19th century. Faxed signatures have also been accepted since the 1980s. [2] In my personal experience I find that nowadays printed, hand-signed and then scanned or photographed electronic documents/filled forms sent in e-mail is accepted by many institutions. No wonder, as it is quite similar to the aforementioned and previously widely accepted fax signature. In my humble opinion this kind of electronic signature can be enough for everyday administration tasks of lesser importance.

In recent decades, various laws have been enacted around the world to create the legal basis for the use of electronic signatures in national and international trade, so there are many different definitions.

First of all, the United States has multiple federal and state laws regarding electronic signature. On one hand, in 2000, "Electronic Signatures in Global and National Commerce Act" (ESIGN Act) Sec 106 (US federal law) defined a quite basic electronic signature as follows "The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.", stating nothing on authentication, verifiability, or non-repudiation. [3]

On the other hand, in "Government Paperwork Elimination Act" (GPEA) Sec 1710 (US federal law) the term "electronic signature" means "a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message; and indicates such person's approval of the information contained in the electronic message." [4]

In Canada "Personal Information Protection and Electronic Documents Act" (PIPEDA) regulates the use of electronic signatures. It distinguishes between two different types of electronic signatures: "electronic signature" and "secure electronic signature". An electronic signature is a "signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to, or associated with an electronic document.". The other type, secure electronic signature is special kind of electronic signature, "that results from the application of a technology or process prescribed by regulations made" having a few restrictions: it has to be unique to the signatory, it has to provide mechanics for verifying the signature, and changes made to the signed document since the signature creation must be detectable. [5]

eIDAS ("electronic IDentification, Authentication, and trust Services") is the EU regulation "on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", taken effect in 2016. One main goal of the regulation is supporting the Digital Single Market (DSM) for EU member states. [6]

The "Digital Single Market Strategy" is one of the European Commission's top ten priorities for creating an ecosystem that supports consumers and businesses in e-commerce across Europe using common solutions. [7]

The regulation thus also facilitates the transparent, secure, technology-neutral and trouble-free flow of commerce in the EU. eIDAS applies across borders as well as within individual member countries standardizing the use of electronic identification (eID), defining the "electronic trust services" (eTS), ensuring the legal validity of electronic signatures. As a result of consistent, Europe-wide regulations electronic trust services can be accessed through an internal market in the EU. [8] [6]

From now on I shall focus on the electronic signature model defined in eIDAS. Trust services are out of the scope of the current paper.

There are three kinds of electronic signatures defined by eIDAS: Electronic Signature (formerly known as Simple Electronic Signature), Advanced Electronic Signature (AES – not to be confused with Advanced Encryption Standard which a cryptographic algorithm), and Qualified Electronic Signature (QES). [6]

Electronic signature "means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign". According to eIDAS the even most basic form of electronic signatures e.g., a simple name

typed as text at the end of an electronic document, can be accepted as valid, since "an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures." [6]

An "Advanced Electronic Signature" in eIDAS has the same properties as the "secure electronic signature" in the Canadian PIPEDA, that is it must be one-to-one mapped to the signer. One must be able to identify the signer of a document based on the signature. Moreover, further changes on the signed document after the creation of the signature has to be detectable. [6]

"Qualified Electronic Signature" is a special type of "advanced electronic signature" having the same legal effect of a handwritten signature. It has to be created with a "qualified electronic signature creation device" using a qualified certificate for electronic signatures. [6]

A qualified certificate "means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in" the Regulation. A few examples of the set of requirements defined: an indication that the certificate is a qualified certificate for electronic signature, data clearly identifying the issuer (including the Member State). In the case of a natural person, the data must include the name of the person and, in the case of a legal person, the registration number in addition to the name. [6]

eIDAS differentiates between advanced electronic signatures and advanced electronic stamps, the main difference is that the former is issued for a person, the latter is for a legal person. Technologically, at the end of the day, both are based on digital signature algorithms. [6]

Another important concept is electronic timestamp, according to the regulation it "means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time". There are two levels of timestamps, electronic timestamp, and qualified electronic timestamp. A qualified electronic time stamp is "an electronic time stamp which meets the requirements laid down in" the Regulation. [6]

Similarly to basic electronic signatures an electronic time stamp "shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp". In contrast a qualified electronic time stamp shall meet certain requirements: exact time must come from a reliable time source connected to UTC. Date and time data must be signed or sealed with an eIDAS conform advanced electronic signature or seal excluding the possibility of undetected modification. [6]

Although the main concepts are technology-independent, eIDAS stresses the need to create a pan-European public key infrastructure and mentions certificates several times, which means public key certificates (or in other words digital certificates). [6] This also shows that coming across close technical ties at implementation level is inevitable.

From a technical aspect a qualified electronic signature is nothing else than a digital signature created with a public key (digital) certificate. Let us take a closer look on how a digital signature is made.

The high-level requirements of digital signatures are the following according to Tannenbaum:

- authentication: the receiver must be able to check the alleged identity of the sender,
- non-repudiation: the sender cannot later repudiate the contents of the message,
- integrity: the receiver (or anybody else) cannot possibly counterfeit the message in the name of the original sender. [9]

Any public key cryptographic (PKC) primitive meets the above requirements, but the de facto standard is the RSA (Rivest-Shamir-Adleman) public key algorithm. A quick recap: in PKC every participant has a keypair, which consist of a private key and a public key. While the private key is prohibited from being disclosed to others and must only be used by the owner, the public key can be securely transmitted to anyone. [9]

If the public key of a keypair is used for encryption, only the private key can be used for decryption and vice versa. The use cases of the keys can be summarized as follows:

Key	Cryptographic operation	Usecase	Abridgment
Public	Encryption	Encrypt message	public-encrypt
Private	Decryption	Decrypt message	private-decrypt
Private	Encryption	Sign a message	private-encrypt
Public	Decryption	Verify a signature	public-decrypt

1. Table Usecases of keys of a keypair

Another vital cryptographic primitive is also used in the creation of digital signatures: a cryptographic hash function, which calculates a message digest (or hash) of fixed length for input data of any size. [9]

Historically in cryptographic examples the sender, the receiver, and the attacker are named respectively Alice, Bob, and Eve. I shall stick to this nomenclature in the following, where I present the basics of digital signature. [9]

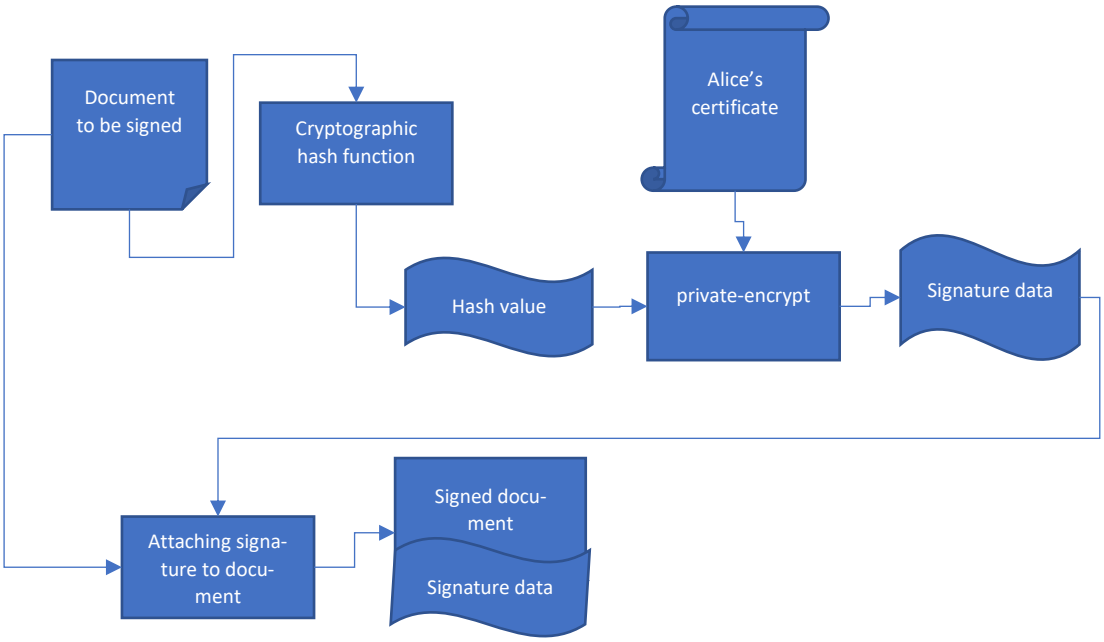
Consider a scenario where Alice wants to create and send a digitally signed document to Bob, with the above-mentioned requirements in place, making sure that Eve would not be able to alter the original document.

Firstly, the hash of the document is calculated with a cryptographic hash function. The hash value is encrypted with Alice's private key, which is stored in Alice's certificate. The singed document then created by attaching the signature data to the original document. [9]

The validity of the signature can be verified by anyone, who holds Alice's certificate (excluding the private key of course). The verification is basically the public-decryption of the signature data, after that the hash of the document is calculated with the same algorithm that of the signer used, and finally the two hashes (the one form the signature data, and the calculated one) are compared.

So, how does electronic signatures implement Confidentiality and Integrity? Should the two above hashes match, Bob can be certain that Alice signed the message (identification of the signatory). PKC guarantees that Alice's private key was used for encryption of the document hash if decryption of the signature data with Alice's public key results in the correct has (non-repudiation). The match of the two hashes guarantees that no modification was made on the original document (integrity).

This is however the most basic scenario with limitations. The signature can only be validated till the signer's certificate is valid (not expired, not revoked).



1. Figure Creation of a basic digital signature

The ETSI EN 319 102-1 V1.3.1 (2021-11) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" European Standard defines how the advanced electronic signature (AdES – AES is the legal concept, AdES is the technical implementation) is to be created and verified in accordance with the eIDAS regulation. AdES however heavily relies on PKC. [10]

Practically speaking ETSI EN 319 102-1 standard supports the eIDAS Regulation for creation of electronic signatures and seals implemented using digital signature technology. [10]

The standard defines four levels of electronic signatures, each level includes the level below itself signing the lower layers' unsigned attributes:

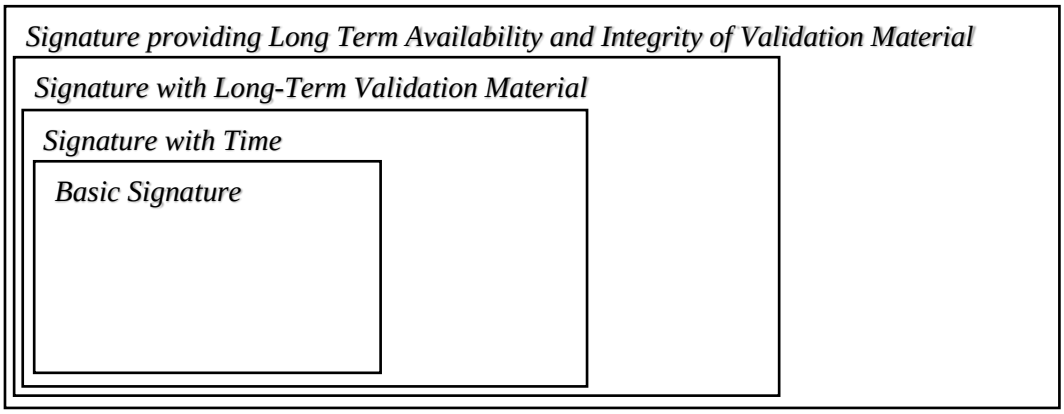
- *Basic Signature*: "is a signature that can be validated as long as the corresponding certificates are neither revoked nor expired."
- *Signature with Time*: "is a signature that proves that the signature already existed at a given point in time."
- *Signature with Long-Term Validation Material*: "is a signature that provides the long-term availability of the validation material by incorporating all the material or references to material required for validating the signature"

- *Signature providing Long Term Availability and Integrity of Validation Material*: "targets long term availability and integrity of the validation material of digital signatures over long term and can help to validate the signature beyond many events that limit its validity (for instance, the weakness of used cryptographic algorithms, or expiration of validation data)." [10]

The types of signatures above fundamentally differ in the number of attributes attached to the signature. The Basic Signature is very similar in essence to the procedure I have presented above. It consists of the signers document, the signing certificate and the signature value. [10]

Signature with Time encapsulates a Time Stamp Token (TST) as an unsigned attribute requested from a Time Stamping Authority (TSA), both defined in RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". This type can be validated as long as the required validation data is on-line available to the verifiers. It is intended to prove the existence of the signature at a given point in time. [10] [11] [12] TSP also relies on PKC being another potential subject to quantum attacks.

Signatures created with Long-Term Validation Material, in contrast, includes the validation data that is necessary for verification beyond the end of the validity of the signing certificate. The "necessary data" is attached as unsigned properties containing the complete certificate (chain of trust) and revocation data. [10] [12]



2. Figure Embedding of different signature types

Signature providing Long Term Availability and Integrity of Validation Material, as its name suggests, targets creating signatures that can be validated long after creation. Built from the previous level, a time stamp token is added on the validation data from the previous level, proving that the validation data existed at a given point of time. [12]

Used in conjunction with appropriate additional measures this kind of signature can be verified long after creation even if the applied cryptographic algorithms were compromised in the meantime. This can be achieved utilizing periodical timestamping which is practically the re-signing of validation data with up-to-date cryptographic primitives. [12] [10]

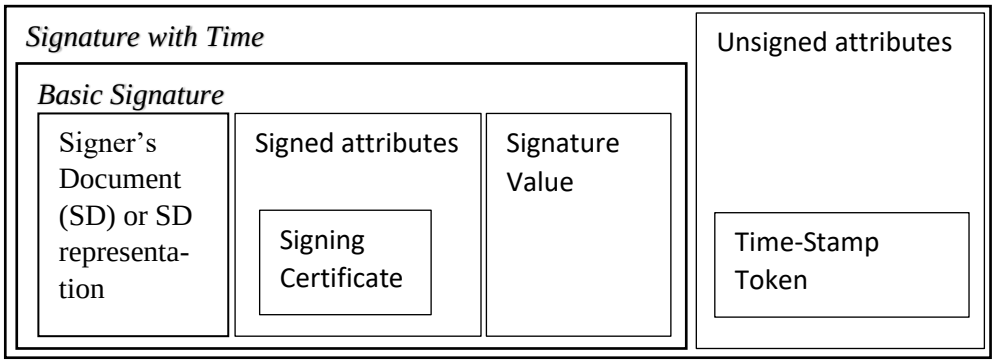
However, in order to make my point in this paper the 'Signature with Time' type of electronic signatures is sufficient to know in detail.

The Signature with Time utilizes the aforementioned Time-Stamp Protocol. With a signed time-stamp token attached to a Basic Signature shortly after signing, this level provides evidence of the existence of the signature at a given point in time. [10]

The Time-Stamp Token is provided by a Trust Service Provider, with the responsibility of proving the validity of the time-stamp when required to do so. [10] Requesting a time-stamp is done in the following way: the requesting entity sends a request (TimeStampReq) to the Time Stamping Authority, which responds with a Time stamp response (TimeStampResp) including a TimeStampToken (TST). Each TST is signed by the TSA with a certificate generated exclusively for this purpose. The validity of a time-stamp can be verified with the public key certificate of the TSA. [11]

A time-stamp token should ideally be created and attached to the signature right away. The sooner the timestamp is attached to the signed document, the lower the risk of repudiation of the signature creation. In certain cases, it is advisable for the verifier to create a Signature with Time on a newly received document: the signer does not provide a Time-stamp token, or the verifier does not trust the provided Time-stamp token. [10]

The logical structure of the signature type is shown in the figure below.



3. Figure Signature with Time

Signature with time consists of a Basic signature and a timestamp signed by a TSA. Let us move on to the threats and challenges regarding to digital signatures.

THREATS FROM QUANTUM COMPUTING

This section is a brief review of what has been discussed in detail regarding the threats posed to today's cryptography by quantum computing in my previous article on the topic, "The Impact of Quantum Computing on IT Security".

Today's PKC is based on mathematical problems that cannot be solved in normal time, such as the factorization problem of integers, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. These problems however can be solved in feasible time on a quantum computer capable of running Shor's prime factor finding algorithm. Increasing the key size in this case shall unfortunately be of no help, new, quantum-safe public-key algorithms must be found and utilized. [13]

Quantum searching algorithms give a quadratic speed up to Known Plaintext Attacks (KPA) against Symmetric Key Cryptographic (SKC) algorithms. Quantum-safeness

can be provided increasing the key size, as a rule of thumb doubling the key size would be enough. [14]

Quantum attacks can potentially accelerate the breaking of cryptographic hash functions. The resistance to such attacks can be increased in a similar way as in the case of SKC, the output length of hash functions needs to be increased. [14]

Practically speaking large-scale quantum computers shall compromise today's PKC and halve the security of SKC and hash functions.

eIDAS qualified electronic signatures are built around public key cryptography, large scale quantum computers shall probably cause many problems in the application of electronic signatures. As stated, before an electronic signature is used to ensure the integrity and non-repudiation of signed documents.

I think that should the quantum apocalypse occur, soon after that quantum cryptographic algorithms shall probably be developed and implemented running on quantum computers. So, the problem of the signature creation shall be solved soon after the quantum apocalypse.

The main problem however arises with previously signed documents: in theory, an attacker using a large-scale quantum computer can easily tamper with the signature data, timestamps and validation material of any signature created with today's technology. So, basically any electronically signed document can be counterfeited.

The above detailed Signature with Time scheme (and so the other schemes as well) could be compromised in many ways. Suppose the attacker has a large-scale, universal quantum computer, being able to counterfeit the signature data, in violation of the Confidentiality and Integrity of the original document. The attacker could create a new version of the document that was apparently signed by the original signer at the original point in time, but with a different content.

In my opinion, because of the technology dependencies of electronic signatures on public-key cryptography, the review and revision of the cryptographic requirements of the regulation should also start in time to ensure a smooth transition into the post-quantum era.

WHAT CAN BE DONE IN THE MEANTIME?

There are several guides in the topic issued by many nations' IT security or standardization organizations. Firstly, the NIST National Cybersecurity Center of Excellence (NCCoE) started a program to develop methods and best practices regarding migration from today's PKC to quantum-safe replacement algorithms, complementing the NIST PQC project. [15] [13]

The paper aims to provide help in discovering quantum-vulnerable cryptographic modules (hardware or software) in cryptosystems, demonstrating through five scenarios listed in the table below. [15]

#	**Title**
Scenario 1	"FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography"
Scenario 2	"Cryptographic libraries that include quantum-vulnerable public-key cryptograpy"
Scenario 3	"Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography"
Scenario 4	"Embedded quantum-vulnerable cryptographic code in computing platforms"

Scenario 5	"Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms"

2. Table Migration to Post-Quantum Cryptography Scenarios

Basically, the possibly quantum-vulnerable components of production cryptosystems should be identified and replaced with quantum-safe alternatives. Replacing them however is not always so straightforward, because the classical primitives are not interchangeable as is with new primitives due to differences in key size, signature size, performance etc. [15]

The first paper in the project, Getting Ready for Post-Quantum Cryptography was originally released on May 26th, 2020, the latest version is dated April 28th, 2021. Not only it describes the possible impact of quantum computing on today's cryptography especially public-key cryptography but introduces the expected challenges of migration to post-quantum cryptography, and post-quantum cryptography itself. [15]

The paper emphasizes the very important concept of "crypto agility", stating that unfortunately many cryptosystems lack this feature. Practically speaking "crypto agility" is the openness of cryptographic systems to rapid replacement of cryptographic primitives. [16]

My understanding is that crypto agility is a vital concept and should be treated as a design pattern in the design of cryptosystems, that is, the possibility that the embedded cryptographic primitives shall become compromised in time making it necessary to replace them, should be considered.

We will have to wait for the end of NIST PQC standardization process for concrete recommendations regarding public key cryptography.

The German Federal Cyber Security Authority (BSI - Bundesamt für Sicherheit in der Infromationstechnik) developed and released a set of recommendations in 2020 written in German. The paper "Migration zu Post-Quanten-Kryptografie" introduces the technological backround of the matter and describes the possible effects of quantum computing getting large-scale. The recommendations are focused around seven points including crypto agility, key sizes for symmetric cryptography, hybrid solutions, quantum-safe key encapsulation mechanisms (KEMs). [17]

The article also stresses out the importance of crypto agility like the above mentioned NIST guide. Furthermore it suggests that some caution should be exercised when applying quantum-safe algorithms, as these are relatively new solutions and their application has not yet had enough time to expose their shortcomings, so it is vital to apply them in combination with classic algorithms, that is hybrid solutions should be used. [17]

As for symmetric-algorithm key sizes it recommends the already mentioned doubling of key sizes with reference to the Grover search algorithm. The size of the keys for symmetric algorithms is even more important when the goal is to provide long-time security for encrypted data. [17]

The ENISA paper "Post-Quantum Cryptography: Current state and quantum mitigation", published on May 3rd, 2021, firstly gives a good technical background on post-quantum cryptography including the description of five main families of algorithms, reviews the NIST PQC project and the Round 3 finalists, and finally comes with two recommendations in the Quantum Mitigation section, in order to improve security against quantum attacks. [18]

One of the two proposals is, similarly to the German paper "Migration zu Post-Quanten-Kryptografie", is the usage of hybrid schemes of pre-quantum and post-quantum cryptographic primitives. The basic idea is to combine a traditional PKC algorithm like RSA with a post-quantum one, at least one of them being secure ensures the security of the cryptosystem. [18]

This scheme can be applied to either in the context of TLS (Transport Layer Security) or that of electronic signatures. The paper cites the article "Transitioning to a Quantum-Resistant Public Key Infrastructure". [18] The article states that X.509 certificates could be used in a hybrid manner in two different ways: Dual certificates, Second certificate in extension [19]

Dual certificates means that there would be two certificates created, since there is no option in X.509 for including more than one keys in a certificate, one for the classical public key algorithm and another one for the post-quantum one, implying that two signatures have to be created for every document, one for each algorithm. [19]

The other approach is the extension of X.509 standard with the possibility of including more keys in a certificate. However, problems arise as a result of the key sizes of the PQC algorithms. [19]

There was an attempt in standardizing the above concept of multiple key certificates in 2018, the IETF draft "Multiple Public-Key Algorithm X.509 Certificates draft -truskovsky-lamps-pq-hybrid-x509-01" proposed ways to embed alternate cryptographic materials in certificates in order to use multiple algorithms with one certificate. But unfortunately, the draft expired on March 2, 2019. [20] To the best of my knowledge, there is no standardized solution for this approach, but many organizations offer non-standard solutions for multiple-key X.509 certificates e.g., the Open Quantum Safe project or ISARA Corporation. [21] [22]

SUMMARY

Universal quantum supremacy is apparently on its way, and it is very difficult to estimate when it shall occur, but should it happen, it shall cause serious problems in cryptography. Companies operating IT systems and IT security professionals need to prepare for the occurrence of the so-called quantum apocalypse. Fortunately, the cryptographic community is working hard to replace quantum vulnerable cryptographic primitives.

In my humble opinion is vital to keep track of the development of quantum computing and post-quantum cryptography so that the necessary steps can be taken in time to maintain and enhance IT security.

In my opinion, the review of eIDAS regulation and the ETSI EN 319 102-1 V1.3.1 (2021-11) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" European standard from a post-quantum point of view is vital and should be done in time to ensure a smooth transition into the post-quantum era.

My understanding is that crypto agility is a vital concept, practitioners should design cryptosystems keeping in mind that the used primitives may become compromised in time making it necessary to replace them.

Transition to post-quantum cryptography is crucial but so as proceeding with caution. The use of hybrid schemes of pre-quantum and post-quantum cryptographic primitives

ensures that we do not fall victim to possible, yet unknown vulnerabilities of post-quantum primitives during the transition period.

RESOURCES

[1] P. Rincon, "IBM claims advance in quantum computing," 17 11 2021. [Online]. Available: https://www.bbc.com/news/science-environment-59320073. [Accessed 20 12 2021].

[2] Turner, Dawn. "What is a Digital Signature - What It Does, How It Works". Cryptomathic. https://www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works [Accessed 05 11 2021].

[3] "Electronic Signatures in Global and National Commerce Act," 30 06 2000. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf. [Accessed 05 11 2021].

[4] "GOVERNMENT PAPERWORK ELIMINATION ACT," 21 10 1998. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf. [Accessed 05 11 2021].

[5] "Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)," 20 10 2021. [Online]. Available: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html. [Accessed 05 11 2021].

[6] 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.

[7] European Economic and Social Committee, "The digital single market - trends and opportunities for SMEs (own-initiative opinion)," 18 09 2020. [Online]. Available: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-single-market-trends-and-opportunities-smes-own-initiative-opinion. [Accessed 05 11 2021].

[8] scrive, "eIDAS and the Digital Single Market," [Online]. Available: https://www.scrive.com/trust-center/eidas-summary/. [Accessed 05 11 2021].

[9] A. S. Tannenbaum, Computer Networks, New Jersey: Pearson Education, 2003.

[10] ETSI, "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation," 11 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf. [Accessed 11 11 2021].

[11] Adams, et al., "RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," 08 2001. [Online]. Available: https://www.ietf.org/rfc/rfc3161.txt. [Accessed 11 11 2021].

[12] W. Vercruysse, "What are the B-T-LT and LTA levels of an electronic signature," 18 12 2019. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/ESIGKB/What+are+the+B-T-LT+and+LTA+levels+of+an+electronic+signature. [Accessed 11 11 2021].

[13] N. Nyári, "The Impact of Quantum Computing on IT Security," Safety and Security Sciences Review, vol. 3, no. 4, pp. 25-37, 2021.

[14] S. Vogt and H. Funke, "How Quantum Computers threat security of PKIs and thus eIDs," 02 06 2021. [Online]. Available: https://dl.gi.de/bitstream/handle/20.500.12116/36504/proceedings-07.pdf?sequence=1&isAllowed=y. [Accessed 21 11 2021].
[15] NIST NCCoE, "Migration to Post-Quantum Cryptography," 08 2021. [Online]. Available: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms. [Accessed 21 11 2021].
[16] NIST, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," 28 04 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf. [Accessed 07 12 2021].
[17] Bundesamt für Sicherheit in der Informationstechnik, "Migration zu Post-Quanten-Kryptografie," 24 08 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf. [Accessed 21 11 2021].
[18] ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation," 03 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. [Accessed 24 10 2021].
[19] Nina Bindel and Udyani Herath and Matthew McKague and Douglas Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure," 24 05 2017. [Online]. Available: https://eprint.iacr.org/2017/460. [Accessed 07 12 2021].
[20] A. Truskovsky, D. Van Geest, S. Fluhrer,P. Kampanakis, M. Ounsworth, S. Mister, "Multiple Public-Key Algorithm X.509 Certificates draft-truskovsky-lamps-pq-hybrid-x509-01," 29 08 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-01. [Accessed 07 12 2021].
[21] Open Quantum Safe, "X.509," [Online]. Available: https://openquantumsafe.org/applications/x509.html. [Accessed 07 12 2021].
[22] ISARA Corporation, "ISARA Radiate OpenSSL Connector 1.4 QS Multiple Public Key Algorithm Certificate Tutorial," 26 03 2018. [Online]. Available: https://www.isara.com/openssl/1.4/OpenSSL-Connector-MPKAC-Tutorial.html#ProgrammersGuidetoMPKAC. [Accessed 07 12 2021].
[23] eIDAS eID Technical Subgroup, "eIDAS Cryptographic Requirements for the Interoperability Framework," 31 08 2019. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf. [Accessed 05 11 2021].
[24] D. J. Bernstein, "Grover vs. McEliece," Sendrier N. (eds) Post-Quantum Cryptography. PQCrypto 2010. Lecture Notes in Computer Science, vol. 6061, 2010.
[25] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on the, Philadelphia, Association for Computer Machinery, 1996, pp. 212-219.

APPLICATION OF ARTIFICAL INTELLIGENCE TECHNOLOGY IN GOODS TRANSPORT

ÖNVEZETŐ TECHNOLÓGIA ALKALMAZÁSA ÁRUSZÁLLÍTÁSBAN

VIKTOR Patrik[1] – MOLNÁR Albert[2] – SIMON Dániel[3]

Abstract

Nowadays, self-driving vehicles are becoming more common on public roads. There is no doubt that self-driving car technology has undergone significant development in recent years and now allows drivers to hand over control to a vehicle under appropriate predictable conditions. The concept of fully autonomous vehicles exists, however, their capabilities in navigating on public roads are still a far cry from reality. There are also several technological and ethical issues to consider concerning autonomous driving, which are expected to be addressed and fully resolved shortly. The research aims to provide an overview of the current stage of technological development of autonomous vehicles through a complex literature review and explore the progress of automation in the case of Hungarian logistics companies in the framework of a quantitative questionnaire. This research will further assess the future and applicability of self-driving vehicles based on the opinions of the interviewed company managers.

Keywords

self - driving vehicles, Autonomous trucks, logistics, shipment, safety, AI.

Absztrakt

Manapság egyre elterjedtebbek az önvezető járművek a közutakon. Kétségtelen, hogy az önvezető autók technológiája jelentős fejlődésen ment keresztül az elmúlt években, és mára lehetővé teszi a sofőrök számára, hogy megfelelő előrelátható körülmények között átadják az irányítást a járműnek. A teljesen autonóm járművek koncepciója létezik, azonban a közutakon való navigálási képességeik még mindig nagyon távol állnak a valóságtól. Az autonóm vezetéssel kapcsolatban számos technológiai és etikai probléma is megfontolandó, amelyeket várhatóan rövidesen megoldanak és teljesen megoldanak. A kutatás célja, hogy egy komplex szakirodalmi áttekintésen keresztül áttekintést adjon az autonóm járművek technológiai fejlődésének jelenlegi stádiumáról, és kvantitatív kérdőív keretében feltárja az automatizálás előrehaladását a magyar logisztikai vállalatok esetében. Ez a kutatás a megkérdezett cégvezetők véleménye alapján tovább méri az önvezető járművek jövőjét és alkalmazhatóságát.

Keywords

önvezetőjármű, autonóm kaminon, mesterséges intelligencia, logisztika, szállítmányozás.

[1] viktor.patrik@uni-obuda.hu | ORCID: 0000-0002-8689-2753 | PhD student, Óbuda University | PhD hallgató, Óbudai Egyetem

[2] treblaranlom@gmail.com | ORCID: 0000-0003-0531-1855 | MSc student, Óbuda University | MSc hallgató, Óbudai Egyetem

[3] simon.daniel277@gmail.com | ORCID: 0000-0001-8333-8936 | MSc student, Óbuda University | MSc hallgató, Óbudai Egyetem

INTRODUCTION

In the last decade, the world economy has faced significant challenges. Increasing globalization, the importance of sustainability and technological development has come to the foreground and initiated deep structural changes in society. With globalization, the volume of goods transported has increased, which has facilitated the division of labor and also enabled the development of new technologies. The negative effects of globalization and internationalization have manifested themselves in the environment, with increased levels of pollution and C02 emissions.

Due to significant emissions from transport, there has been a growing demand in recent years for transport solutions that are reliable, efficient, and eco-friendly. Reducing the number of pollutants emitted by vehicles has become a primary task for vehicle manufacturers.

With the spread of globalization, consumer transportation needs have also changed. Many online platforms now allow us to order products from home with the push of a button, and the demand for accurate and fast delivery has thus increased substantially.

Advances in technological development brought on by Industry 4.0 provide a solution to many of the aforementioned challenges. We are witnessing nothing short of a technological revolution that will not only alter the way companies operate but will also transform our everyday lives.

The research aims to present self-driving technology, its application possibilities in the field of logistics, and to describe the economic and social changes and expectations that the technology will bring about.

With the help of a quantitative questionnaire, we are looking to determine the extent to which the respondents' experiences and expectations correspond to the changes predicted by the literature. In the quantitative survey, we collected the opinions of the employees and chief executives of logistics companies, and the answers were visually represented in graphs, diagrams and we further made statistical inferences.

LITERATURE REVIEW

The development of electric vehicles has laid the foundations for the introduction of a higher level of automation in the field of transport in the future.

The development of vehicles, especially road vehicles has accelerated in recent years, with more and more computer processing units appearing in vehicles. These include engine control, which affects the operation of the vehicle, an electronic stability program that increases the safety of the vehicle, and also cruise control systems that remove additional workload from drivers making the driving experience more comfortable. Some modern vehicles already have communication systems integrated into their processing units, thereby enabling vehicles to connect to other vehicles or the surrounding infrastructure. [1] Currently, the literature defines the following forms of communication: V2V (Vehicle to vehicle), V2I (Vehicle to infrastructure), and V2X (Vehicle to Everything) communication technologies.

In addition to features connected to convenience, data collected while driving is becoming increasingly important. More and more detailed information is emerging about travel, which is currently mostly used separately and independently. Huge opportunities open up, when considering using the information collected while traveling that form the

concept of Big Data. Research involving Intelligent Transport Systems (ITS) is becoming increasingly popular and aims to merge intelligent transport infrastructures that can create a complex network with semi or fully autonomous vehicles.

For decades, these technical innovations have allowed us to consider the possibility of a self-driving car. Cars driving on public roads without a driver are, of course, still perceived with aversion today. [2]

Concept and levels

We have reviewed foreign works on the topic of self-driving vehicles and found that the term autonomous vehicle is frequently used interchangeably with driverless car can be found in numerous terms, such as autonomous car, driverless car, self-driving car, and robotic car. [3]

A generally accepted definition of a self-driving car is that of a vehicle driven without human intervention, using digital technologies, that is able to travel in road traffic, senses the details of its surroundings, and navigates itself. Ironically characterized by alapjarat "There are four key stages to self-driving technology - without a foot, without a hand, without an eye, without thinking - driving assistance systems will be gradually replaced by a self-driving system."[4]

Levels of self-driving

At the lowest level of the stairs is the current knowledge of current cars. On the 1st level there are mainly cars equipped with parking assistance systems, such as reversing radar, but all movements and instructions are decided by man. The driver performs all driving operations, and the vehicle is fully human is under control.[5]

They start at level 2 with driver assistance and self-driving on the highway implementing vehicles that are already able to intervene actively in driving, such as lane keeping. The driving assistance system is the steering or take over the braking and acceleration operation or help make it safer operation. However, the vehicle is completely under human control.

Level 3 is equivalent to maneuvers such as the Tesla Autopilot can also be found in the system, such as overtaking on the highways, the car fully man-controlled, the driving environment is the automated system watching. We are now at level 3 in everyday use.[6]

There are two more levels left to achieve full self-direction, the 4th step is already complete

allows the car autonomy, but the driver must always be prepared to intervene if necessary, and the car must be given sufficient time to do so to the driver. The highest level 5, called complete self-drive, is already possible makes the car invent itself in any traffic situation.[7]

Implementing self-driving requires three main components, a perception, ie the recognition of the environment, decision-making and subsequent action, that is, issuing commands to the car. The first component is perception, recognizing the environment for which one is great precision laser rangefinder is mounted on the top of the car but the car at various points, several additional cameras also help to map the environment. [8] This the camera system helps the driver orient himself, giving the driver an image as if the car would have been picked up from above. The driver of the vehicle sees what is going on on a screen

behind, in front of and next to the car.[9] This high definition camera has lights and white-boards it also plays a role in recognizing the data from the laser rangefinder are compared to a high-precision map database so that vehicle control is aware of the area with applicable traffic regulations. Even a GPS sensor is essential, which can determine the position of the car with an accuracy of a few meters.[10] The camera system contains a kind of artificial intelligence called neural network-based recognition and 3D reconstruction of the environment, so we know to tell where we are in space, what is around us and how that changes, given we can track objects and predict their location.[11]

APPLICATION OF AUTONOMOUS DRIVING SOLUTIONS

Research topic, assumptions

The research aims to present self-driving technology and its application possibilities in the field of logistics, with a strong emphasis on environmental impacts. The scope of the research covers the opportunities and obstacles inherent in the introduction of self-driving technology in vehicles, their expected economic benefits, and environmental impacts.

The following assumptions were made while conducting the research:

- A. It is assumed that technological development hinders the introduction of self-driving trucks in logistics.
- B. We assume that the cost of trucks will inevitably increase in the future with the introduction of new technologies, which is why the range of companies is expected to change. The size of well-established logistics and truck manufacturing companies is likely to increase, while it will become harder for new companies to enter the market and to compete.

The research seeks to find answers to the following questions:

- Q1. What are the barriers to the introduction of autonomous trucks, according to the respondents?
- Q2. What are the expected benefits and drawbacks of the introduction and usage of autonomous trucks, according to the respondents?
- Q3. According to the respondents when can we expect autonomous trucks to be used in commerce and shipments?

Methodology

The paper presents the term autonomous vehicles from several angles and how self-driving technology is expected to affect the operations of logistics and shipping companies. The aim is to summarize and explore all those factors and challenges shipping companies are expected to face when following the introduction of autonomous transporting vehicles.

The study is based on a quantitative method, as it is one of the most suitable ways to measure the expected behavior of enterprises, and the data can be well analyzed using quantifiable and statistical methods. Within this framework, the questionnaire method was used.

In compiling the questionnaire, questions were formulated to compare the expected changes that come with the introduction of autonomous vehicles in literature with those obtained in the survey from respondents. We also considered how well the expected changes, opportunities, and obstacles mentioned in the literature meet the expectations of the selected employees and executives.

Results

The demographic composition of the survey shows that 57% of the chief employees of companies are men. More than half (57%) of the respondents were between the ages of 30 and 45, while those employees under 30 comprised 29% of the total population. The smallest group included people between 45 and 60, making up 14% of the total.

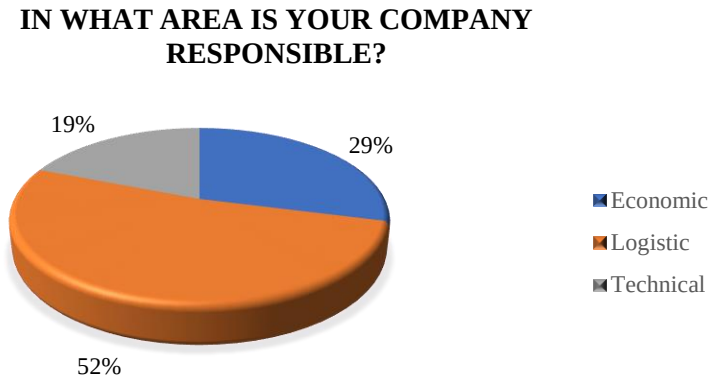


Figure 1:Field of responsibilities of the surveyed employees.Source: own research

Over half of the respondents (52%) identified logistics as their primary field of responsibilities at work. At the same time, 29% perform economics-related activities in their companies and 19% of the respondents work in the field of engineering and technology. The composition of the respondents confirms that the target group selection method ensured that the majority of the respondents had a certain level of knowledge in the field of transport and technology in the field of logistics.

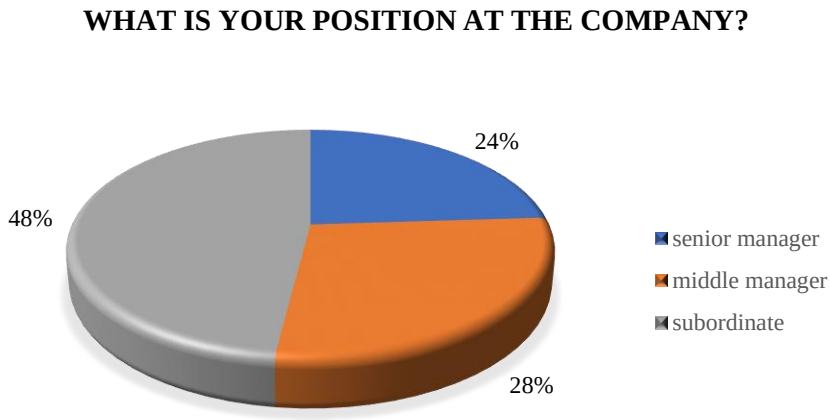


Figure 2: Positions of the employees in their companies. Source: own research

There was a nearly equal number of upper- and middle-level managers among the respondents. 24% of the respondents are top managers and 28% are middle managers.

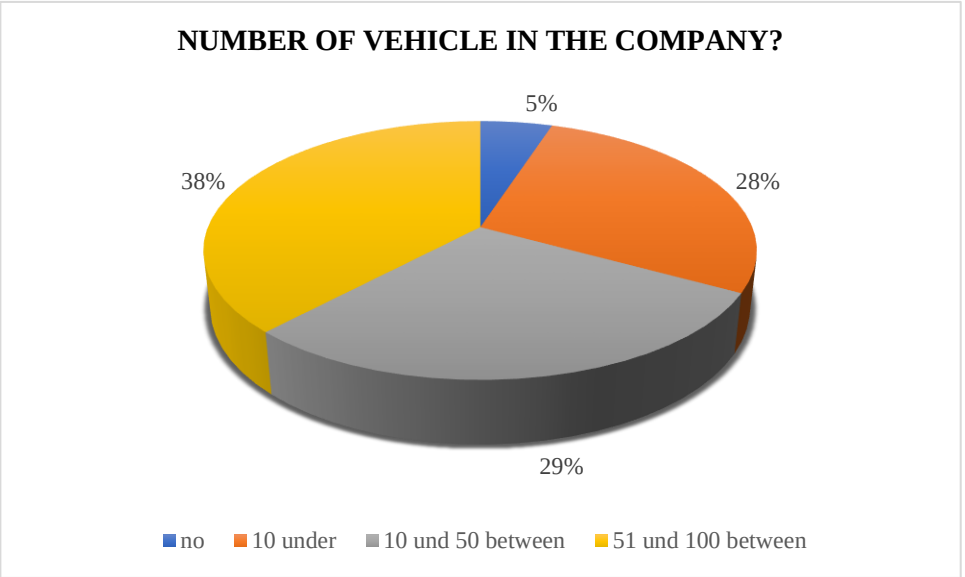


Figure 3 : Number of vehicles used in commercial activities of companies. Source: own research

It is typical for the respondents to work for bigger logistics and transportation companies with a lot of and operational vehicles. 38% of the companies use 50 to 100 transporting vehicles for their operations, while 29% use 10 – 50 vehicles. Almost a third of the companies (28%) operate with a number of vehicles that is equal to or lower than 10. Five percent of the respondents reported that they do not use any sort of transporting vehicles at all for their operations.

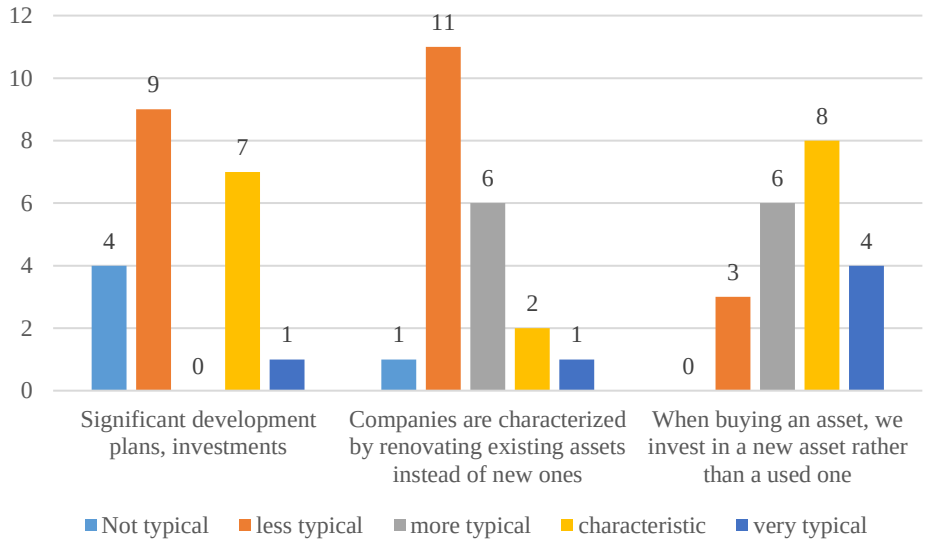


Figure 4: Company statements. Source: own research

According to the respondents, 8 out of 21 companies have a strategic plan and 18 companies prefer to buy a new asset in case of investment. Respondents reported that only 8 companies would prefer utilizing existing equipment instead of investing in a new one. Based on this, it can be concluded that the respondents are relatively willing to invest and prefer purchasing new assets.

15 out of the 21 respondents highlighted the exact same issues when answering to the question of obstacles and difficulties their companies face today. One of the most common responses was labor shortages, in particular, driver shortages, which were mentioned by 10 respondents. In addition, the following problems were highlighted:

- Increases in fuel prices, tolls, vehicle and parts prices, compulsory third party vehicle insurance.
- Freight rates and a rapidly changing market environment.
- High dependance on operation of transport, outsourcing and foreign workers.
- Issues with subcontractors

Autonomous driving technology awareness

Respondents were almost completely familiar with the concept of self-driving technology, with 20 of the 21 respondents providing positive answers to the question of : "Have you heard of self-driving technology?".

For an open ended question of "What, in your opinion, is meant by autonomous driving technologies?" the respondents gave specific answers mentioning a certain area of application of self-driving technology. The respondents referred to the following forms of autonomous vehicles:

- Forklifts in warehouses (1 answer)
- Application of robots (2 answers)
- Automated driving without human intervention (12 answers)
- Platooning (1 answer)

Some of the respondents with a deeper knowledge of the subject gave detailed answers, for instance:

„Driving is performed with "smart vehicles" that communicate with each other and with other interfaces instead of being controlled directly through human intervention. Such vehicles are also equipped with additional functions, such as safety, energy saving, comfort and environmental friendliness"

„ Autonomous vehicles are technologically controlled vehicles capable of travelling without human intervention. However, to the best of my knowledge, current "self-driving" vehicles still need a human presence and sometimes control."

The effects of autonomous vehicles, barriers of implementation

Seven questions were formulated regarding the introduction of self-driving technology, self-driving trucks, the expected effects and the factors hindering their introduction into commerce and shipment. The summaries of the received answers can be seen in the diagrams below.

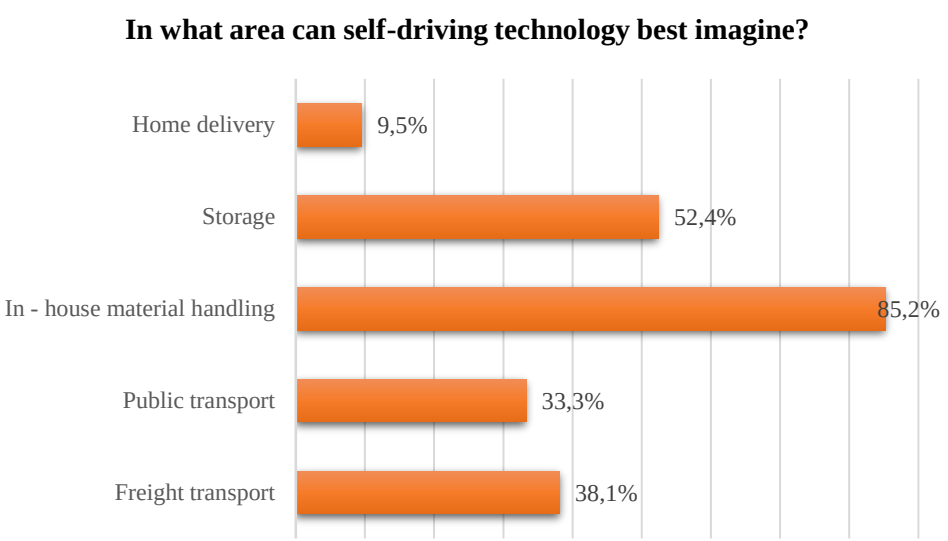


Figure 5: Areas self-driving technologies could be implemented in. Source: own research

Respondents are most likely to imagine the use of self-driving technology in the field of intra-factory logistics and handling, with 85.7% indicating this answer. Warehousing is also considered an important area, as every second respondent can imagine introducing it in this area as well. Its use in freight transport and public transport was chosen by 38.1% and 33.3% of the respondents, respectively. Delivery was indicated by only two respondents.

According to the respondents, the current condition of critical infrastructure poses the main threat, and simultaneously, the largest obstacle for the development and introduction of technology on public roads. 90.5% of respondents believe that this factor will hinder the spread of self-driving vehicles. 61.9% of the respondents mentioned the speed of technological development to be the main factor hindering the spread of autonomous vehicles. Every third respondent believes that technical development is not yet at the level to be introduced into everyday use in the near future. 52.4% believe that prejudice and lack of trust will be barriers to the adoption of the technology. The development of legal regulations and IT networks was perceived as an impediment by 38.1% of respondents, while less than the previous ones.

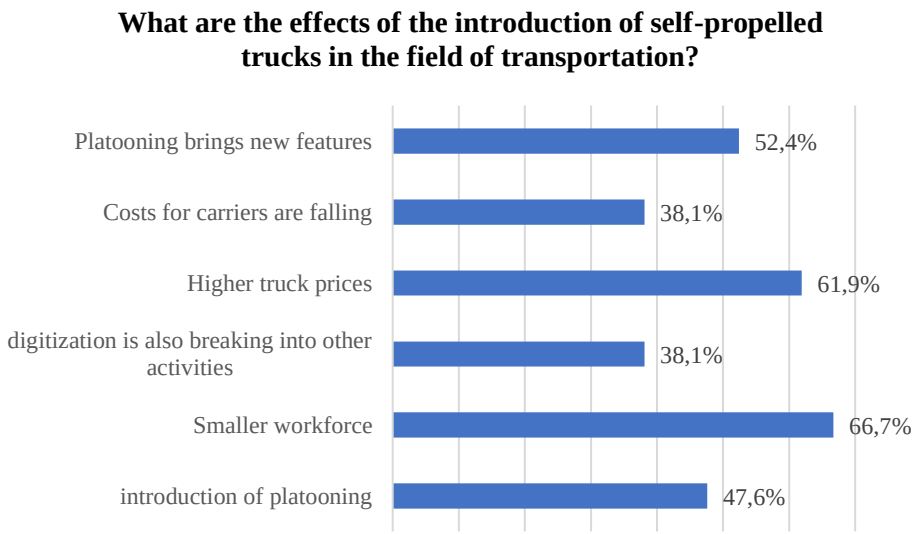


Figure 6: The effects of introduction of autonomous trucks in shipping and logistics. Source: own research

Among the expected effects of the introduction of self-propelled trucks, the respondents mentioned that the field of transportation is influenced by two main factors. The first one is that there is a significantly smaller need for a workforce in the case of this technology, with 66.7% of respondents saying this will have a significant impact on the shipping industry. The other is the high price of self-driving trucks, which could drive smaller companies out of the market, according to 61.9% of respondents. As a result of the introduction of the platooning technology, 52.4% of the respondents reported that they may create new services, while 47.6% mentioned that they will increase the utilization of vehicles. The least influential factors were reported to be digitalization and reduction of operating costs for haulers, both of which were identified by 38% of the respondents.

According to 95.2% of the respondents, the development of the road network is the biggest obstacle to the introduction of self-driving trucks. This factor was also highlighted in question 13 when examining the barriers of introduction of self-driving vehicles. The other main obstacle is the efficient and successful handling of the drivers' tasks. This answer was indicated by 66.7% of the respondents. Purchasing price and legal regulations were identified by 52.4%, with technical equipment being the least disruptive, with only 23.8% choosing it. Three of the listed factors could be identified.

SUMMARY

When choosing the research topic, we did not possess a deeper knowledge of self-driving technology, mainly because of the curiosity and topicality of the topic and its connection to the field of logistics. During the processing of the literature, we were enriched with interesting information. Numerous articles can be read online about self-driving technology, related developments, companies involved in the development, experiments demonstrating its use, but the evaluation of the expected barriers and impacts of the introduction receives less attention. More detailed articles and studies related to the topic are still

available primarily in foreign literature. The choice of topic, however, has limited a lot of possibilities, the analysis of the individual highlighted factors and effects could also be the topic of an independent research in the future.

- Research has shown that self-driving technology will significantly transform all sectors of the economy and change the labor market and our working conditions. The changes that most affect our daily lives may be the following:
- Public transportation is expected to gain more traction and popularity in the future, reducing the number of privately owned vehicles.
- The increase of public transport on roads will reduce emissions from transport by orders of magnitude, additionally, it will improve air quality and have a positive impact on health.
- Areas currently used for parking may become vacant, making cities less congested and more livable, and safer. The vacated areas will be used to alleviate the housing shortage, so other areas of the economy may also be positively impacted.
- Self-driving cars will also allow mobility for those who are currently unable to afford a car or are currently unable to drive, like the elderly or disabled.
- Cheaper transport leaves resources that can be spent freely by households, some of which will appear as additional consumption by households and businesses.
- Traffic jams are reduced, traffic becomes safer, as the number of cars reduces.
- One of the most vivid effects this will have on our daily lives is that the time spent on leisure will increase. We will be able to spend our time on other activities.

It will also fundamentally change the field of shipping and will result in substantial changes, the most important of which are:

- In the field of logistics, several applications will become more widespread, for example, autonomous forklifts will be able to handle materials on their own, programmed robots will be used to sort goods, and wire-based transport can be a new way of transporting online orders. A new mode of freight transportation strategy will gain spread - platooning, the essence of which is that self-driving trucks will travel in convoys and only the leading car will have a driver behind the wheel, followed by other units without a driver, braking, accelerating, and performing evasive maneuvers at the same time
- As a result of self-driving technology, the composition of the workforce of logistics companies will inevitably change. The current large-scale logistics business will operate with a smaller workforce, as there will be no need for drivers, at least not on this scale.
- The composition and role of transport participants are changing, and new activities are emerging or disappearing. New activities emerge from the replacement of tasks performed by the driver by A. I include the online management and tracking of shipments, the operation of online certification systems (CMR, transport documents, invoice, customs). The new process will involve significant digitization, IT development, and manpower.
- Reductions in fuel costs are due, among other things, to favorable changes in external factors affecting consumption, such as the driving technique and the route chosen. Maintenance costs are also reduced, as electric vehicles have a much lower chance of failure.

- A significant increase in the cost of transport equipment is expected. Due to the high cost of transport, only large, capital-intensive companies can initially invest in self-driving vehicles, which may result in small companies being pushed out of the market in the initial stages of the technologies' introduction.

The research summarized the changes and effects expected with the introduction of self-driving technology. It also highlighted the obstacles to its introduction and drew attention to the changes generated by self-driving technology, which we can prepare for and the transition of which we can manage.

REFERENCES

[1.] Koopman, Philip és Michael Wagner. "Kihívások az autonóm járművek tesztelésében és érvényesítésében." SAE International Journal of Transportation Safety 4.1 (2016): 15-24.

[2.] Varga I. és Tettamanti T. A jövő intelligens járművei és az infokommunikáció hatása, Magyar jövő Internet Konferencia LXXI.(2016) https://www.hte.hu/documents/10180/1727937/HT_2016- 1_MJIK2015_9_Varga_Tettamanti.pdf

[3.] Alapjarat.hu. Minden, amit az önvezető autókról tudnod kell https://alapjarat.hu/hasznos-infok/minden-amit-az-onvezeto-autokrol-tudnod- kell, (2018) [olvasva: 2021.01.31]

[4.] Narayanan, Santhanakrishnan, Emmanouil Chaniotakis, and Constantinos Antoniou. "Shared autonomous vehicle services: A comprehensive review." Transportation Research Part C: Emerging Technologies 111 (2020): 255-293.

[5.] Liu, Shaoshan, et al. "Creating autonomous vehicle systems." Synthesis Lectures on Computer Science 6.1 (2017): i-186.

[6.] Kuutti, Sampo, et al. "A survey of deep learning applications to autonomous vehicle control." IEEE Transactions on Intelligent Transportation Systems 22.2 (2020): 712-733.

[7.] Kusumakar, Rakshith, et al. "INTRALOG–intelligent autonomous truck applications in logistics; single and double articulated autonomous rearward docking on DCs." IET Intelligent Transport Systems 12.9 (2018): 1045-1052.

[8.] Tohme, Rita, and Matthew Yarnold. "Steel Bridge Load Rating Impacts Owing to Autonomous Truck Platoons." Transportation Research Record 2674.2 (2020): 57-67.

[9.] Gomes, Iago Pachêco, et al. "Diagnostic analysis for an autonomous truck using multiple attribute decision making." 2018 Latin American Robotic Symposium, 2018 Brazilian Symposium on Robotics (SBR) and 2018 Workshop on Robotics in Education (WRE). IEEE, 2018.

[10.] Ágnes, Kemendi ; Pál, Michelberger ; Agata, Mesjasz-Lech ICT security in businesses – efficiency analysisENTREPRENEURSHIP AND SUSTAINABILITY ISSUES 9 : 1 pp. 123-149. , 27 p. (2021)

[11.] Janz, Alexej, and Uwe Schob. "Highly autonomous truck driving on the freeway and in urban traffic." ATZ worldwide 120.1 (2018): 68-71.

THE PAST, PRESENT AND FUTURE OF ARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF SENIOR AND JUNIOR EXPERTS (PART 1)

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

HEITLERNÉ LEHOCZKY Mária[2] – KOLLÁR Csaba[3]

Abstract

The Artificial Intelligence Workshop at the Bánki Donát Faculty of Mechanical and Safety Engineering of Óbuda University is engaged in technical-informatics research, development, maintenance of subjects, thesis and doctoral thesis topics, teaching and topic management, as well as research in the impact of artificial intelligence on society. Our research uses qualitative, quantitative and hybrid methods in online and offline environments to explore the present and possible future of AI in order to contribute to the creation of an ethical AI-based world. In the present research, we used a focus group expert interview method. The first part of our study, after presenting the methodology, presents the views of senior experts.

Keywords

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

Absztrakt

Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnök karon működő Mesterséges Intelligencia Műhely a műszaki-informatikai kutatások, fejlesztések, tantárgyak gondozása, szakdolgozati és doktori témák meghirdetése, oktatás és témavezetés mellett a mesterséges intelligencia társadalomra gyakorolt hatásaival is foglalkozik. Kutatásaink során online és offline környezetben kvalitatív, kvantitatív és hibrid módszerekkel vizsgáljuk a mesterséges intelligencia jelenét és lehetséges jövőjét annak érdekében, hogy ajánlásainkkal hozzá tudjunk járulni az etikus mesterséges intelligenciára épülő világ megteremtéséhez. Jelen kutatásunkban fókuszcsoportos szakértői megkérdezés módszerével vizsgáltuk a témát. Tanulmányunk első része a módszertan bemutatása után a senior szakértők véleményét ismerteti.

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] 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 Biztoságtudományi Doktori Iskola | tag, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

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

BEVEZETÉS: A KUTATÁSI MÓDSZER ISMERTETÉSE

A fókuszcsoportos megkérdezés/beszélgetés a kvalitatív kutatási módszerek közé tartozik, s egyaránt találkozhatunk vele a szociológia, s tágabban véve a társadalomtudományok, valamint a marketing-, reklám-, piac- és közvéleménykutatás, illetve a pszichológia területén is. Jelen kutatásunkban alkalmazott módszertanunk kidolgozásában, valamint az eredmények, mint szöveges tartalmak feldolgozásában és kiértékelésében a társadalomtudományos alapokat Cseh-Szombathy és Ferge [1], Earl [2], Krippendorff [3], Horváth és Mitev [4], Gordon és Langmaid [5], Langer [6] írásai jelentették. Bár kutatásunk nem volt marketinges irányultságú, a fókuszcsoport megszervezésében, valamint a fókuszcsoportos beszélgetések megvalósításában Malhotra [7], Scipione [8], Kollár [9] Vicsek [10] műveire támaszkodtunk. A két (senior és junior) csoport tagjainak kiválasztásánál – ahogy arról még később részletesen írni fogunk – a hagyományos kiválasztási módszerekhez és eljárásokhoz képest lényegesen szigorúbban jártunk el annak érdekében, hogy a senior csoport tagjai minden szempontból megfeleljenek a szakértői kiválasztás [11] követelményeinek, míg a junior szakértők kiválasztásánál nem annyira szigorúan, de arra törekedtünk, hogy a csoport tagjaira igaz legyen az a megállapítás, hogy a mesterséges intelligenciával és a rotobotikával egy átlagos érdeklődőhöz képest műszaki-informatikai ismereteiknek köszönhetően igazolhatóan és ténylegesen mélyrehatóbban és alaposabban foglalkoznak.

A két szakértői csoport általános jellemzőit, illetve az általunk használt módszertan ismérveit a következőkben adjuk meg. A csoportok tagjai többféle, maguk által konstruált valóságképpel rendelkeznek, melyet megosztanak egymással, illetve a beszélgetés során a feltett kérdések és az egymással történő interakciók során alakítanak, formálnak magukban. A mérés, az adatok számszerűsítése a nagyon egyszerű demográfiai csoportleírást leszámítva nem fontos. Mintavételünk célja a szakértők álláspontjának és véleményének mélyebb megismerése, ennek érdekében olyan légkört teremtettünk az online és a fizikai világban is, hogy szakértőink egymással és velünk kötetlenül, beszélgettek. Az oldott, baráti légkör megteremtését szolgálták a nyitókör és a ráhangolódás részekben feltett kérdéseink is. Elemzésünk alapját a „jelenségek lényegét megőrző, kontextusba ágyazott leírása, megértése” [4: 35 p.] jelentette.

Kutatásunkat Malhotra [7: 206 p.] alapján az alábbi tervezési és lebonyolítási lépések szerint valósítottuk meg:

1. Célkitűzések meghatározása és a kutatási probléma definiálása: a mesterséges intelligencia az elmúlt 10-15 évben a tudományos életben szinte valamennyi területen a diskurzusok középpontjába került. Megannyi kérdőíves kutatás és a mesterséges intelligenciával és robotikával foglalkozó kísérlet eredményét lehet megismerni szakmai-tudományos folyóiratokban, illetve a teoretikus szerzők önálló, vagy társszerzőkkel írt könyvei is gazdag ismeretanyaggal szolgálnak a téma iránt érdeklődők számára. Ugyanakkor hiányát éreztük egy olyan friss, Magyarországon végzett kvalitatív kutatásnak, melyben a témával foglalkozó, az átlaghoz képest lényegesen gazdagabb és megalapozottabb tudással rendelkező szakemberek osztják meg egymással, illetve tanulmányunkon keresztül az olvasókkal is véleményüket a mesterséges intelligenciáról, annak hatásairól, milyennek értékelik a mesterséges intelligencia jövőjét, benne saját és a társadalom szerepét, milyen kihívásoknak kell megfelelni tíz év múlva, illetve, hogy a mesterséges intelligenciára összességében inkább kockázatként, vagy lehetőségként tekintenek.

2. A kvalitatív kutatás célkitűzéseinek, módszerének meghatározása: a mesterséges intelligencia jelenlegi és jövőbeli lehetőségeinek és kockázatainak feltérképezése szigorú kiválasztáson átesett senior és junior szakértők körében végzett fókuszcsoportos szakértői megkérdezés módszerével célunk továbbá a két csoport véleménye és álláspontja közötti hasonlóságokat és különbözőségek megismerése. A senior és junior vélemények összevetése lehetőséget adott a számunkra a mesterséges intelligencia generációk közötti megítélésének a vizsgálatára is (lásd: tanulmányunk 2. része).
3. A fókuszcsoportok által megválaszolandó kérdések meghatározása: részletesen lásd az egyes szakértői csoportoknál a „csoport körében vizsgált kérdések, területek" alfejezetet.
4. A szűrő kérdőív: a szűrő kérdőív fogalma alatt jelen kutatásunkban a szakértők kiválasztásával kapcsolatos szűrést [11] értettük, vagyis azt, hogy milyen elvárásoknak kell megfelelnie azoknak a csoporttagoknak, akiket beválogattunk a senior, illetve a junior csoportokba.
5. A moderátorok interjú-vezérfonalának összeállítása: a beszélgetés vezérfonalát mindkét csoport esetében a (1) nyitókör, a (2) ráhangolás, a (3) főkérdések, illetve (4) a zárókör kérdései alapján építettük fel. A nyitókör és a ráhangolás – ahogy fentebb írtuk – hozzájárult az oldott légkör megteremtéséhez, míg a főkérdésekben a résztvevők a mesterséges intelligencia megjelenési területeivel, a jelenlegi és jövőbeli lehetőségeivel és korlátaival, valamint a mesterséges intelligencia rájuk, mint szakértőkre, illetve az általuk képviselt/ismert területeikre gyakorolt hatásaival foglalkoztak.
6. A fókuszcsoportos beszélgetések lebonyolítása: lásd az 1. táblázatban.
7. Az adatok elemzése: az adatokat a két szakértői csoportnál külön-külön elemeztük, ezek szerepelnek tanulmányunkban az adott szakértői csoportnál „A kutatás eredménye" című alfejezetekben.
8. Az eredmények összefoglalása: kutatási eredményeinket külön-külön közöltük az egyes szakértői csoportoknál.
9. Az eredmények komparatív összevetése és összefoglalása: tanulmányunk zárásaként (2. rész) a két csoportnál kapott eredményeket vetettük össze.

A fókuszcsoportos szakértői beszélgetések általános ismérveit Gordon és Langmaid [5: 57-58 pp.] felsorolása alapján a 1. táblázatban adjuk meg.

Ismérv	Senior szakértői csoport	Junior szakértői csoport
A szakértői beszélgetés időpontja	2022. február 21., hétfő, 18:00-20:05	2022. február 23., szerda, 10:00-12:15
A szakértői beszélgetés helyszíne	online (Zoom)	Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 306-os terem
A szakértői beszélgetés időtartama	125 perc	135 perc
A résztvevők demográfiai jellemzői	1 nő, 7 férfi min. életkor: 28 év max. életkor: 61 év életkori átlag: 43 év	3 nő, 2 férfi min. életkor: 20 év max. életkor: 28 év életkori átlag: 24 év

Ismérv	Senior szakértői csoport	Junior szakértői csoport
	felsőfokú végzettséggel rendelkező szakemberek	egyetemi hallgatók (biztonságtechnikai mérnök)
A résztvevők száma	8 fő	5 fő
A helyiség ülésrendje	a Zoom alkalmazás által biztosított kezelőfelület alapján monitoron láthatták egymást és a moderátorokat a résztvevők	az asztal két oldalán, egymással szemben
A válaszolók és a moderátorok elhelyezkedése		az asztal rövidebb oldalán ült a két moderátor
A moderátorok személye	Az online és offline környezetben végzett kvalitatív és kvantitatív kutatásokban gyakorlott szakemberek: Heitlerné Lehoczky Mária (pszichológus-közgazdász), illetve Kollár Csaba (mérnök-bölcsész, a közgazdaságtudomány doktora).	
Megfigyelők, egyéb résztvevők	Annak érdekében, hogy minden kiválasztott és meghívott résztvevő a beszélgetés során végig aktív maradjon, ezért úgy döntöttünk, hogy a passzív résztvevőket, megfigyelőket nem engedjük be a beszélgetésbe.	
Technikai berendezések, informatikai háttér	Zoom alkalmazás, a résztvevők kérésére felvételt nem készítettünk	diktafon, a résztvevők hozzájárultak hangfelvétel készítéséhez

1. Táblázat: A fókuszcsoportos szakértői megkérdezések általános ismérvei [5] alapján saját szerkesztés.

A SENIOR SZAKÉRTŐI CSOPORT

A csoport bemutatása

A senior szakértők kiválasztásánál követve Kollár [11] ajánlásait az alábbiak szerint jártunk el. A fókuszcsoportos online szakértői beszélgetésen, általunk felkért szakértőkre a következő állítások igazak:

- felsőfokú végzettséggel rendelkezik
- tagja legalább az egyik szakmai-tudományos szervezetnek:
    - Óbudai Egyetem Mesterséges Intelligencia Műhely
    - Mesterséges Intelligencia Koalíció
    - Hírközlési és Informatikai Tudományos Egyesület Mesterséges Intelligencia Szakosztály
    - Humán Szakemberek Országos Szövetsége
    - Magyar Hadtudományi Társaság Elektronikai, Informatikai és Robotikai Szakosztály
    - Magyar Tudományos Akadémia Köztestület
- mesterséges intelligenciához, digitális társadalomhoz, ember-robot kapcsolathoz, ipar 4.0-hoz kapcsolódó területeken
    - dolgozik legalább 5 éve
    - legalább 3 darab, lektorált szakmai-tudományos folyóiratban megjelent tanulmánya van
    - legalább 3 előadást tartott szakmai-tudományos konferencián

A klasszikus fókuszcsoportos szakértői megkérdezésnél a szakértők a kutatási jelentésekben, s az abból készített tanulmányokban nevesítve szerepelnek. Az általunk felkért szakértők ehhez nem járultak hozzá, mivel többen olyan állami, kormányzati területen dolgoznak, melynél a nevesített nyilatkozatuk előtt engedélyt kellett volna kérniük az intézménytől, illetve a munkahelyi belső szabályzatok értelmében csak olyan véleményt fogalmazhatnak meg, amelyik egyben az intézmény álláspontját is tükrözi. Szakértőinknek az idő rövidsége miatt nem volt lehetőségük engedélyt kérni a névvel és munkahellyel felvállalt véleményük közléséhez, illetve fontosabbnak tartottuk a szakértők által megfogalmazott egyéni nézőpontok elemzését ahhoz képest, hogy a szervezet álláspontját elemezzük. A szakértői online fókuszcsoportos beszélgetésen 8 szakértő vett részt, 1 nő és 7 férfi. Senior szakértőink közül a legfiatalabb 28 éves, a legidősebb 61 éves, átlagéletkoruk 43 év. Az online fókuszcsoportos szakértői beszélgetésben résztvevők a következő felsőfokú végzettségekkel rendelkeznek: mérnök-informatikus-közgazdász, mérnök-közgazdász, mérnök-informatikus (2 fő), közgazdász-pszichológus, szociológus, mérnöktiszt, informatikus. A diplomák átlagos száma személyenként 1,75. Tudományos doktori fokozattal (közgazdaságtudomány, katonai műszaki tudomány, biztonságtudomány) 3 fő rendelkezik, illetve egy-egy résztvevőnk a Humán Szakemberek Országos Szövetsége szakértője, illetve a Magyar Hadtudományi Társaság szakértője.

A csoport körében vizsgált kérdések, területek

Nyitókör:

- Kérlek, mutatkozz be röviden.
- Jelenleg milyen területen dolgozol, mivel foglalkozol?

Ráhangolás:

- Mikor találkoztál először a mesterséges intelligenciával?
- Mi ragadott meg benne?
- Mikor és miért döntöttél úgy, hogy elkezdesz vele foglalkozni?

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 az online 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 bemutatkozás során – melyben a szakértők arra kértek, hogy ne lehessen következtetni személyükre – a következő fontosabb életutak, eredmények hangoztak el. Releváns, akár több területen szerzett szakmai tapasztalat (ez alátámasztja a csoport demográfiai leírását), eredményekben, sikerekben, elismerésekben és minősítésekben gazdag szakmai életút, a felsőfokú végzettségek mellett, annak megszerzését követően további szakirányú végzettségek és minősítések (certificate-ok), vállalati/szervezeti belső képzések, több esetben nemzetbiztonsági átvilágítás (ami feltétele bizonyos munkakörök betöltésének). A beszélgetésben résztvevő szakértőink közül többen adják át tudásukat külsős oktatóként felsőfokú intézményekben, illetve vesznek részt oktatóként/trénerként vállalati/szervezeti képzéseken is. Szakértőink közül hárman dolgoznak állami területen (nemzetbiztonság, 100%-os állami tulajdonban levő vállalat, minisztérium), öten pedig a versenyszférában tevékenykednek, de közülük ketten tanácsadóként/szakértőként részt vesznek állami projektekben is.

Megkérdezett szakértőink a mesterséges intelligenciával – életkorukból adódóan (legfiatalabb 28, legidősebb 61 éves) – eltérő korban találkoztak. A legfiatalabb szakértőnk a középiskolában ismerkedett meg a robotikával, s annak részeként a mesterséges intelligenciával, a többség viszont vagy egyetemi tanulmányai alatt, vagy azt követően továbbképzés során. Megemlítették, hogy a mesterséges intelligenciával való első találkozást úgy is átfogalmaznák, hogy a mesterséges intelligencia mögött húzódó adattudománnyal és algoritmizációval már régebben találkoztak, de a mesterséges intelligenciával, mint fogalommal csak később. Véleményük szerint a mesterséges intelligenciával kapcsolatos ismereteik sokkal megalapozottabbak annak köszönhetően, hogy előzetesen már ismerték a kibernetikát és annak elsősorban elméleti modelljeiket, s már szinte várták, hogy a számítástechnika, különösen a számítási kapacitások annyit fejlődjenek, hogy az elméleti modelleket ki lehessen próbálni sok adaton a gyakorlatban is.

A mesterséges intelligenciával és a hozzá szorosan kapcsolódó területekkel történő tudományos-szakmai elköteleződésben komoly szerepet játszott szakértőinknél az a vágy, hogy a mesterséges intelligencia segítségével olyan problémákra is megoldást lehet találni, amelyek bonyolultságuknál és komplexitásuknál fogva csak emberi erőfeszítés és hagyományos számítógépek és programok segítségével nem, vagy csak hosszú időt igénylő számításokat követően van lehetőség. A robotok és a mesterséges intelligencia iránti érdeklődés felkeltésében és megtartásában valamennyi szakértő kiemelte, hogy a sci-fi- és robotirodalom klasszikusai (pl.: Karel Čapek: Rossum's Universal Robots, Ira Levin: A stepfordi feleségek, Isaac Asimov: Én a robot, Stanisław Lem munkái, illetve a Magyarországon népszerű Galaktika magazinban megjelenő írások), a sci-fi, illetve a sci-fi-horror filmek (pl.: Nyolcadik utas a halál (Alien), Robotzsaru, A nap, mikor megállt a Föld, Tiltott bolygó, Feltámad a vadnyugat, Szárnyas fejvadász, Terminátor, Mátrix) nagy hatást tettek rájuk. Ahogy az egyik szakértő fogalmazott: „azt hiszem tudom, hogy mi a különbség a tudomány és a fantasztikum között, de pont e két terület egymásra hatása eredményezi mindkét terület fejlődését". Egy másik résztvevő pedig úgy gondolja, hogy „a mi területünkön fontos, hogy lássuk, olvassuk, hogyan gondolkodnak a sci-fi művészek, hogy aztán az inspiráljon minket a valódi világban megvalósuló, az emberiség fejlődését segítő, mesterséges intelligenciával támogatott megoldások kifejlesztésére".

Az inspiráció és a fiatalkori élmények mellett szakértőink több ok miatt kezdtek el mesterséges intelligenciával foglalkozni: „jó érzés tudni, hogy a leginnovatívabb területtel tudok foglalkozni", „ez a terület folyamatosan arra ösztönöz, hogy képezzem, tovább képezzem magam, mert ha ezt nem teszem, akkor gyorsan piacképtelenné válok", „az adattudomány és a mesterséges intelligencia együttese hosszú távon garantál biztos megélhetést".

Szakértőinket arra kértük, hogy alkossák meg a mesterséges intelligencia definícióját. Mind a nyolc szakértő felvázolt egy definíciót, ugyanakkor több átfogalmazás során sem tudtunk elfogadni egy olyan definíciót, amelyik eszenciája lenne a külön-külön megalkotott definícióknak. A különbségek abból adódtak, hogy a kényelem-biztonság fogalmi tengelyén egyesek a biztonságot tartották a fontosabbnak, s ennek rendelték alá a mesterséges intelligencia által nyújtott kényelmet, míg mások úgy gondolták, hogy ha a mesterséges intelligencia használata (beleértve a kezelőfelületeket is) kényelmetlen, nehezen megérthető, akkor az átlagos felhasználó nem fog élni a mesterséges intelligencia által kínált lehetőségekkel, tehát hiába folynak a fejlesztések, a fejlesztésekre fordított összegek nem, vagy nem minden területen fognak megtérülni.

Mi a különbség a robotok és a mesterséges intelligencia között – tettük fel a kérdést szakértőinknek. Meglátásuk szerint a robotok és a mesterséges intelligencia két külön terület, melynek vannak metszéspontjai. A „sima" robotok nem feltétlenül rendelkeznek mesterséges intelligenciával, hiszen például egy összeszerelő üzemben a robotokat rendszerint egy szoftver is képes a meghatározott mozgások és idők alapján működtetni. A mesterséges intelligencia pedig létezhet robot test nélkül, hiszen például az informatikai rendszerek biztonságáért felelős mesterséges intelligencia nem más, mint egy bonyolult, több rejtett réteggel rendelkező, lágyszámításra épülő innovatív megoldás. A robotika és a mesterséges intelligencia metszéspontjába helyezték el szakértőink a kiber-fizikai rendszereket (ipar 4.0) és az interaktív robotokat (társadalmi, társas készségekkel rendelkező robotok, terápiás képességgel rendelkező robotok), ez utóbbinál megállja a helyét az a megközelítés, hogy az emberszerű, vagy állatszerű robot (humanoid, animoid) hordozza a „fejében" a mesterséges

intelligenciát. Egyik szakértőnk megjegyezte, hogy egy átlagember számára ezek a robotok jelentik a testet öltött mesterséges intelligenciát, különösen, hogy elég sok disztópikus filmben az ilyen humanoidok veszik át az emberek felett a hatalmat, s az emberek fölé kerekedve, az emberiséget rabszolgává teszik, vagy megpróbálják ki is irtani. Ugyanakkor az ilyen emberszerű robotok szerethető formában is megjelennek, amelyek éppen a mesterséges intelligenciával ellátott robotok elfogadását teszik lehetővé, ami már pszichológiai vonatkozásokat is érint, a társas kapcsolatokat és az érzelmeket (félelem, szorongás).

Szakértőink az élet szinte valamennyi területén találkoztak a mesterséges intelligenciával. A következő területeket nevesítették: okosotthonok (domotika), személyre szabott gyógyítás és gyógyszerezés, személyi asszisztensek, intelligens biometrikus azonosító rendszerek, információbiztonság és informatikai rendszerek védelme, ipar 4.0 megoldások, katonai és nemzetbiztonsági megoldások, nagyvárosok, megapoliszok intelligens irányítása, közlekedés, önjáró/önvezető autók, környezetvédelem, mezőgazdaság, géntechnológia, gazdasági és pénzügyi előrejelzések, a kínai társadalmi kredit rendszere és hasonló, az emberi viselkedés elemzésére épülő rendszerek, személyre szabott tanítás, ismeretátadás, egyéni mentális és fizikai fejlesztő módszerek. Szakértőink vegyesen nyilatkoztak az említett területeken szerzett tapasztalataikról. Megkülönböztették a jópofa és a profi mesterséges intelligenciára épülő megoldásokat. Az első csoportnál, amelyiknél a működés inkább növelte a kényelmet, illetve szórakoztató volt, a szakértőink úgy gondolták, hogy fontos a könnyű használat, míg a profi megoldásokat elképzelhetetlennek tartották megfelelő adat- és információbiztonsági elvárások megléte nélkül. Az elégedettség kapcsán került említésre az a nézőpont is, hogy a mesterséges intelligenciára épülő alkalmazások és megoldások hibás működése (történjen kibertámadás, vagy hibás tanítás, vagy hibás programozás miatt is) milyen közvetlen, vagy közvetett veszélyt, vagy pénzben, illetve egyéb erőforrásban kifejezett kárt jelent az ember, vagy a mesterséges intelligenciát használó szakember, illetve szervezet számára. Amikor a kár elhanyagolható, akkor szakértőink sokkal elnézőbbek a hibás működést illetően, ugyanakkor a komolyabb károk esetében már sokkal szigorúbb elvárásokat fogalmaztak meg a mesterséges intelligencia működésével és biztonságával kapcsolatban.

Szakértőink úgy gondolják, hogy mivel az elmúlt közel tíz-tizenöt év a mesterséges intelligenciáról szól, ezért szinte biztosra tehető, hogy az élet valamennyi területén fejlődni fog. Az átlagoshoz képest nagyobb fejlődést ott tartják valószínűnek, ahol a mesterséges intelligencia használata vagy biztonsági kérdés (pl.: katonai és nemzetbiztonsági területek), vagy ahol a mesterséges intelligenciára épülő alkalmazások megvásárlása a fejlesztőket nagyon nagy bevételhez juttatja. Akár a biztonsági, akár a profit fókuszát is nézzük, úgy gondolják szakértőink, hogy sajnos számolni kell olyan megoldások megjelenésével, amelyek vagy csak egy szűk érdekcsoport hatalomvágyát szolgálják ki, vagy a fejlesztések során nem, vagy nem kellő hangsúllyal jelennek meg az etikus mesterséges intelligenciával szemben támasztott elvárások. A kellően sötét képet színesíti azonban a boldogabb, biztonságosabb, kényelmesebb jövőbe vetett bizalom, ami megjelenik az emberi életminőség javításában, a globális problémák eddigiekhez képest hatékonyabb megoldásában, az erőforrások mesterséges intelligencia segítségével történő észszerűbb és körültekintőbb felhasználásában, a kedvezőtlen folyamatok megállításában, illetve visszafordításában. Ahogy az egyik résztvevő fogalmazott: „mi, akik aktívan részt veszünk a mesterséges intelligencia segítségével a jövő alakításában, nem tehetjük meg, hogy ne gondoljuk arra, hogy csakis olyan

fejlesztési irányokat szabad támogatnunk, melyre gyerekeink és unokáink is elismerően tekintenek majd, s a számura is például szolgálnak".

A társadalom alapvetően nincs felkészülve a mesterséges intelligencia által gerjesztett gyors változásokra, vélik szakértőink. Egyértelműen látják, hogy számos szakma meg fog szűnni, s mellette olyan új szakmák is megjelennek, amelyeknek jelenleg még a nevét sem ismerjük. Régóta nyomon követhető az a folyamat, amelyik bizonyos területeken (pl.: autógyártás, elektronikai berendezések gyártása) radikálisan csökkentette a gyárban dolgozó emberek számát azzal, hogy az általuk végzett munkát automatizálták és robotokkal váltották ki. Mindkét közgazdasági végzettséggel rendelkező szakértőnk elmondta, hogy a vállalatok költséghatékony működésénél már évtizedekkel ezelőtt megfogalmazódott az a gondolat, hogy ha az adott munkatevékenység gazdaságosabban váltható ki robotokkal és automatizációval, s ezeknek a fejlesztéseknek a megtérülési ideje viszonylag egzakt módon meghatározható és így elfogadható, akkor az embereket a gépek le fogják váltani. Sajnos azok az alacsony képzettségű, idősebb munkavállalók, akik nem hajlandók, vagy nem képesek újabb szakmát tanulni, vagy magukat tovább képezni, illetve átképezni, egyértelműen vesztesei lesznek a modernizációs folyamatoknak, így például az ipar 4.0-nak, s majd az ipar 5.0-nak. Az esetükben nagy valószínűség szerint az adott ország társadalombiztosítási rendszerének kell majd számukra is elfogadható megoldást kínálni. Ha a társadalom magasabb végzettségű, fiatalabb, a változásokat jobban elviselő és azokhoz jobban alkalmazkodni tudó tagjait vizsgáljuk, akkor a mesterséges intelligencia inkább az újdonság varázsát, személyes fejlődésük egyik lehetőségét és támogatóját jelenti – vélik a szakértőink. Szakértőink maximálisan egyetértenek abban, hogy a vitáknak már nem arról kellene folynia szakmai körökben, hogy a mesterséges intelligencia fontos-e, hasznos-e, hanem arról, hogy hogyan kell, vagy kellene a társadalom minél több csoportját minél hamarabb felkészíteni a változásokra. Ehhez pedig közérthető és szakmailag modern tananyagokra van szükség. Ami szakértőink saját jövőképét illeti, bizakodva tekintenek a mesterséges intelligencia által körbe szőtt világra, s saját szerepükre: inkább előidézői, alakítói, semmint elszenvedői akarnak lenni a változásoknak. Ez pedig folyamatos szakmai fejlődéssel, az ismeretek mélyítésével és más kapcsolódó területek megismerésével érhető el szerintük.

A jövőről alkotott kép megfogalmazásánál egy konkrét évhez, 2032-höz is kötöttük a szakértői vélemények megfogalmazását. Milyen is lesz a világ tíz év múlva? Szakértőink részint szubjektív, részint objektív véleményt fogalmaztak meg. A szubjektív véleményük bizakodó. Bíznak abban, hogy a társadalmi és gazdasági folyamatok olyan irányt vesznek, mely összességében inkább pozitív lesz a világ számára. Objektív véleményük azonban nem ennyire optimista kicsengésű. Nagy valószínűség szerint megjelennek a különböző érdekcsoportok által finanszírozott, saját érdekeiket szolgáló fejlesztések. Számolni kell olyan esetekkel, amikor a mesterséges intelligencia hibás működéséből eredő következmények sokkal nagyobb katasztrófát idézhetnek elő annál, mint ha nem használták volna a mesterséges intelligenciát. A fegyverkezési versenyhez hasonlóan a mesterséges intelligencia fejlettségének bemutatásával meg lehet félemlíteni a másik felet, ami eddig nem ismert új politikai és gazdasági erőterek megjelenését jelenti. Valószínűsíthető, hogy az ezeket az erőtereket alakító és formáló erők nem az emberek fejlődését fogják szem előtt tartani, még akkor sem, ha esetleg ezt kommunikálják az általuk uralt és használt médiában.

A beszélgetésben résztvevő szakértők szerint boldogság és gondterheltség keveredni fog a mesterséges intelligencia által behálózott világban. A mesterséges intelligenciára épülő virtuális világokban és metaverzumokban az emberek megtalálhatják majd azt a boldogságukat, melyet hiába keresnek a valós, fizikai világban. A fizikai világ gondjai és problémái elől a metaverzumokba lehet menekülni, melyben mi, vagy avatárunk boldog, elégedett lehet, s a szituációkban esélye van hősnek lenni, vagy legalábbis érdekeit megfelelően képviselni. Szakértőink biztosak abban, hogy ezek a virtuális világok pont az említett okok miatt népszerűek lesznek, ugyanakkor az idősebb generáció tagjainak jelentős része mivel nem érti ezek értelmét és működését, nem fogja használni.

A beszélgetés során szakértőink többször érintették az etikus mesterséges intelligenciát. Ezért külön is megkérdeztük tőlük, hogy milyen módon lehet a mesterséges intelligenciát olyan irányokba fejleszteni, hogy az ne veszélyeztesse az emberiség jövőjét. Elmondták, hogy az Európai Uniónak, valamint több, mesterséges intelligenciával foglalkozó nemzetközi szervezetnek van ajánlása az etikus, alapvetően az asimovi elvekre épülő mesterséges intelligencia fejlesztésére vonatkozóan, ami jó. Az oktatásban is részt vevő szakértők elmondták, hogy számukra és tanártársaik számára is magától értetődő, hogy felhívják a diákok figyelmét a mesterséges intelligencia etikus fejlesztésének fontosságára, illetve már a projektfeladatok kiírásánál is csak olyan témákat írnak ki, amelyekben a mesterséges intelligencia fejlesztése során kizárólag etikus elvek mentén folyhat a fejlesztés. Kutatóként úgy gondoljuk, hogy a mesterséges intelligenciával és a kapcsolódó területeivel foglalkozó szakemberektől, szakértőktől, tanácsadóktól, oktatóktól maximálisan elfogadható az az attitűd, melyet az általunk megkérdezett nyolc szakértő képvisel. Ugyanakkor számunkra és a szakértőink számára is világos, hogy egyre több olyan fejlesztés jelenik meg – nem csak katonai területen – amelyikre sem az etikus, sem a humánus jelzők nem igazak. „A mesterséges intelligenciáról szóló ajánlások, szabályzatok, törvények csak annyit érnek, amennyit betartanak belőle. Ugyan a büntetés bizonyos esetekben visszatartó erővel bírhat, ugyanakkor sajnos általánosságban azt lehet mondani, hogy aki ártó szándékkal és önös céllal fejleszti a mesterséges intelligenciát, azt semmilyen büntetés nem fogja visszatartani" – összegezte véleményét az egyik szakértőnk. Egy másik szakértőnk pedig felhívta a figyelmet arra, hogy bár technikai körökben gyakran alulértékelik a társadalom erejét, számos eset igazolja, hogy a társadalom józan ítélőképessége és tömeges kiállása bizonyos ügyek, döntések mellett, vagy éppen ellen, képes megváltoztatni a dolgok állását, így a mesterséges intelligencia fejlődési irányait is. Ahogy fogalmazott „amit az ember lát a mesterséges intelligenciából, az a számára lehet szimpatikus, meg antipatikus is. De bárhogy is legyen, ha sokan vélekednek hasonlóan a mesterséges intelligencia bizonyos irányairól és megjelenési formáiról, s ennek hangot is adnak, azzal lehetőséget adnak maguknak, hogy a fejlődés irányát még a számukra elfogadható mederben tartsák". Ez persze csak akkor képzelhető el – véli válaszában másik szakértőnk – ha a társadalom minden tagja reális és kellően alapos ismeretekkel rendelkezik a mesterséges intelligenciáról.

Vannak olyan esetek és területek, amikor a mesterséges intelligenciára épülő alkalmazások nem, vagy csak részint felelnek meg az asimovi törvényeknek, s ez alapvetően – vélik szakértőink – mégis elfogadható. Ez a (nemzet)biztonság és a honvédelem. Ugyanakkor még ezeken a területeken is meg kell jelennie egyfajta mesterséges humánumnak a mesterséges intelligencia részéről. Ez a gyakorlatban azt jelenti, hogy az ellencsapás a csapás mértékéhez képest ne legyen kirívóan nagyobb, legyen lehetőség emberi beavatkozásra és

a békés rendezésre még azt megelőzően, hogy a mesterséges intelligencia az ellenség/ellenfél oldalán komoly károkat okozna. Ugyancsak fontos, hogy egyik fél se akarja az ellenfelet totálisan megsemmisíteni, s tartsa be a hadviselésre és a háborúkra vonatkozó etikai előírásokat, valamint a nemzetközi jogi szabályokat és megállapodásokat.

Beszélgetésünk zárásaként arra kértük szakértőinket, hogy összegezzék véleményüket. Íme: „A világ fejlődése már elképzelhetetlen a mesterséges intelligencia nélkül. Az, hogy ezen az emberiség nyer, vagy veszít, csak rajtunk, embereken múlik". „Korábban ember harcolt ember ellen, aztán technika technika ellen, s most úgy tűnik, hogy mesterséges intelligencia mesterséges intelligencia ellen. Lehet, hogy jobban járnánk, ha a harc helyett az együttműködést választanánk". „Amit nem ismerünk, attól rendszerint félünk, s félelmünk gyakran elutasítás, gyűlölet formájában jelenik meg. Ez így van a mesterséges intelligenciával is. Egy út van az emberiség számára: ismerje meg a mesterséges intelligenciát, hogy aztán tudatosan el tudja dönteni, hogy szereti, vagy gyűlöli". „A mesterséges intelligenciával kapcsolatos utópiák és disztópiák között nehéz megtalálni a reális és elfogadható forgatókönyvet. A szakemberek dolga, hogy ezt megtegyék, majd közérthető formában megismertessék az emberekkel". „Tudjuk, hogy a mesterséges intelligencia egyszer okosabb lesz nálunk. Az azonban nem mindegy, hogy egy nálunknál okosabb entitás hogyan viszonyul hozzánk. Azon kell dolgoznunk, hogy barátként tekintsen ránk". „A mesterséges intelligencia olyan lesz, amilyennek mi fejlesztjük. Egy normálisan gondolkodó szakembernek érdeke lehet, hogy ellenünk hangolja? Őszintén remélem, hogy nem!". „Nem vagyok biztos, hogy egy mondatban megfogalmazható a mai beszélgetés tanúsága. De abban igen, hogy az ilyen eszmecserék mindannyiunk számára hasznosak saját területünk fejlődése szempontjából". „Elmondhatjuk, hogy a mesterséges intelligencia volt, van, lesz. Ahogy azt is, hogy az ember volt, van. Hogy lesz-e az embernek jövője, az azon múlik, hogy mi szakemberek kellően hangosak leszünk akkor, amikor olyan irányba megy a mesterséges intelligencia fejlesztése, ami megítélésünk szerint már káros az emberiség számára".

A SENIOR SZAKÉRTŐK VÉLEMÉNYE ALAPJÁN MEGFOGALMAZOTT KÖVETKEZTETÉSEK, JAVASLATOK

A szakértői csoport többségének első tapasztalatai még az elméleti, kibernetikai modellekre épültek, melyre támaszkodva jelenleg is a mesterséges intelligencia fejlesztésének, oktatásának területén dolgoznak, így történeti rálátással rendelkeznek a mesterséges intelligencia fejlődésének folyamatáról és ezáltal a jövőbeli trendek alakulásának becslésében mérvadó a véleményük. Ahogyan a pályaválasztási döntések gyakran gyermekkori élményekre alapozódnak, a mesterséges intelligenciával, robotokkal kapcsolatos film és olvasmány élmények náluk is meghatározó szerepet töltöttek be. Emellett a munkájuk során folyamatos inspirációs báziskén használják a fikciókat, amely viszonylag ritka jelenség a hivatások között. A jövőben egyre növekszik az *igény a magasan képzett szakértőkre és fejlesztőkre* [12], ezért az érdeklődésre építve a filmek, játékok által a mesterséges intelligencia különböző területei, mint potenciális pályaválasztási irány, orientálhatók lehetnek a gyermekek számára.

A mesterséges intelligencia fogalmának meghatározásában a szakértők nem jutottak konszenzusra, ahogyan a szakirodalom sem egységes, inkább gyűjtőfogalomként érde-

mes tekinteni rá. A robotok és a mesterséges intelligencia megkülönböztetése kapcsán kirajzolódott a két lehetséges forgatókönyv: a humanoid/animoid robotok egy fenyegető, disztópikus jövőben az ember versenytársaként lépnek fel és átveszik a hatalmat, leigázzák az embereket, azonban nem említették a szakértők a *társadalmi egyenlőtlenségek* fokozódásával járó feszültségnövekedés veszélyét. Az optimista elképzelés szerint a robotok és a mesterséges intelligencia az emberi életminőségben pozitív változásokat fognak eredményezni, mert az emberi társadalom képes lesz a megküzdési potenciálját konstruktívan használni.

A mesterséges intelligencia nehéz definiálhatóságát indokolja, hogy rendkívül sokszínű jelenlegi alkalmazása is, a szakértők ezek felsorolásával egyidejűleg implicit formában érintették a társadalmi bizalom kérdését: az emberek az általuk nem ismert technikai háttérrel szemben gyanakvóvá válhatnak, visszaélésektől tartanak, ezért a *bizalmi deficit* [12] következtében elutasíthatják használatukat. A szakértők felvetették a *figyelemgazdaság* hatását is, azt az ellentmondást, hogy a „felhasználóbarát" („figyelemfelkeltő", kényelmes, szórakoztató, kevés kognitív erőfeszítést igénylő) alkalmazások nem feltétlenül biztonságosak, megbízhatók, a biztos profitszerzésre irányuló érdekeket szolgálja. Ezzel szemben a professzionális rendszerek költségeinek megtérülése nem minden esetben garantálható, a befektetők ezért gyakran szkeptikusak a mesterséges intelligencia gazdaságosságát tekintve [12].

A mesterséges intelligencia komplexitása következtében a kockázatelemzés gyakorlati megvalósítása, a potenciális veszélyek (hibás programozás, külső támadás stb.) felmérése és a károk mértékének megbecsülése a szakemberek számára is kihívást jelent. Ez felveti a mesterséges intelligencia kockázatértékelésében a másodlagos károk kezelésének kérdését, azaz emberi tevékenységből eredő hibák rendszerezését és kezelési módjainak feltérképezését, mint pl. az algoritmusok torzításai, a humán kognitív kapacitás korlátai[12].

A várható fejlődésben a szakértők technopesszimista álláspontja szerint a kompetitív motivációk dominanciája erősödik, azaz a gazdasági, hatalmi, biztonsági fölény megszerzése, háttérbe szoríthatja az etikai szempontokat, a humán értékeket, a demokratikus jogokat és az emberek a fizikai világ helyett a metaverzumokban találhatják meg a boldogulásukat. Annak ellenére, hogy számos nemzetközi szabályozás lépett életbe a mesterséges intelligencia humáncentrikus megvalósítására (pl. 2021-ben 193 ország elfogadta az Etikus Mesterséges Intelligenciára vonatkozó megállapodást [13]) a szakértők szerint ezek nem akadályozzák meg társadalom szempontjából veszélyes fejlesztéseket, önmagukban nem elegendőek, még szélesebb körű fellépés szükséges. A civil felhasználáson túl a honvédelemben és a nemzetbiztonsági területeken sem tartják megengedhetőnek a mesterséges intelligencia korlátok nélküli felhasználását, a vonatkozó jelenlegi, nemzetközileg érvényes szabályok, megállapodások etikai normáinak felülírását, az ellenség megsemmisítését. Ezen veszélyek elleni védekezésben kulcsfontosságúnak tartják a szakértők a mesterséges intelligenciával kapcsolatos széleskörű „társadalmasítást", szemléletformálást, oktatást, a folyamatos tudatosság fenntartását, ezáltal valósulhat meg az a társadalmi kontroll, amely az optimista jövőképet megalapozza. Minden résztvevő egyetértett abban, hogy a mesterséges intelligencia fejlesztésében, oktatásában elengedhetetlen az univerzális emberi értékek közvetítése és ezt saját munkájukban prioritásként kezelik. Bár Magyarország Mesterséges Intelligencia Stratégája 2020-2030 [14] átfogóan ismerteti a társadalom felkészítésére vonat-

kozó irányelveket és a várható munkaerő-piaci változásokat, a szakértők szerint már lemaradásban vagyunk a változásokra való felszülésben, nemcsak a disszeminációban, hanem a konkrét tervek és megvalósításuk területén is, különösen a robotizáció, automatizáció következtében kialakuló tömeges munkanélküliség kezelését szolgáló intézkedésekben, amelynek elmulasztása társadalmi szintű krízissé eszkalálódhat.

Az emberiség egy soha nem látott egzisztenciális kihívással néz szembe. A mesterséges intelligencia jelenlegi szintjén még nyitva áll mind a kooperatív mind a kompetitív koevolóció lehetősége, azaz „barátságos, megbízható, támogató" társ, vagy ellenség, amely egy szűk réteget szolgál ki, esetleg az emberi faj ellen fordul. A fejlődés iránya attól függ, hogy a mesterséges intelligenciával kapcsolatos társadalmi kontroll és a formális intézmények egymással összhangban képesek lesznek-e a közjó szolgálatába állítani.

FELHASZNÁLT IRODALOM

[1] Cseh-Szombathy L. és Ferge Zs. (szerk.), *A szociológiai felvétel módszerei*. Budapest: Közgazdasági és Jogi Könyvkiadó, 1971.
[2] B. Earl, *A társadalomtudományi kutatás gyakorlata*. Budapest: Balassi Kiadó, 2000.
[3] K. Krippendorff, *A tartalomelemzés kódszertanának alapjai*. Budapest: Balassi Kiadó, 1995.
[4] Horváth D. és Mitev A., *Alternatív kvalitatív kutatási kézikönyv*. Budapest: Alinea Kiadó, 2015.
[5] W. Gordon és R. Langmaid, *Kvalitatív piackutatás*. Budapest: HVG Kiadó, 1997.
[6] Langer K., *Kvalitatív kutatási technikák*. Gödöllő: Szent István Egyetemi Kiadó, 2009.
[7] K. N. Malhotra, *Marketingkutatás*. Budapest: KJK Kerszöv, 2002.
[8] P. A. Scipione, *A piackutatás gyakorlata*. Budapest: Springer Hungarica, 1984.
[9] Kollár Cs., *Reklám- és reklámszöveg kutatás*. Budapest: Protokollár Tanácsadó Iroda, 2004.
[10] Vicsek, L., *Fókuszcsoport*, Budapest, Osiris kiadó, 2006.
[11] Kollár Cs. „A szakértővé válás, illetve a szakértők kiválasztásának és megkérdezésének módszertani kihívásai" *VEZETÉSTUDOMÁNY* vol. 49:2 pp. 63-75., 2018, doi: 10.14267/VEZTUD.2018.02.07.
[12] D. G. Harkut, K. Kasat and V. D. Harkut, *Introductory Chapter: Artificial Intelligence - Challenges and Applications*. Artificial Intelligence - Scope and Limitations Edited by Dinesh G. Harkut 2019.: DOI: http://dx.doi.org/10.5772/intechopen.84624 (letöltés 2022.03.10.)
[13] UN News, *193 countries adopt first-ever global agreement on the Ethics of Artificial Intelligence*, 25 November 2021., https://news.un.org/en/story/2021/11/1106612 (letöltés 2022.03.10.)
[14] *Magyarország Mesterséges Intelligencia Stratégiája 2020-2030*, Mesterséges Intelligencia Koalíció, Digitális Jólét Program, Innovációs és Technológiai Minisztérium, https://digitalisjoletprogram.hu/hu/kiadvanyaink (letöltés 2022.03.10.)

QUALITATIVE SURVEY OF OCCUPATIONAL SAFETY PERFORMANCE AND ORGANIZATIONAL CULTURE IN MEDIUM AND LARGE ENTERPRISE ENVIRONMENT

MUNKAVÉDELMI TELJESÍTMÉNYMÉRÉS ÉS SZERVEZETI KULTÚRA KVALITATÍV FELMÉRÉSE KÖZÉP- ÉS NAGYVÁLLALATI KÖRNYEZETBEN

FARAGÓ Ferenc[1]

Abstract

Occupational health and safety performance measurement methods, which are already typically integrated into the management practice of medium-sized and large companies, are not uniform. The aim of the study is to assess the occupational safety organizational culture and occupational safety performance measurement practices of companies operating in Hungary, to identify the applied procedures, and to determine the accuracy of the metrics. The study was conducted using the method of qualitative research and expert interviews. Based on the results of the research, the characteristics and differences of the companies' occupational safety performance measurement practices were determined, as well as the assumptions on the basis of which further, detailed examination of the methods used to measure occupational safety performance and increase efficiency is proposed.

Keywords

performance measurement, occupational safety performance, occupational safety organizational culture

Absztrakt

A munkavédelmi teljesítménymérés a közepes- és nagyvállalatok menedzsment gyakorlatába már jellemzően beépült, a teljesítmény mérésére és nyomon követésére kialakult módszerek azonban nem egységesek. A tanulmány célja a Magyarországon működő vállalatok munkavédelmi szervezeti kultúrájának, munkavédelmi teljesítménymérési gyakorlatának felmérése, az alkalmazott eljárások azonosítása, a metrikák precizitásának meghatározása. A vizsgálat kvalitatív kutatás módszerével, szakértői interjúk segítségével történt. A kutatás eredményei alapján meghatározásra kerültek a vállalatok munkavédelmi teljesítménymérési gyakorlatának jellemzői, illetve különbségei, valamint megfogalmazásra kerültek azon feltételezések, amelyekre alapozva a munkavédelmi teljesítmény mérése és a hatékonyság növelése érdekében alkalmazott módszerek további, részletes vizsgálata javasolt.

Kulcsszavak

teljesítménymérés, munkavédelmi teljesítmény, munkavédelmi szervezeti kultúra

[1] farago.ferenc@uni-obuda.hu | ORCID: 0000-0001-6627-9604 | PhD Student, Óbudai University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A vállalati teljesítmény mérése és figyelemmel kísérése a hatékony vállalatvezetés meghatározó eszköze. A vállalatok bonyolult világában a döntéshozók számára a cég különböző egységeinek teljesítményét, illetve időben változásait mutatószámokkal leképzett adatok, úgynevezett kulcs-teljesítménymutatók teszik érthetővé, könnyen kezelhetővé. Közép- és nagyvállalatok jellemző gyakorlata a szervezet különböző folyamatainak nyomon követése, melynek révén a vezetők számára a szervezeti egységek minden fontosabb folyamatáról megfelelő információ áll a rendelkezésére. A teljesítmény folyamatos nyomon követése és értékelése nagymértékben megkönnyíti a döntéshozók munkáját, hozzásegíti a vezetőket ahhoz, hogy a folyamatokat figyelemmel kísérhessék és a vállalati céloknak megfelelő, megalapozott döntéseket hozzanak.

A különböző pénzügyi, gazdasági folyamatok mellett a munkakörülmények és a munkavédelem színvonala is hozzájárul a vállalat értékteremtő folyamataihoz. A munkavédelem az OHSAS 18001 szabvány magyar fordításával létrejött MSZ 28001:2003 A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR) című szabvány megjelenését követően került be a vállalatirányítási rendszerekbe. Az elmúlt közel 20 évben a vállalatok munkavédelemmel kapcsolatos folyamatai folyamatosan változtak, fejlődtek, egységes gyakorlat azonban nem alakult ki. Jelen tanulmány célja a Magyarországon működő közép- és nagyvállalatok munkavédelmi szervezeti kultúrájának tanulmányozása volt a teljesítménymérésre alkalmazott eljárások, illetve a munkavédelmi teljesítményt befolyásoló szervezeti tényezők felmérése révén.

SZAKIRODALMI ÁTTEKINTÉS

"Ha mérni tudjuk, amiről beszélünk, és számokkal kifejezni, akkor tudunk valamit róla; de ha nem tudjuk mérni, ha nem tudjuk számokkal kifejezni, akkor tudásunk szegényes és nem kielégítő." (Lord Kelvin, 1824-1907.) Lord Kelvin gondolatait alapul véve azt mondhatjuk, hogy ha valamilyen tevékenységet, folyamatot meg szeretnénk ismerni, elemezni, vagy értékelni, akkor mérnünk kell, számszerű adatokkal kell tudjuk kifejezni azt. Ez az alapja a vállalati teljesítménymérésnek is, mely mára az üzleti élet szerves része lett. A vállalatok környezete az elmúlt évtizedekben bonyolulttá vált, szerteágazó és kiterjedt – beszállítói, vevői, munkavállalói, alvállalkozói, állami és lakossági – kapcsolatrendszerrel. Folyamatosan követniük kell érintettjeik elvárásait, érdekeit és igényeit. Ennek megfelelően a vállalati folyamatok is összetetté váltak [1].

A gazdálkodó szervezetek célja az erőforrásaikkal való jó gazdálkodás, a működés optimalizálása úgy, hogy az a kitűzött célok teljesülését a leghatékonyabban biztosítsa. Végső soron, hogy a legjobb (pénzügyi) teljesítményt érjék el. A folyton változó piaci környezetben a teljesítmény mérése és nyomon követése a gazdasági siker elengedhetetlen feltétele lett. Az eredményes működéshez a vállalatoknak ismerniük és érteniük kell saját és környezetük működését. A vállalkozás által elért teljesítmény szintje az általa végzett tevékenységek hatékonyságának és eredményességének függvénye, ennek megfelelően a teljesítménymérés meghatározható a cselekvés hatékonyságának és eredményességének mérési folyamataként [2]. A teljesítménymérési rendszert úgy lehet meghatározni, mint a cselekvések hatékonyságának és eredményességének számszerűsítésére használt metrikák halma-

zát [3]. Wimmer [4] szerint az üzleti teljesítménymérés az értékteremtés, a vállalati teljesítmény fejlesztésének fontos támogatója. Ma is helytálló Wimmer [5] megállapítása, mely szerint „a sikeres vállalatokat az értékteremtő folyamatokat támogató teljesítménymérési gyakorlat jellemzi". A teljesítmény mérése tehát a teljesítmény menedzselésének, befolyásolásának feltétele. A megalapozott vezetői döntések támogatásához a szervezet működésére vonatkozó meghatározó információk szükségesek. A teljesítményt befolyásoló tényezők (értékteremtő tényezők) megértése és nyomon követése elengedhetetlen a sikerhez [5].

A vállalati teljesítménymérés ugyanakkor egy döntéstámogató eszköz, amely számszerű, értékelhető információt biztosít az érintetteknek a mért tevékenységekről, azok eredményességéről, állapotáról és trendjéről. A teljesítménymérés célja a vállalat különböző szintjein szükséges döntésekhez a megfelelő információ szolgáltatása, a vállalati célok teljesítésének nyomon követése, valamint az eredményesség értékelésének biztosítása. Célja továbbá a működésre vonatkozó releváns információk "láthatóvá tétele", kommunikálása a vállalat érintettjei felé. Wimmer [6] szerint a legátfogóbb értelmezést talán Neely és munkatársai [7] megfogalmazása biztosítja számunkra, mely szerint „az üzleti teljesítménymérés feladata a megalapozott döntések és cselekvések támogatása, azáltal hogy a megfelelő adatok összegyűjtésével, feldolgozásával, rendszerezésével, elemzésével és értelmezésével számszerűsíti a múltbeli cselekedetek hatékonyságát és eredményességét".

A nagyvállalatoknál végzett stratégiai tervezések során felismertük, hogy a fenntartható működéshez nagymértékben hozzájárul a munkavédelem is. A magyarországi vállalatok között 2019-ben végzett felmérés szerint a munkavállalók a munkahelyváltás egyik gyakori okaként a nem megfelelő munkakörülményeket jelölték meg [8]. A vállalatvezetők számára a fluktuáción felül a munkabalesetek is problémát jelentenek, hiszen ezek közvetlenül és közvetve is rontják a cég gazdasági mutatóit és a vállalatról alkotott képet.

Az egészséges és biztonságos munkahelyek kialakítása, a megfelelő, vonzó munkakörülmények biztosítása napjainkban már szintén a versenyképesség egyik feltétele. Hozzájárul például a munkaerő megtartásához, a fluktuáció csökkentéséhez, a minőségi munkaerő megszerzéséhez. A biztonságra való törekvések hosszú múltra tekintenek vissza. Az ipari forradalom korszakára jellemző rossz munkakörülmények javításától kezdve folyamatosan szélesedett a biztonsággal foglalkozók látóköre, ma pedig a biztonság már komplex műszaki tudományágnak tekinthető, mely vezetői, ergonómiai, pszichológiai és mérnöki tudományok ismeretét és alkalmazását igényli. Ennek megfelelően a termelési folyamatokhoz kapcsolódó hagyományos pénzügyi, termelési, logisztikai teljesítménymérés mellett a munkavédelmi teljesítmény mérése is a teljesítménymenedzsment részévé vált.

Napjainkban jellemző tehát, hogy modern vállalatvezetési eszközökkel a vállalatok működésének ellenőrzése folyamatosan biztosított, a vezetőség naprakész információkkal rendelkezik a vállalat teljesítményéről. A fejlett vezetési eszközök ellenére a munkavédelmi tevékenység jellemzően utólagos jellegű: egy-egy esemény bekövetkezése és a kiváltó okok elemzése után hozott intézkedésekkel próbálják a hasonló balesetek ismétlődését megakadályozni. A vállalat szempontjából a balesetek a termelést megzavaró tényezők, melyek egyrészről a költségeket növelik, másrészt pedig – bizonyos esetekben – jelentősen rontják a vállalatról alkotott képet. Függetlenül attól, hogy milyen szinten tart az adott vállalatnál a munkavédelem, és hol helyezkedik el a vállalat szervezeti struktúrájában, eredményességét nagymértékben meghatározza a szervezet vezetőinek támogatásán és elkötelezettségén túl

az, hogy a döntésekhez szükséges, megfelelő információk a vezetőség számára rendelkezésre állnak-e?

Szabó Gyula kiemeli a kockázatértékelés fontosságát, hangsúlyozva, hogy a jó kockázatértékelés biztosít alapot a megfelelő intézkedésekhez [9]. A kockázatértékelés alapja, hogy az események mögötti oksági összefüggések megismerése révén következtetni lehet a jövőre vonatkozóan, amennyiben a múltbéli eseményekkel és a vizsgált pillanatnyi állapottal kapcsolatos ismeretekkel rendelkezünk [9]. A különböző területek kockázatértékeléseinek összessége alakítja ki a vállalat pillanatnyi kockázati képét, amely nagymértékben befolyásolja a vezetői döntéseket.

A vállalat vezetőinek, döntéshozóinak valamilyen módon bizonyítani kell a meghozott intézkedések sikerességét, visszajelzést kell adni a szervezet működéséről, illetve annak hatékonyságáról. A megfelelő vezetői döntésekhez a vállalat helyzetét, aktuális állapotát leíró pontos információkra van szükség. Egyrészt ezek alapján tudja a vezetőség a meghatározott céloknak megfelelően irányítani a vállalatot, másrészt pedig ezek alapján tudja a cég sikerességét igazolni a felső vezetés, illetve a tulajdonosok felé. Mindezekhez tehát a vállalat működési paramétereinek folyamatos ismerete szükséges. Ennek eszköze a vállalati teljesítménymérés.

Neely és munkatársai [7] teljesítmény mérésre vonatkozó kutatásainak tükrében a munkavédelmi teljesítménymérés feladatát ekképpen definiálhatjuk: a vállalat munkavédelmi stratégiai céljainak meghatározásához szükséges információk biztosítása, a célok elérése érdekében hozott szervezési és műszaki intézkedések eredményességének nyomon követése és értékelése, valamint mindezen információk rendszerezése és megosztása az érintettekkel a munkavédelmi teljesítmény további javítása érdekében.

Az egészséges és biztonságos munkavégzéshez való jog Alaptörvénybe foglalt alapjog [10]. A munkavállalók e jogaikkal kapcsolatos érdekeik képviseletére jogosultak maguk közül képviselőt, vagy képviselőket választani [11]. A munkavédelmi érdekképviselet szintén fontos információ forrás lehet a vállalatvezetők számára. Szabó Imre doktori értekezésének bevezetőjében rámutat arra, hogy a munkaügyi kapcsolatokat Magyarországon „gyengülő szervezkedési szabadság és szakszervezeti jogok, egyre inkább kiüresedő (országos és ágazati) érdemi érdekegyeztetés, továbbá ellentmondásos szabályozási környezet jellemzi" [12]. Ennek megfelelően fontos a munkavédelmi teljesítmény menedzsmentje kapcsán az érdekképviseletek működésének eredményességét is vizsgálni.

MÓDSZERTAN

A kutatás célja a magyarországi vállalatok munkavédelmi szervezeti kultúrájának, munkavédelmi teljesítménymérési gyakorlatának felmérése, a teljesítménymérésre alkalmazott módszerek azonosítása, az alkalmazott metrikák precizitásának meghatározása. További célkitűzés a jellemző baleseti kockázatok és az azokat befolyásoló szervezeti tényezők meghatározása, illetve a vállalatok balesetek megelőzése érdekében tett intézkedéseinek megismerése.

Kutatásunk célkitűzései alapján az alábbi kutatási kérdéseket fogalmaztuk meg:

K1: Hogyan jellemezhető a szervezet munkavédelmi teljesítménymérésre kialakult gyakorlata?

K2: Milyen mutatószámokat használnak a munkavédelmi teljesítmény mérésére és ezeket hogyan (miből) képzik?

K3: A teljesítménymérés során mennyire törekszik precíz adatgyűjtésre a vállalat? Van olyan esemény, amely nem kerül be az értékelésbe (bejelentésre nem kötelezett baleset, kvázi balesetek stb.)?

K4: Irányítási rendszert működtetnek-e? Ha igen, melye(ke)t (MIR, KIR, MEBIR, egyéb)? A munkavédelmi teljesítménymérési folyamat hogyan jelenik meg a vállalat irányítási rendszerében?

K5: Integrált teljesítménymérés és –értékelés történik a vállalatnál, vagy az egyes szakterületek csak a saját mutatószámaikat követik nyomon?

K6: Hogyan működik a munkavédelmi érdekképviselet?

A vállalatirányítás területén végzett kvantitatív kutatások eredményei csak a kulcs teljesítménymutatókban megjelenő számszerű információkat rögzítik, de nem adnak lehetőséget a problémák, a folyamatok, a szervezeti és munkavállalói (individuális) viselkedés mélyebb megértéséhez [13]–[15]. Ennek kiküszöbölése érdekében kvalitatív kutatási módszerrel történő vizsgálatot láttunk szükségesnek a vállalati teljesítménymérést befolyásoló szervezeti folyamatok és emberi jelenségek megismerésére, az attitűdök, illetve az alkalmazott eljárások összegyűjtése és elemzése érdekében. Lampek és Horváthné [16] szerint a kvalitatív vizsgálatok lehetőséget biztosítanak a kutatott terület alapos, mélyreható felmérésére és „általában kis mintát alkalmaznak, melyekben nem cél a reprezentativitás". A kvalitatív kutatás egyik lényeges feladata az egyéni jellegzetességek kidomborítása [13].

Félig strukturált interjú elvégzése mellett döntöttünk. Kovács Interjús módszerek és technikák című fejezetében [17] leírtak szerint az ilyen mélyinterjús beszélgetés légköre nyitott, támogató, manipulációmentes [13]. Mint Kelemen rámutat: Seidman [18] szerint az interjúkészítés célja, hogy megértsük mások tapasztalatait és azt, ahogyan e tapasztalatokat értelmezik [13]. A kutatás során a vállalatoknál alkalmazott teljesítménymérési eljárások megismerése érdekében szakértői interjúkat alkalmaztunk. A munkavédelmi teljesítménymérési eljárás folyamatait ismerő és alkalmazó, illetve az adatokért felelős személyek jellemzően a vállalatok munkavédelmi szakemberei, illetve az adott terület vezetői. Ennek megfelelően a kutatást a szakterületek vezetőivel (munkavédelmi, illetve EHS menedzserek) folytattuk le.

A mintába kerülés feltételeként közepes- és nagyvállalati méretet határoztunk meg. A munkavédelmi teljesítménymérést 8 mélyinterjú alapján vizsgáltuk, mely 2 fővárosi és 6 vidéki telephellyel működő vállalati vezető vélekedéseit takarja. Az interjúk elemzésére tudományos analitikai módszereket, a beszámolók tartalomelemzését és grounded theory módszert alkalmaztunk, „mely vegyes módszertannak is megfeleltethető" [19]. Az alkalmazott kvalitatív adatelemzési eljárások biztosítják a kutatás tudományosságát [13], [14].

A koronavírus járvány terjedésének megakadályozása érdekében a vizsgálat időpontjában nem volt lehetséges a megkeresett interjú alanyokkal történő személyes találkozó. A vállalatok pandémiás intézkedési tervei a lehetséges kontaktok csökkentésének érdekében a külső partnerekkel, látogatókkal való személyes kapcsolatokat korlátozták. A járványügyi helyzetre való tekintettel a személyes interjúk online zajlottak, Skype, illetve Microsoft Teams felületen keresztül, videó beszélgetés formájában.

EREDMÉNYEK

A kutatás eredményeinek összegzése alapján megállapítható, hogy a vállalatok teljesítménymérési gyakorlatába beépült a munkavédelemmel kapcsolatos teljesítmény mérése. A vizsgált vállalatok különböző stratégiák szerint, de foglalkoznak a munkavédelmi teljesítmény nyomon követésével és fejlesztésével. A teljesítménymérésre és a munkavédelmi kultúrára ható folyamatok kölcsönhatásait az 1. sz. ábrán vázoltuk.

A munkavédelmi teljesítményméréshez az adatgyűjtés folyamatosan, a nyomon követés jellemzően havi gyakorisággal történik. A folyamatosság azt jelenti, hogy a belső eljárásoknak megfelelően a munkavédelemmel foglalkozó szakemberek a balesetekről azonnal értesítést kapnak. A szükséges intézkedéseket (elsősegély, balesetvizsgálat stb.) követően a baleset tényét és adatait a vállalati eljárás szerint regisztrálják. Az adatbázis alapján készítik el a vezetők számára a jelentéseket – ez a nyomon követés és teljesítményértékelés alapja. A vizsgált vállalatoknál a környezetvédelmi és munkavédelmi (EHS vagy SHE) felelős, vagy -osztály feladata az adatgyűjtés és a menedzsment felé történő jelentés. A balesetek kivizsgálását követő adatrögzítés eredményeit heti vezetői, illetve havi és éves felsővezetői nyomon követés során ellenőrzik a vezetők.

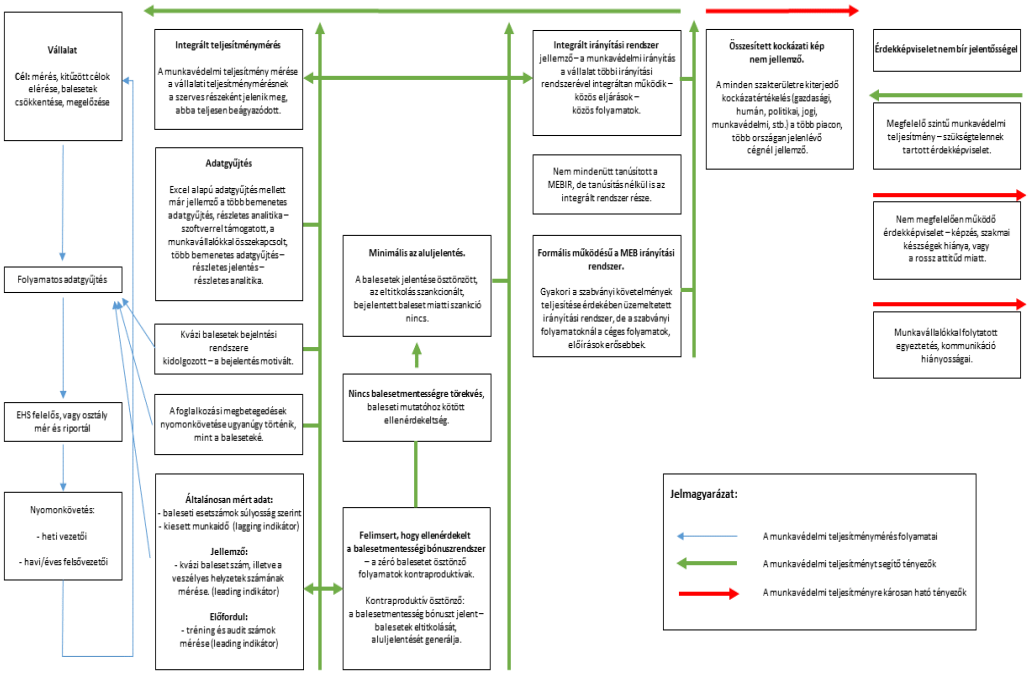
A teljesítménymérésre használt adatok és mutatószámok tekintetében nincs egységes gyakorlat. A munkavédelmi teljesítmény mérésére különböző teljesítménymutatókat használnak a vállalatok. Általánosan, minden vizsgált vállalatnál mért adat a baleseti esetszám (súlyosság szerint), illetve a kiesett munkaidő (óra). Ezek a lagging indikátorok a már bekövetkezett esetekre utalnak és minden vizsgált vállalat gyakorlatában előfordultak.

Jellemző a kvázi baleset szám, illetve a veszélyes helyzetek számának mérése. E két mutató leading, vagyis vezető indikátor, melyek tulajdonképpen előre jelzik a kockázatok megnövekedését. Az, hogy egyre több vállalat követi nyomon a kvázi baleseteket (angolul: near miss), azt jelzi, hogy hangsúlyos lett a proaktív, megelőző szemlélet. Ezt igazolja az is, hogy a vizsgált vállalatok esetében a kvázi balesetek bejelentési rendszere, illetve az erre vonatkozó eljárás kidolgozott, a munkavállalókat a bejelentésre motiválják.

Három vállalat esetében előfordult még a tréningek és auditok számának mérése is. Ezek szintén vezető mutatók, melyek a megelőzés érdekében tett erőfeszítéseket (oktatások, ellenőrzések) és ezek eredményeit mérik. A vizsgált vállalatok esetében a foglalkozási megbetegedések nyomon követése a baleseti eseményekhez hasonlóan történik.

A teljesítményméréshez szükséges adatokat a leggyakrabban valamilyen táblázatkezelő szoftver segítségével rögzítik, de az Excel alapú adatgyűjtés mellett a nagyobb multinacionális cégeknél már jellemző a több bemenetes adatgyűjtést, részletes analitikát támogató szoftveres környezet alkalmazása is. Ez tulajdonképpen kifejezetten erre a feladatra létrehozott célszoftver használatát jelenti, amely biztosítja a munkavállalókkal való közvetlen kapcsolatot, a több bemenetes adatgyűjtést. Vagyis a munkavállalók, illetve a területi vezetők a szoftver segítségével képesek a baleset, a kvázi baleset, illetve az észlelt kockázat adatait a rendszerbe rögzíteni és a munkavédelemért felelős személynek vagy osztálynak megküldeni. A szoftverbe a kivizsgálás eredményei és az intézkedések is rögzítésre kerülnek. Így minden eset pontosan nyomon követhető. További előny, hogy e szoftverek lehetővé teszik részletes jelentés és részletes analitikák elkészítését is. Ez a módszer egyrészt nagymértékben megkönnyíti az adatok rögzítését, másrészt pedig lehetőséget ad a munkavédelmi szakembereknek arra, hogy a baleseti adatokat részletesen elemezzék és meghatá-

rozzák a leggyakrabban előforduló eseteket, illetve azokat a munkahelyeket, vagy területeket, ahol legsűrűbben történnek események. Jó példa erre az SAP vállalatirányítási rendszer egyedi igény szerinti kibővítése a kutatásban részt vevő egyik nagyvállalat esetében, illetve az Ideagen vállalat „Safety management system" nevű szoftverének használata egy másik nagyvállalatnál. A kutatásba bevont vállalatok közül 4 használt célszoftvert a munkavédelmi esetek rögzítésére és analitikájára.



1. Ábra: A munkavédelmi teljesítménymérés kölcsönhatásai, saját szerkesztés.

Mint fentebb említettük a vizsgált vállalatok mindegyike foglalkozik a munkavédelmi teljesítmény mérésével és nyomon követésével. Vizsgálatunk kiterjedt arra is, hogy a munkavédelmi teljesítménymérés hogyan épül be a vállalati teljesítménymérési folyamatba: az irányítási rendszer szerves részeként, vagy önálló folyamatként jelenik-e meg.

A vizsgált vállalatoknál integrált teljesítménymérés történik, vagyis a munkavédelmi teljesítmény mérése a vállalati teljesítménymérésbe beágyazódott. Ennek jelentősége az, hogy nem elszigetelt folyamatként zajlik a munkavédelmi teljesítmény nyomon követése. A vállalati teljesítménymérés szerves részeként nagyobb vezetői figyelmet kap, de beépül a munkavállalók mindennapjaiba is, a teljesítmény javítása érdekében célokat határoznak meg és erőforrásokat rendelnek hozzá. A vállalatok teljesítménymérésének szerves részévé vált a munkavédelmi teljesítmény mérése és nyomon követése. Eltérő mutatószámok alkalmazásával, de a cégek figyelemmel kísérik a munkavédelmi teljesítményt.

A nulla baleset koncepciója megszűnni látszik. Erre az interjúk során kitértek a vállalatok, kiemelve, hogy a korábban jellemző balesetmentességi bónuszrendszert megszűntették, mert ellenérdekelté tette a munkavállalókat. A zéró balesetet ösztönző folyamatok

kontraproduktívak – a balesetmentesség bónuszt jelent, így a balesetek eltitkolását, aluljelentését generálja. A vizsgált vállalatoknál nincs tehát balesetmentességre törekvés, baleseti mutatóhoz kötött ellenérdekeltség. Ennek megfelelően a vállalatok minimális aluljelentésről számoltak be. A balesetek jelentése minden megkérdezettnél ösztönzött, az eltitkolás szankcionált, bejelentett baleset miatti szankció nincs. A cégek elszakadtak tehát a nulla baleset szemlélettől, a balesetmentességre törekvéstől, felismerve, hogy a balesetmentességre való ösztönzés a munkavédelmi teljesítmény szempontjából kontraproduktív, a nulla baleset víziója a balesetek eltitkolásával járhat. A munkavédelmi teljesítménymenedzsment gyakorlatában jóval nagyobb fontosságot kap a balesetek tényleges bejelentése és kivizsgálása, mint korábban.

A kockázatértékelés módszertana jól ismert a gazdasági és egyéb területeken. A munkavédelmi intézkedések alapját is a kockázatértékelés képezi. A kockázatértékelések általában az adott szakterületek vezetői számára biztosítanak lényeges információkat. Az összesített kockázati kép ugyanakkor a felsővezetés számára szolgáltat döntéseket megalapozó adatokat. Összesített kockázati térkép, tehát a vállalat különböző működési területén jelentkező kockázatokat egyesítő elemzés a vizsgálatban részt vevő vállalatok esetén nem volt jellemző. A minden szakterületre (gazdasági, humán, politikai, jogi, munkavédelmi stb.) kiterjedő kockázatértékelés egyedül a több piacon, több országban jelen lévő cégnél jellemző.

A Munkahelyi egészségvédelem és biztonság irányítási rendszerek (OHSAS, MEBIR) működését az elemzésben résztvevő vállalatok formálisnak tartják. Ennek magyarázata, hogy a szabványi követelmények teljesítése érdekében üzemeltetett irányítási rendszer követelményeinél, a szabványi folyamatoknál a céges folyamatok, előírások a legtöbb esetben erősebbek, magasabb elvárásokat támasztanak. Nem hagyhatjuk azonban figyelmen kívül az irányítási rendszereket, mivel ezek megadják a teljesítménymérés keretrendszerét. A legtöbb esetben integrált irányítási rendszer működik, vagyis a munkavédelmi irányítás a vállalat további irányítási rendszereivel (pl. minőségirányítási rendszer, környezetközpontú irányítási rendszer stb.) integráltan működik. Az integrált irányítási rendszerben a főbb eljárások és folyamatok közösek, csakúgy, mint a különböző szakterületek teljesítményének mérésére és a teljesítmény nyomon követésére vonatkozó szabályozások. Bizonyos elemek szakterületenként specifikusak, egyediek. A MEBIR a vizsgálatba bevont vállalatok nem mindegyikénél volt tanúsított (külső szervezet által ellenőrzött és értékelt), de így is az integrált rendszer része.

Az irányítási rendszerek háttere tehát nem jelent feltétlenül hozzáadott értéket, formális jellegűvé válnak a cégek erősebb szabályozása miatt. Szerepük a teljesítménymenedzsment szempontjából (figyelemmel kísérés és fejlesztés) bír jelentőséggel.

Fontos kérdés a munkavédelmi teljesítmény vizsgálatakor a munkavédelmi érdekképviseletek működése. Az érdekképviselet jogszabály által megfogalmazott célja, hogy hozzásegítse a munkáltatókat a biztonságos és az egészséget nem veszélyeztető munkahelyek kialakításához, részt vegyenek a munkavédelem mind szélesebb körű megismertetésében [11].

A vizsgálat eredményei alapján a nem megfelelően működő érdekképviselet a jellemző. Ennek okaként a képzés, a szükséges szakmai ismeretek hiányát, illetve a képviselők rossz attitűdjét jelölték meg a megkérdezett szakemberek. Két vállalat esetében a megfelelő

szintű munkavédelmi teljesítménnyel magyarázták azt, hogy a munkavállalók szükségtelennek tartják az érdekképviseletet. A munkavédelmi érdekképviseletek tehát nem, vagy nem jól működnek, illetve az érdekképviselet a munkavédelem tekintetében nem bír jelentőséggel. A munkavédelmi teljesítményhez hozzáadott értéke nem számottevő.

KÖVETKEZTETÉSEK, JAVASLATOK

A vizsgálat rámutat arra, hogy a Magyarországon működő közép- és nagyvállalatoknál a munkavédelmi teljesítménymérés a vállalati teljesítménymérési eljárások részévé vált. A kutatás kiterjesztésével célszerűnek látszik a munkavédelmi teljesítménymérés gyakorlatának szélesebb körű felmérése a jellemző vállalati nagyságrendek és a működtetett eljárások meghatározása érdekében. További kutatások segítségével javasolt a leggyakrabban alkalmazott mutatószámok felmérése és meghatározása. Hasonlóképpen javasolt a megelőzés érdekében kialakított módszertanok vizsgálata és eredményesség szempontjából történő értékelése.

Bár jellemző a balesetekkel kapcsolatos aluljelentés csökkentésére, illetve a balesetek bejelentésére való ösztönzés, de a kibővített kutatások során figyelmet kell fordítani a különböző teljesítménymérési módszerek adatgyűjtési metódusainak pontosságára. A munkavédelmi teljesítmény szélesebb körű vizsgálata során a munkavédelmi érdekképviseletek hozzáadott értékének meghatározására, illetve a működés megfelelőségének vizsgálatára is célszerű fókuszálni. Javasolt a munkavédelmi képviseletek működését jellemző mérőszámok kidolgozása.

ÖSSZEFOGLALÁS

Jelen kutatás célja a Magyarországon működő közép- és nagyvállalatok munkavédelmi szervezeti kultúrájának, munkavédelmi teljesítménymérési gyakorlatának felmérése, a teljesítménymérésre alkalmazott módszerek azonosítása, az alkalmazott metrikák precizitásának meghatározása volt. A kvantitatív kutatás eredményei rámutattak arra, hogy a munkavédelmi teljesítménymérés a menedzsment eljárások részévé vált. Az alkalmazott teljesítménymutatók és stratégiák különbözőek, de az elérni kívánt cél hasonló: a balesetek csökkentése, illetve megelőzése.

Az a tény, hogy a munkavédelmi teljesítmény növelése a vállalati törekvések eleme lett, a problémakör részletes vizsgálatára sarkall. A vizsgálat során megfogalmaztuk azokat a feltételezéseket, amelyek további vizsgálatával tervezzük meghatározni a munkavédelmi teljesítmény mérése és növelése érdekében alkalmazott módszereket. Ezek:

H1: A cégek elszakadtak a nulla baleset szemlélettől, a balesetmentességre törekvéstől (felismerve, hogy a nulla baleset víziója a balesetek eltitkolásával járhat).

H2: A balesetmentességre való ösztönzés kontraproduktív.

H3: A munkavédelmi teljesítménymenedzsment gyakorlatában jóval nagyobb fontosságot kapott a balesetek tényleges bejelentése és kivizsgálása, mint korábban.

H4: Az irányítási rendszerek háttere nem jelent feltétlenül hozzáadott értéket, formális jellegűvé válnak a cégek erősebb szabályozása miatt.

H5: A munkavédelmi érdekképviseletek általában nem, vagy nem jól működnek. A munkavédelmi teljesítményhez hozzáadott értéke nem jelentős.

H6: Összesített kockázati kép nem jellemző.

A tanulmány végén meghatároztuk a további lehetséges kutatási irányokat és javaslatot tettünk a kutatás kibővítésére.

IRODALOMJEGYZÉK

[1] L. Sajtos, "A vállalati marketingteljesítmény értékelésének többdimenziós megközelítése és alkalmazása a Magyarországon működő vállalatok körében," *Vezetéstudomány*, vol. XXXVII., no. 3., pp. 18–30, 2006.

[2] A. Neely, M. Gregory, and K. Platts, "Performance measurement system design: A literature review and research agenda," *Int. J. Oper. Prod. Manag.*, vol. 25, no. 12, pp. 1228–1263, 2005, doi: 10.1108/01443570510633639.

[3] K. Neely, A., Gregory,M., Platts, "Performance measurement system design.," *International Journal of Operations & Production Management*, vol. 15, no. 4. pp. 80–116, 1995.

[4] Á. Wimmer, "Teljesítménymérés: az üzleti kapcsolatok értékelése , fejlesztése, menedzsmentje," vol. 489. Budapesti Közgazdaságtudományi és Államigazgatási Egyetem Vállalatgazdaságtan tanszék H, Budapest, pp. 1–19, 2004.

[5] Á. Wimmer, "A vállalati teljesítménymérés az értékteremtés szolgálatában A működési és a pénzügyi teljesítmény kapcsolatának vizsgálata," Budapesti Közgazdaságtudományi és Államigazgatási Egyetem, 2000.

[6] Á. Wimmer, "Üzleti Teljesítménymérés," vol. 489. Műhelytanulmányok Vállalatgazdaságtan Tanszék Veres Pálné u. 36. H-1053 Hungary, Budapest, pp. 1–48, 2002, [Online]. Available: http://edok.lib.uni-corvinus.hu/35/1/Wimmer17.pdf.

[7] A. Neely, C. Adams, and M. Kennerley, "The Performance Prism: The Scorecard for Measuring and Managing Business Success," *Cranf. Sch. Manag.*, no. January 2002, pp. 159–160, 2002.

[8] P. J. A. Imrich, Csapó I., Karácsony P., Kovács Á., "A magyarországi munkaerőpiac átalakulásának okai egy hazai empirikus kutatás tükrében," *Opus Educ.*, vol. 7, no. 4, 2020, [Online]. Available: http://www.opuseteducatio.hu/index.php/opusHU/article/view/407/709.

[9] Szabó Gyula, "A munkavédelemi kockázatkezelés sajátosságai," *Bánki Közlemények*, vol. 3, no. 1, pp. 5–12, 2020.

[10] "Magyarország Alaptörvénye (2011. április 25.)," 2011. https://net.jogtar.hu/jogszabaly?docid=a1100425.atv (accessed Sep. 25, 2021).

[11] "1993. évi XCIII. törvény a munkavédelemről," 1993. https://net.jogtar.hu/jogszabaly?docid=99300093.tv (accessed Sep. 25, 2021).

[12] I. Szabó, "A szakszervezet jogállása a magyar munkajogban," Pécsi Tudományegyetem Állam - és Jogtudományi Kar Doktori Iskola, 2021.

[13] A. Kelemen-Erdős, Anikó ; Mitev, "Tematikus szolgáltatásélmény art- és romkocsma környezetben," *Tur. és Vidékfejlesztési Tanulmányok*, vol. 2, no. 3, pp. 58–73, 2017.

[14] A. Kelemen-Erdős and A. Molnár, "Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units," *Econ. Cult.*, vol. 16, no. 1, pp. 58–69, 2019, doi: 10.2478/jec-2019-0007.

[15] A. Kelemen-Erdős, "Dead-end development or real progress? Paradigm shift

initiatives in marketing theory.," vol. XV, no. 1, pp. 26–38, 2019.
[16] I. Boncz, *Kutatásmódszertani alapismeretek*. Pécsi Tudományegyetem Egészségtudományi Kar, 2015.
[17] Feischmidt Margit, "Kvalitatív módszerek az empirikus társadalom és kultúrakutatásban," 2006. http://mmi.elte.hu/szabadbolcseszet/mmi.elte.hu/szabadbolcseszet/index72c4.html?option=com_tanelem&id_tanelem=835&tip=0. (accessed Sep. 12, 2021).
[18] Irving Seidman, "Az interjú mint kvalitatív kutatási módszer." Műszkai könyvkiadó, Budapest, 2002, doi: 963162756X.
[19] Neulinger Ágnes, "Több-módszertanú és vegyes módszertanú kutatások," *Vezetéstudomány*, no. XLVII. évf., pp. 63–66, 2016, [Online]. Available: http://unipub.lib.uni-corvinus.hu/2353/1/VT2016n4p63.pdf.

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