ISSN 2676-9042

Vol 2, No 3, 2020.

2020, II. évf. 3. 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
**ÉZSIÁS István**
sculptor/szobrászművész
**Constructive sculpture** | **Konstruktív plasztika**
statue | című szobra 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 |
| 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 |
| 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, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.

**A folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.

**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.

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

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.

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.

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 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 2, No 3, 2020.** | **2020. II. évf. 3. szám**

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

## BABOS Tibor

babos@uni-obuda.hu

Tibor Babos is the founding director of Szent István University, Szent István Safety Research Center and associate professor of the Faculty of Mechanical Engineering, Honorary University Professor of the University of Óbuda, Founding Director of the Security Science Center and Founding Director of the Security Science College, Thesis Supervisor and Teacher of the Doctoral School of Security Sciences, and a university professor at the National University of Public Administration, a lecturer and supervisor at the Doctoral School of Military Sciences and the Doctoral School of Public Administration. As Colonel of the Defense Forces, he is a Chief Military Adviser in the Ministry of Defense, specializing in security, defense and military policy.

Babos Tibor a Szent István Egyetem, Szent István Biztonságkutató Központ alapító igazgatója és a Gépészmérnöki Kar egyetemi docense, az Óbudai Egyetem címzetes egyetemi tanára, a Biztonságtudományi Központ alapító igazgatója és a Biztonságtudományi Szakkollégium alapító igazgatója, a Biztonságtudományi Doktori Iskola témavezetője és tanára, valamint a Nemzeti Közszolgálati Egyetem egyetemi magántanára, a Hadtudományi Doktori Iskola és a Közigazgatás-tudományi Doktori Iskola oktatója és témavezetője. Honvéd ezredesként a Honvédelmi Minisztériumban katonai főtanácsadó, szakterülete a biztonság-, védelem- és katonapolitika.

## BESZÉDES Bertalan

beszedes.bertalan@amk.uni-obuda.hu

Bertalan Beszedes (1988) electrical engineer, mechatronics engineer, currently enriching his knowledge at the Doctoral School of Safety and Security Sciences on University of Óbuda. His field of research is high-reliability hybrid electronic circuits in the field of embedded systems. He is an assistant professor at the Óbuda University, Alba Regia Technical Faculty, Institute of Engineering.

Beszédes Bertalan (1988) villamosmérnökmérnök, okleveles mechatronikai mérnök, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit. Kutatási területe a nagy megbízhatóságú hibrid elektronikus áramkörök a beágyazott rendszerek területén. Az Óbudai Egyetem Alba Regia Műszaki Karán a Mérnöki Intézet egyetemi tanársegédje.

## JACKOVICS Péter

peter.jackovics@katved.gov.hu

Firefighter Colonel Péter Jackovics PhD, civil protection counselor, Head of Department for Emergency Management, National Directorate General for Disaster Management (NDGDM), Ministry of the Interior, has two decades of professional experience in domestic and international disaster relief and assistance. He is the commander of HUNOR. He led the governmental rescue team in Srí Lanka, Indonesia, Haiti, Ukraine, Malta and Serbia. He is Hungary's UNDAC expert. As deputy head of the EU civil protection team, he directed the assistance granted by EU countries to Japan. Under his leadership, the basic professional requirements, the National Classification System for voluntary rescue organizations to be deployed in rescue operations have been elaborated in the six different branches of

Dr. Jackovics Péter tűzoltó ezredes, tanácsos, a BM Országos Katasztrófavédelmi Főigazgatóság Vészhelyzet-kezelési Főosztály vezetője. Két évtizedes szakmai tapasztalattal rendelkezik a hazai és nemzetközi katasztrófa- és humanitárius segítségnyújtásban. Ellátja Magyarország központi mentőszervezetnek, a HUNOR parancsnoki teendőit. Kormányzati mentőcsapatot vezette Srí Lanka, Indonézia, Haiti, Ukrajna, Málta és Szerbia nemzetközi segítségkérése alkalmával. Magyarország ENSZ Katasztrófa-becslő és Koordinációs (UNDAC) szakértője. Az Európai Unió polgári védelmi csoportjának helyetteseként irányította az EU-tagországok Japánnak nyújtott támogatását. Magyarországon, Vezetése alatt a mentési műveletek hat különböző ágazatában kidolgozták az alapvető szakmai követelményeket, a mentési

rescue. He has a doctoral degree on the Safety and Security Science of the Óbuda University. His area of research is the Technical Rescue Operations and for that Preparation for Disaster Management Exercises with Applied Mathematical and Psychological Approach.

műveletekben bevezetendő önkéntes mentőszervezetek nemzeti minősítő rendszerét. Doktori fokozatot szerez az Óbudai Egyeteme Biztonságtudományi Doktori Iskolában. Kutatási területe a különleges mentések és az arra felkészítő katasztrófavédelmi gyakorlatok vizsgálata alkalmazott matematikai és pszichológiai megközelítéssel.

**KOLLÁR Csaba**

kollar.csaba@phd.uni-obuda.hu

Communications engineer, certified communications specialist, head of electronic information security, doctor of economics (PhD), 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, and social credit system, domotics. He is an associate professor at the Óbuda University, lecturer and supervisor at the National University of Public Service Doctoral School of Military Engineering. He is a registered mediator of the Ministry of Justice, and 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 is currently expanding his knowledge at the Doctoral School on Safety and Security Sciences at Óbuda University. He has been a member of the Artificial Intelligence Consortium since Q4 2018.

Kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), 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 egyetemi docense, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, témavezetője. Az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), elnök a szakmai képesítő vizsgákon (OKJ). A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

**KUN Tamás**

kun.tamas@phd.uni-obuda.hu

Economist in Business Development. PhD student of Óbuda University, Doctoral School of Safety and Security Sciences. In his research, he studies the issues of social engineering, cybersecurity, critical infrastructures and geopolitics. His research topic title is “Significance and geopolitical effects of Social Engineering”.

Okleveles közgazdász, vállalkozásfejlesztés szakon. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területén belül a pszichológiai manipuláció, a kiberbiztonság, a kritikus infrastruktúrák, valamint a geopolitika kérdéseit vizsgálja. Kutatási témájának címe: „A pszichológiai manipuláció jelentősége és geopolitikai hatásai”.

**LIEBMANN Gábor**

liebmann.gabor@gmail.com

PhD student at the Doctoral School of the Safety and Security Sciences at the Óbuda University in Budapest, Hungary. Electrical engineer (1996) and after it he graduated and finished his master studies at OE as

Az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatója. Villamosmérnök (1996), okleveles biztonságtechnikai mérnök. Kutatási területe a komplex vagyonvédelmi rendszerek hatékonysága,

security engineer. His research topic is the measurment of the efficiency in the complex security systems. Deputy director the Safety and Security Directorate of Semmelweis University.

illetve azok objektív mérésének lehetősége és a rendszerek üzemeltetése. A Semmelweis Egyetem Biztonságtechnikai Igazgatóságának igazgató-helyettese.

**MOLNÁR Ferenc**

molnar.ferenc@phd.uni-obuda.hu

Electrical processing engineer, certified electrical engineer, certified economist, nuclear power plant operation specialist engineer. He works for MVM Hungarian Electricity Ltd. by head of sustainable production team. Head of Commissioning and project manager during significant domestic power plant investment works (large power plant reconstructions, new power plant implementations). He is a priority-project manager during the 20-year lifetime extension of the Paks Nuclear Power Plant. Managing Director of MVM Energy Romania Ltd. Management of the permitting and construction of the first solar power plants over 20MWp capacity in Hungary (Felsőzsolca, Paks) as a project manager. 2019. MVM Group Man of the Year award. Invited presenter of professional organizations (IIR, MNNSZ, MEE…). He is invidet lecturer at the University of Óbuda Donát Bánki Faculty of Mechanical and Safety Engineering, Kálmán Kandó Faculty of Electrical Engineering and Keleti Faculty of Business and Management. He is currently a student of the Doctoral School on Safety and Security Sciences at Óbuda University. His research interests include the security of electricity supply in Hungary, especially the issue of carbon-free sources.

Villamos üzemmérnök, okleveles villamosmérnök, okleveles közgazdász, atomerőmű üzemeltetési szakmérnök. Az MVM Magyar Villamos Művek Zrt. fenntartható termelési csoportvezetője. Jelentős hazai erőmű beruházási munkák (nagyerőművi rekonstrukciók, új erőmű létesítések) során üzembehelyezési vezető, projektvezető. A Paksi Atomerőmű 20 éves üzemidő hosszabbítása során kiemelt projektvezető. Az MVM Energy Románia Ltd. ügyvezetője. Magyarországon az első 20MWp feletti naperőművek (Felsőzsolca, Paks) engedélyeztetésének és létesítésének irányítása projektvezetőként. 2019. az MVM csoport év embere díj. Szakami szervezetek (IIR, MNNSZ, MEE…) meghívott előadója. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, a Kandó Kálmán Villamosmérnöki Kar és a Keleti Károly Gazdasági Kar meghívott előadója. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója. Kutatási területe Magyarország villamosenergia-ellátás biztonsága, különös tekintettel a karbonmentes források kérdése.

**UJHEGYI Péter**

ujhegyi.peter@phd.uni-obuda.hu

With medium to large enterprise use over the past 20 years, IT operations and IT Security are focused on teams of 5-25 people. I designed and implemented the management of the international services of the service providers, the managing nationwide network of service partners, Fujitsu-Siemens takes care of, developed and operated the IT system in the corporate and financial sector, built biometric products and transformed the partner network. With a plethora of product and service selection and management projects, technical solutions for its design and operational responsibilities are being developed in the development project of Hungary's first road insurance technology system, which is behind us.

Az elmúlt 20 évben közép és nagyvállalati területen IT üzemeltetés és IT Biztonság fókusszal vezettem 5-25 fős csapatokat. Megterveztem és bevezettem outsourcing szolgáltatást nemzetközi cégnél, vezettem országos lefedettségű szervizpartneri hálózatot a Fujitsu-Siemens részére, fejlesztettem és üzemeltettem nagyvállalati és pénzügyi szektorban IT rendszereket, építettem biometriával kapcsolatos termék mögé viszonteladói partneri hálózatot. Rengeteg termék és szolgáltatás kiválasztási és bevezetési projecttel a hátam mögött jelenleg épp Magyarország első cross-country insure-tech rendszerének fejlesztésének projectjében a technikai megoldások tervezéséért és az üzemeltetésért felelek.

**ZAKAR Ákos**

zakarakos85@gmail.com

Graduating as an economist, Ákos Zakar earned his second degree in information security. Besides the CEH certificate, he has an ISMS's auditor, Risk manager as well as Incident manager TÜV qualifications, too. As beginner he worked in the private security field, after this he had been serving his country in the field of law enforcement for 13 years. After facility and public order protection, he also worked in detective and analyst positions. In the course of his criminal work, he tasked with detection and investigation against life and property cases, as well as crimes committed using and against the IT system. As a professional recognition, he was awarded by one of the biggest domestic financial institutions. Furthermore a report was made with him by the television show 'Kékfény' on the topic of credit card fraud series. Continuing his experience at the Police, he is working as an information security expert at the a State owned economic company. The human role of information security in preventing attacks against social engineering is his research field.

Zakar Ákos közgazdász diplomája után a másodikat információbiztonságból szerezte. Certified Ethical Hacker tanúsítványa mellett, Információbiztonsági Irányítási Rendszer auditor, Kockázatkezelő valamint Incidensmenedzsment TÜV minősítései is vannak. Pályakezdőként a vagyonvédelemben helyezkedett el, majd 13 évig a rendvédelem területén szolgálta hazáját. Az objektumvédelem és közrendvédelem után nyomozó majd elemző beosztásokban is dolgozott. Munkája során számos élet és vagyon elleni, valamint informatikai rendszer felhasználásával és ellenük elkövetett bűncselekmények felderítése, vizsgálata volt a feladata. Szakmai elismerésként az egyik legnagyobb hazai pénzintézet jutalomban részesítette, valamint a Kékfény című televíziós műsorban is készült vele egy riport, bankkártyás csalássorozatok témájában. A Rendőrségnél szerzett tapasztalatát követően jelenleg egy állami tulajdonú gazdasági társaságnál dolgozik, információbiztonsági szakértő pozícióban. Kutatási területe az információbiztonság humán szerepe, a social engineering elleni támadások megelőzésében.

**ZÁHONYI Lajos**

zahonyi.lajos@phd.uni-obuda.hu

Corporate management and controlling economist, operations manager, project manager, quality- and information security manager and auditor. He is currently a PhD student at the Doctoral School of Security Sciences of the University of Óbuda. Research interests: Developmental history of information security, systems of reference tools and information security aspects of Enterprise Resource Planning (ERP) systems.

Vállalatirányítás és kontrolling szakközgazdász, operatív vezető, projektmenedzser, minőségirányítási- és információbiztonsági vezető és auditor. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területe: Az információbiztonság fejlődéstörténeti vizsgálata, viszonyulási eszközrendszerei és a vállalatirányítási rendszerek információbiztonság szempontú aspektusai.

| 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 2, No 3, 2020. | 2020. II. évf. 3. szám**

## CONTENT | TARTALOM

# STRENGTHENING EUROPEAN DISASTER RESPONSE CAPACITIES: THE RESCEU

# AZ EURÓPAI KATASZTRÓFA-BEAVATKOZÁSI KÉPESSÉGEK ERŐSÍTÉSE: A RESCEU

JACKOVICS Péter [1]

**Abstract**

The Union Civil Protection Mechanism ('the Union Mechanism') set out in Decision No 1313/2013/EU strengthens cooperation between the Union and the Member States and facilitates coordination in the field of civil protection in order to improve the Union's response to natural and man-made disasters. Decision No 1313/2013/EU defines the legal framework of rescEU. RescEU aims to provide assistance in overwhelming situations where overall existing capacities at national level and those committed by Member States to the European Civil Protection Pool are not able to ensure an effective response. In recent years there has been a sharp increase in the number of extreme forest fires in Europe with serious economic, environmental and social consequences. In particular, the 2017 and 2018 forest fire seasons demonstrated the need to be prepared when disasters severely and simultaneously affect several Member States. The author has been analysed the documents which are published so far on the topic and summarizes the essential elements of rescEU capacities.

**Keywords**

rescEU, HUNOR, civil protection mechanism, forest fire, Disaster Management

**Absztrakt**

Annak érdekében, hogy az Unió jobban tudjon válaszolni a természeti és az ember okozta katasztrófákra, az 1313/2013/EU határozattal létrehozott uniós polgári védelmi mechanizmus (a továbbiakban: uniós mechanizmus) megerősíti a tagállamok és az Unió közötti együttműködést és elősegíti a koordinációt a polgári védelem területén. Az 1313/2013/EU határozat meghatározza a rescEU jogi keretét. A rescEU célja az olyan kezelhetetlen helyzetekben való segítségnyújtás, amelyekben a tagállami szinten meglévő és a tagállamok által az európai polgári védelmi eszköztár céljára rendelkezésre bocsátott képességek összessége nem elegendő a hatékony beavatkozás biztosításához. Az elmúlt években jelentősen megnőtt Európában a kivételesen súlyos erdőtüzek száma, és ezek komoly gazdasági, környezeti és társadalmi következményekkel jártak. Különösen a 2017. és a 2018. évi erdőtüzek mutattak rá annak szükségesség. A szerző a témában eddig megjelent dokumentumokat rendszerezi és összegezi a rescEU-képesség lényegi elemeit.

**Kulcsszavak**

rescEU, HUNOR, polgári védelmi mechanizmus, erdőtűz, katasztrófavédelem

[1] peter.jackovics@katved.gov.hu | ORCID: 0000-0002-1809-029X| head of department/főosztályvezető| BM Országos Katasztrófavédelmi Főigazgatóság

## AZ UNIÓS POLGÁRI VÉDELMI MECHANIZMUS

Az uniós polgári védelmi mechanizmust 2001-ben hozták létre azzal a céllal, hogy javítsa az EU válaszadási képességét az olyan természeti és ember okozta katasztrófákra, mint például a futótüzek, az áradások, a tengeri szennyezés, a földrengések, a hurrikánok és az ipari balesetek. Az uniós polgári védelmi mechanizmus önkéntes kölcsönös segítségnyújtási rendszeren és a tagállamok által felkínált, előzetesen rendelkezésre bocsátott képességen nyugszik. Az EU feladata, hogy összehangolja és kiegészítse a katasztrófák megelőzésére, valamint az azokra való felkészülésre és mentésekre irányuló nemzeti fellépéseket. A 2017. és 2018. évi erdőtüzek azonban rávilágítottak az önkéntes megközelítés korlátjaira azokban az esetekben, amikor összetett és visszatérő katasztrófákra kell hatékonyan reagálni [1].

Annak érdekében, hogy hatékonyabban tudja megvédeni polgárait, nem utolsósorban terrortámadás vagy vegyi, biológiai, radiológiai vagy nukleáris baleset esetén, az EU úgy döntött, hogy egy közös európai forrástartalék, a „rescEU" létrehozásával megerősíti az Európai Unió (EU) mentési (angolul: rescue, ebből Rescue+EU=RescEU) képességét. Ez a lehetőség végső eszközként, az EU-tagállamok által nemzeti szintű (uniós terminológiában: „polgári védelmi", itthon a hazai használatban: „katasztrófavédelmi") a katasztrófareagálásra önkéntesen felajánlható tartalékok kimerítését követően kerül felhasználásra. A rescEU képesség (1) egészségügyi személyzetből, illetve tábori kórházakból, (2) tűzoltó repülőgépekből, (3) nagyteljesítményű vízszivattyúkból és földrengés sújtotta térségben bevethető (4) városi kutató- és mentőegységekből áll. A rescEU-képességeknek a tagállamok adnak otthont, és az EU bizonyos feltételek mellett társ finanszírozza azokat. A továbbfejlesztett uniós polgári védelmi mechanizmus célja a katasztrófák megelőzése és a katasztrófák következményeire való felkészültség javítása, segítve ezzel az EU-tagállamokat [1]. Az európai polgári védelmi képesség-lista és szakértői tudáshálózat kidolgozása ösztönözi a EU-tagállamok, így akár Magyarország, Visegrádi 4 országok együttműködését a képzés, a kutatás és az innováció terén, valamint a bevált gyakorlatok cseréjét [2].

A mechanizmus tényleges célkitűzései a következők [10]:

- a katasztrófák elleni védelem magas szintjének elérése az alábbiak révén:
  - a katasztrófák lehetséges hatásainak megelőzése vagy csökkentése,
  - a katasztrófa-megelőzés kultúrájának elősegítése; és
  - a polgári védelmi és más szervezetek közötti együttműködés javítása;
- a katasztrófa-segítségnyújtás területén a felkészültség növelése nemzeti és az EU szintjén,
- a gyors és hatékony mentés/beavatkozás elősegítése katasztrófák vagy várható katasztrófák esetén, többek között a katasztrófák közvetlen következményeinek felszámolására irányuló intézkedések meghozatala révén;
- a nyilvánosság tájékoztatásának és a katasztrófákra való felkészültségének a fokozása;
- a katasztrófákra vonatkozó tudományos ismeretek rendelkezésre állásának és felhasználásának növelése; és
- a határokon átnyúló, továbbá az azonos típusú katasztrófák által veszélyeztetett tagállamok közötti együttműködési és koordinációs tevékenységek fokozása.

**Jogalap, szubszidiaritás és arányosság uniós elve, pénzügyi keret [13]**

Az uniós polgári védelmi mechanizmust azért hozták létre, mert a súlyos katasztrófák meghaladhatják bármely egyedül fellépő tagállam mentési vagy beavatkozási képességeit. A mechanizmus középpontjában a tagállamok közötti jól összehangolt és gyors kölcsönös segítségnyújtás áll.

A koherencia és az egyszerűsítés biztosítását célzó polgári védelmi mechanizmus további lehetőségeket is előirányoz a katasztrófákra való felkészülés és az azok való reagálás együttes képességének megerősítésére. Ez különösen jelentős egy vagy több katasztrófa esetén, amelyek olyan hatásokkal járnak, amelyek egy időben több tagállam kapacitását haladják meg, és megbénítják közöttük a kölcsönös segítségnyújtást. Hasonló a helyzet az olyan kapacitások esetében is, amelyekre az alacsony valószínűségű, de nagy hatású jelentős katasztrófa esetén lenne szükség. Ilyen esetekben egyértelmű, hogy a tagállamok önmagukban nem képesek megfelelően reagálni, ezért az Európai Unió működéséről szóló szerződés 196. cikkével összhangban a tagállami fellépés támogatásához és kiegészítéséhez uniós támogatás szükséges.

Az 1313/2013/EU határozat 19. cikke szerint az uniós mechanizmus végrehajtásának pénzügyi keretösszege a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi keret időszakában 368,4 millió euró. Ez az összeg a 3. fejezetből (Biztonság és uniós polgárság) származó 223,8 millió euró és a 4. fejezetből (Globális Európa) származó 144,6 millió euró összegű hozzájárulásból tevődik össze. Ezenkívül az adminisztratív és emberi erőforrásokkal kapcsolatos költségeket az 5 fejezet szerint finanszírozzák, összesen 52,5 millió euró értékben.

**Klímaváltozás és szélsőséges időjárás hatása**

A globális klíma változás okozta légköri melegedés hatására évről-évre erdőtüzek pusztítanak Európa-szerte, melyeknek több ezer hektárnyi erdő esik áldozatul. Noha Dél-Európában magasabb a kockázat, erdőtüzek bármelyik európai országban előfordulhatnak [6].

Európa-szerte erdőtüzek tomboltak Portugáliában, Horvátországban, Franciaországban és Görögországban, a Brit-szigeteken az Ophelia nevű hurrikán söpört végig, Németországban pedig árvizek okoznak rendszeresen súlyos gondokat. A természeti katasztrófák súlyos gazdasági következményekkel is járnak. 1980 óta az uniós tagállamok a szélsőséges időjárási események miatt – az emberéleteken kívül – a Bizottság adatai szerint több mint 360 milliárd euró veszteséget szenvedtek. Egyedül Portugáliában közel 600 millió eurót tesz ki az a közvetlen gazdasági kár, amit a június és szeptember között bekövetkezett erdőtüzek okoztak. Ez az ország bruttó nemzeti jövedelmének 0,34 százalékát jelenti [5].

**Az erdőtüzek közös, uniós szintű kezelése**

Az Európai Unió tagállamaiban az elmúlt években sok halálos áldozatot követelő erdőtűz pusztított. A tűzesetek következtében több száz ember vesztette életét, és több milliárd euró összegű kártérítést regisztráltak.

Gyakran előfordul, hogy amikor egy erdőtűz léptéke meghaladja az adott ország oltási képességét, az uniós tagországok a szolidaritás jegyében segítséget nyújtanak: tűzoltó

repülőgépeket, helikoptereket, földi tűzoltási képességet, humanitárius segélyeket és szakembereket bocsátanak rendelkezésre. Európai szinten az ilyen segítségnyújtás strukturáltan történik. A Veszélyhelyzet-reagálási Koordinációs Központ (ERCC) az Európai Bizottság központi reagálási egységeként működik. Az Európai Unió polgári védelmi mechanizmusának egy érintett tagállam általi aktiválásakor az ERCC összehangolja az európai szintű segítségnyújtást, és biztosítja, hogy az hatékony és eredményes módon történjen. Az Európai Bizottság tehát összehangolja, illetve társ finanszírozza az érintett területre irányuló segítségnyújtást [6].

**Uniós polgári védelmi mechanizmus aktiválása és az erdőtüzek**

Az uniós polgári védelmi mechanizmust 2017-ben az Európában kitört erdőtüzek megfékezése céljából 18 alkalommal aktiválták. Az erdőtüzekre való reagálás céljából létrehozott mechanizmuson keresztül Portugália, Olaszország, Montenegró, Franciaország és Albánia kapott támogatást. Az uniós polgári védelmi mechanizmus keretében egy ízben a chilei kormány is segítséget kért. A portugál, spanyol és francia segítség mellett az Unió kilenc tagú polgári védelmi szakértői csapatot küldött Chilébe, hogy segítsen megbirkózni az ország történelmének legsúlyosabb erdőtüzeivel [6].

A mechanizmust 2018-ban 5 alkalommal aktiválták az európai erdőtüzek esetében – 2 alkalommal Svédország, egyszer pedig Portugália, Görögország és Lettország esetében. Összességében az EU 15 repülőgépet, 6 helikoptert, több mint 400 tűzoltót és legénységet, valamint 69 járművet bocsátott rendelkezésre. Az EU Kopernikusz katasztrófakezelési szolgáltatásának műholdas térképkészítő programját szintén több alkalommal igénybe vették, hogy az erdőtüzek oltására hatékonyan és gyorsan reagáljanak. Csak 2018-ban 139 műholdas térkép segítette az EU-t és a tagállami hatóságokat abban, hogy azonosítsák és értékeljék a leginkább érintett helyszíneket, megállapítsák a tüzek földrajzi kiterjedését, és felmérjék a károk intenzitását és mértékét [6].

Az európai erdőtűz-információs rendszer adatai szerint tavaly a következő országokban terjedt ki a legtöbb tűz 30 hektárnyi vagy azt meghaladó területre: Olaszország (147 tűzeset, 14.649 hektárnyi leégett terület), Spanyolország (104 tűzeset, 12.793 hektárnyi leégett terület), Portugália (86 tűzeset, 37.357 hektárnyi leégett terület), az Egyesült Királyság (79 tűzeset, 18.032 hektárnyi leégett terület) és Svédország (74 tűzeset, 21.605 hektárnyi leégett terület) [7].

Svédországot a valaha feljegyzett legsúlyosabb tűzidény sújtotta. A 21.605 hektárnyi teljes leégett területével Svédország a második az EU-ban, ami egy északi ország esetében igen szokatlan. A leégett terület nagyságát illetően az első ismét Portugália, azonban ez a terület a 2017-ben leégettnek csak a töredékét teszi ki, és az elmúlt tíz évet tekintve is az egyik legkisebbnek számít [7].

2019-ben a száraz és szeles időjárási körülmények, valamint a magas hőmérséklet miatt hamar kezdetét vette a tűzidény. Idén már márciusra magasabb volt a tüzek száma az előző évtized egész éves átlagánál; sok tűz pusztított a hegyvidékeken és teremtett kritikus helyzetet a Duna-deltában [7].

Az Európai Bizottság statisztikája szerint 2019-ben az uniós polgári védelmi mechanizmus 20 alkalommal volt aktiválva főleg árvíz, földrengés és erdőtűz miatt, de

megjelent a trópusi ciklon, a járvány és a tengerszennyezés okozta károk következményeinek felszámolására szóló EU-n kívüli mechanizmus aktiválás is [8].

## A RESCEU KÉPESSÉG [3]

A regisztrált erdőtüzek tekintetében 2017 az egyik legrosszabb év volt Európában. A lángok 127 emberrel végeztek és több mint 1,2 millió hektár földterületet égettek le az Európai Unióban. Az anyagi károkat több mint 10 milliárd euróra becsülik. Ez az év kihívások elé állította a nemzeti képességeket és az Európai Polgári Védelmi Mechanizmust egyaránt. Ez a helyzet pedig rámutatott az együttműködés fokozásának szükségességére. 2018-ban több mint 100 ember halt meg Európában természeti vagy ember által okozott katasztrófákban. Önmagukban az erdőtüzek 22 európai uniós tagállamot érintettek. A mediterrán térségben, de az olyan országokban is, ahol az erdőtüzek száma általában alacsony, például Svédországban, Németországban, Írországban, Finnországban és Lettországban, az utóbbi években az esetek számának emelkedése tapasztalható. Ez a kockázat a jövőben várhatóan növekedni fog az összes európai területen az éghajlatváltozás miatt, ami szélsőséges időjárási körülményeket és hosszú száraz időszakokat okoz. Az utóbbi események figyelembevételével az Európai Bizottság javaslatot tett az Európai Polgári Védelmi Mechanizmus megerősítésére és korszerűsítésére. A Parlament és a Tanács jóváhagyását követően 2019-ben létrejött a rescEU.

A rescEU a következő NÉGY képességekből tevődik össze [10] [12]:

- légi erdőtűzoltás;
- nagy teljesítményű szivattyúzás;
- városi kutatás és mentés;
- tábori kórház és sürgősségi orvosi csoportok.

### Első lépések a rescEU képesség kialakításában

A tűzoltó repülőgépek és helikopterek első flottáját májusban hoztuk létre, még a 2019. évi erdőtűz időszakot megelőzően. Ez a tartalék flotta segíti az EU-t abban, hogy gyorsabb és átfogóbb választ legyen képes adni az egyes válságokra. A flotta biztonsági hálóként is működik, abban az esetben, ha a nemzeti képességek túlterheltek és az Európai Polgári Védelem Eszköztár nem áll rendelkezésre.

A rescEU kiegészíti a nemzeti polgári védelmi erőfeszítéseket. Ez akkor fontos különösen, amikor több ország egyidejűleg azonos típusú katasztrófával néz szembe, és nem tudnak egymásnak segíteni. Eddig hat ország (Franciaország, Görögország, Horvátország, Olaszország, Spanyolország és Svédország) bocsátotta eszközeit a rescEU-flotta rendelkezésére, beleértve tűzoltó repülőgépeket és helikoptereiket is.

### A rescEU-képesség alkalmazására vonatkozó szabályok [11]

A segítségnyújtás iránti kérelem beérkezését követően az ERCC értékeli, hogy a tagállamok által az uniós mechanizmuson keresztül felajánlott meglévő képességek és az európai polgári védelmi eszköztár számára előzetesen rendelkezésre bocsátott képességek elégségesek-e a kérelemre való hatékony válaszadáshoz. Amennyiben nem biztosítható ha-

tékony reagálás, a Bizottság az ERCC-n keresztül határoz a rescEU-képességek telepítéséről az 1313/2013/EU határozat 12. cikkének (6) bekezdésében meghatározott eljárásnak megfelelően.

A rescEU-képességek telepítésére vonatkozó döntésnél az alábbi tényleges ismérveket kell figyelembe venni:

- a különböző tagállamok műveleti helyzete, illetve a lehetséges katasztrófakockázatok;
- a rescEU-képességek megfelelősége és elégségessége a katasztrófák kezelésére;
- a rescEU-képességek földrajzi helye, beleértve az érintett területre való becsült szállítási időt;
- egyéb releváns ismérvek, beleértve a rescEU-képességek operatív szerződésekben meghatározott feltételeit.

Egymással ütköző segítségnyújtási kérelmek esetén a rescEU-képességek telepítésére vonatkozó döntésnél a következő további ismérveket kell figyelembe venni:

- az emberéleteket veszélyeztető várható kockázatok;
- a 2008/114/EK tanácsi irányelv (4) 2. cikkének a) bekezdése szerinti kritikus infrastruktúrát veszélyeztető várható kockázatok, függetlenül attól, hogy az az Unió területén belül vagy kívül található;
- a katasztrófák várható hatása, beleértve a környezeti hatásokat is;
- az ERCC által azonosított szükségletek és a meglévő telepítési tervek;
- a katasztrófák terjedésének lehetséges kockázata;
- társadalmi-gazdasági hatások;
- a szolidaritási záradék életbe lépésének kiváltása az Európai Unió működéséről szóló szerződés 222. cikke alapján;
- egyéb releváns műveleti tényezők.

**A rescEU-képességek nemzeti célokra való használata [11]**

A rescEU-képességeket nemzeti célokra használó tagállamok a következőket biztosítják:

- a vonatkozó minőségi követelményekben meghatározott időtartamon belül rendelkezésre állás és felkészültség az
- uniós mechanizmus keretében végzett műveletekre, kivéve, ha a Bizottsággal másként állapodtak meg;
- a rescEU-képességek és egyéb nemzeti képességek azonos kezelése a megfelelő karbantartás, tárolás, biztosítás,
- személyzet és egyéb vonatkozó irányítási és karbantartási tevékenységek tekintetében;
- kár esetén gyors javítás.

A tagállamok az ERCC-n keresztül értesítik az Európai Bizottságot a rescEU-képességek nemzeti célokra való használatáról és a használatot követően jelentést nyújtanak be. Amennyiben a rescEU-képességek nemzeti célokra való használata e cikk (1) bekezdésének a) pontja szerint hatással van a rendelkezésre állásra, a tagállam a telepítés előtt az ERCC-n keresztül megszerzi a Bizottság jóváhagyását. A tagállamok a lehető legrövidebb

időn belül biztosítják a rendelkezésre állást, amennyiben a szóban forgó rescEU képességekre szükség van az uniós mechanizmus keretében végzett mentési műveletekhez.

## AZ UNIÓS POLGÁRI VÉDELMI MECHANIZMUS EREDMÉNYE

Az Európai Polgári Védelmi Mechanizmus korszerűsítése megszilárdította és megerősítette az Európai Unió katasztrófakockázat-kezelésének minden elemét. A rescEU létrehozása mellett ez az új jogszabály növeli a nemzeti képességeket és támogatja a résztvevő országok megelőzési és felkészültségi tevékenységeit. Az EU emellett növelte az Európai Polgári Védelmi Eszköztárban regisztrált képességek pénzügyi támogatását is. Ez a 2013-ban létrehozott eszköztár fokozza a katasztrófákra adott európai válasz következetességét, biztosítva, hogy a lehető legtöbb képesség legyen bevethető a katasztrófa bekövetkezése előtt. A pénzügyi támogatás felhasználható a kapacitások módosítására és javítására, valamint az ezen helyzetekre való reagálási képesség operatív költségeinek (EU-n belüli) és a szállítási költségeinek (EU-n kívüli) fedezésére, ha azokat az Európai Polgári Védelmi Mechanizmus alapján állítják fel [9].

Az újonnan létrehozott Európai Polgári Védelmi Tudáshálózat az ismeretek, az elérhető legjobb gyakorlatok és a következtetések megosztására szolgáló platform a polgári védelem szakértői és a katasztrófavédelemben dolgozók számára. A hálózaton keresztül az EU az európai katasztrófakockázatkezelés megerősítését tervezi. A továbbfejlesztett uniós Polgári Védelmi Mechanizmus korszerűsíti és egyszerűsíti az adminisztratív eljárást annak érdekében, hogy csökkenjen a segítségre szoruló emberek eléréséhez szükséges idő [3].

A 2019-es nyár folyamán az EU légi járművekből álló átmeneti tűzoltó flottát hozott létre, amelyet a görögországi és libanoni erdőtüzek elleni küzdelemben már kétszer is bevetettek. Emellett az Európai Bizottság kezdeményezte az erdőirtással és erdőpusztulással szembeni uniós fellépés fokozását, valamint további intézkedések mellett kötelezte el magát, például az európai erdőtűz-információs rendszer világszintű erdőtűzfigyelő-eszközzé való továbbfejlesztésére [7].

A rescEU flotta létrehozása mellett az Európai Bizottság megerősíti a nyomon követési és koordinációs képességeit az erdőtüzek által érintett időszakra való felkészülés jegyében [4].

- Az EU Veszélyhelyzet-reagálási Koordinációs Központját (ERCC), amely a nap 24 órájában és a hét minden napján rendelkezésre áll, egy tagállami szakértőkből álló, erdőtüzekre szakosodott támogató csapattal fogják bővíteni nyáron.
- Az ERCC a nyár folyamán rendszeres videokonferenciákat fog szervezni a tagállamokkal annak érdekében, hogy megossza az információkat az Európa-szerte előfordul erdőtüzekről.
- Az EU Kopernikusz műholdas rendszerét fogják használni az erdőtüzek okozta vészhelyzetek feltérképezésére.
- Minden uniós tagállam és a partnerországok is részt vettek az erdőtüzekkel kapcsolatos éves találkozón Brüsszelben, a következő erdőtüzekkel érintett időszakra történő felkészülés jegyében.

- Az elmúlt hónapokban több erdőtüzekkel kapcsolatos terepgyakorlatot is tartottak. Ide tartoznak a MODEX polgári védelmi és erdőtüzekkel kapcsolatos terepgyakorlatok, amelyeken különböző uniós tagállamokból szakértők és mentőcsapatok vettek és vesznek részt [4].

2019 augusztusában Görögország jelentős erdőtüzekkel szembesült Evia szigetén, és segítségért kérte az ERCC-n keresztül további légi tűzoltási eszközök beszerzéséhez. Az EU polgári védelmi mechanizmusának aktiválását követően az EU válaszában a mentőegység tartalékát először mozgósították. Három repülőgépet - két olasz és egy spanyol - feladtak Evia szigetére. Az EU tagállamainak szoros együttműködése kulcsfontosságú volt a tüzek elleni küzdelemben, az emberek megmentésében, a közeli faluban és a védett erdőben [8].

## JÖVŐBENI CÉLOK

A kezdeti átmeneti időszak a rescEU tekintetében 2025-ig tart. További képességekkel és eszközökkel egy olyan állományt fogunk létrehozni, amely képes reagálni a különféle katasztrófákra, ideértve az egészségügyi veszélyhelyzet, valamint a biológiai, radiológiai, vegyi és a nukleáris incidenseket is. A rescEU tovább erősíti az EU katasztrófa-megelőzési, valamint a katasztrófákra való felkészülési és reakcióképességét is. Egy szolidaritáson alapuló Unióban ez biztosítja, hogy egyetlen ország se maradjon egyedül a nehéz helyzetekben [3].

Cél a katasztrófákra való uniós válasz kollektív képességének megerősítése és az azonosított kapacitási hiányosságok kiküszöbölése a RescEU létrehozásával, valamint a meglévő önkéntes készlet fejlesztésével, amelyet európai polgári védelmi eszköztár (ECPPool) neveznek. 2019-ben az EU megerősíti a katasztrófákra adott kollektív európai reagálást egy ismert tartalékkapacitás fejlesztésével, mint mentőegység-tartalék, és utólagos lehetőségként használható fel, ha a tagállamok kapacitásait már teljes mértékben kihasználják [8].

Az Európai Humanitárius-segítségnyújtási és Polgári Védelmi Műveletek Főigazgatósága (DG ECHO) meglévő belső felügyelet rendszerét tervezik használni annak biztosítására, hogy az új eszköz keretében rendelkezésre álló forrásokat helyesen és a megfelelő jogszabályokkal összhangban használják fel [13].

A rendszer jelenlegi kialakítása a következő:

- A DG ECHO belüli belső felügyeleti csoport, amely az érvényben lévő igazgatási eljárások és a polgári védelem terén hatályos jogszabályok betartására összpontosít. E célból a Bizottság belső ellenőrzési keretrendszerét használják.
- Az eszköz keretében odaítélt támogatások és szerződések a DG ECHO külső könyvvizsgálói általi rendszeres ellenőrzésinek teljes mértékben beépülnek a Főigazgatóság éves ellenőrzési tervébe;
- A tevékenységek külső partnerek általi értékelése.

A gyors és hatékony veszélyhelyzet-reagálási beavatkozások elősegítése súlyos katasztrófák vagy azok fenyegető közelsége esetén tényleges uniós célkitűzés:

- A műveletek sebessége: a segítségnyújtás iránti kérelem és a segítség helyszíni telepítése, valamint a katasztrófa-becslő és koordináló csoportok teljes működőképessége között eltelő idő;

- A rescEU és az európai polgári védelmi eszköztár által telepített eszközök aránya;
- a szállítási támogatások és szolgáltatások száma;
- Az Európán belüli és kívüli rescEU műveletek uniós pénzügyi fedezet összege (rendkívüli körülmények esetén az üzemeltetési és szállítási költségek);
- Az európai polgári védelmi eszköztár Európán belüli és kívüli műveletei uniós társfinanszírozásának összegei (szállítási műveletek);
- A tagállamoknak nyújtott uniós társfinanszírozás teljes összege
- Az összevont események számát használták fel, szemben az uniós polgári védelmi mechanizmus keretében végrehajtott küldetések teljes számával.

A katasztrófák elleni védelem magas szintjének elérése a katasztrófák hatásainak megelőzése vagy csökkentése, valamint a megelőzés kultúrájának megteremtése útján a fő célkitűzés:

- A nemzeti kockázatértékelést és katasztrófakockázat-kezelési tervet benyújtó tagállamok száma;
- a katasztrófavédelmi tervezésük összefoglalóját benyújtó tagállamok száma;

Az Unió katasztrófareagálásra való felkészültségének fokozása érdekében a kiemelt célkitűzés:

- Az uniós polgári védelmi mechanizmus által képzett szakértők száma, akiket az uniós polgári védelmi mechanizmus keretében válaszadási küldetések telepítenek;
- Az EU-n belüli és a szomszédokkal folytatott szakértőcserék száma;
- A rescEU részeként megszerzett eszközök száma és típusa;
- Az európai polgári védelmi eszközhöz való csatlakozáshoz hitelesített eszközök száma és típusa;
- Az európai polgári védelmi eszköz céljára eszközöket biztosító tagállamok száma;
- A rescEU küldetések száma, illetve az európai polgári védelmi eszközkeretében reagálást végrehajtó missziók teljes száma.

**Uniós polgári védelmi célok 2021-2027. közötti időszakra**

2018. május 2-án a Bizottság javaslatot fogadott el a 2021–2027 közötti időszakra vonatkozó többéves pénzügyi keretre.

A Strasbourgban 2018. május 29-én kiadott, az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alap Pluszra, a Kohéziós Alapra és az Európai Tengerügyi és Halászati Alapra vonatkozó közös rendelkezések, valamint az előbbiekre és a Menekültügyi és Migrációs Alapra, a Belső Biztonsági Alapra és a Határigazgatási és Vízumeszközre vonatkozó pénzügyi szabályok megállapításáról szóló Európai Parlament és Tanács rendelet IV. függeléke megfogalmazza a szakpolitikai célkitűzést, amely zöldebb, karbonszegény Európa a tiszta és méltányos energetikai átállás, a zöldebb és kék beruházás, a körforgásos gazdaság, az éghajlatváltozáshoz való alkalmazkodás, valamint a kockázatmegelőzés és –kezelés előmozdítását célozza meg [16]. Uniós cél:

- Az éghajlatváltozáshoz való alkalmazkodáshoz kapcsolódó intézkedések, valamint az éghajlattal összefüggő kockázatok megelőzése és kezelése:
    - árvizek (ideértve a tudatosságnövelést, a polgári védelmet, valamint a katasztrófavédelmi rendszereket és infrastruktúrákat is)

  - tűzvészek (ideértve a tudatosságnövelést, a polgári védelmet, valamint a katasztrófavédelmi rendszereket és infrastruktúrákat is).
  - egyéb, például viharok és aszályok (ideértve a tudatosságnövelést, a polgári védelmet, valamint a katasztrófavédelmi rendszereket és infrastruktúrákat is)
- Kockázatmegelőzés és a nem az éghajlattal kapcsolatos természeti kockázatok (pl. földrengések), valamint az emberi tevékenységekhez kapcsolódó kockázatok (pl. technológiai balesetek) kezelése, ideértve a társadalmi tudatosság fokozását, a polgári védelmet és a katasztrófavédelmi rendszereket és infrastruktúrákat is.

## A RESCEU LÉNYEGÉNEK ÖSSZEFOGLALÁSA [15] [17]

A rescEU képességeket tagállamok szerzik be, bérelik vagy lízingelik, illetve azok a tagállamok vezetése és irányítása alatt állnak. Ugyanakkor a összehangolt és egyben gyors reagálás biztosítása érdekében, a kapacitások telepítésére és demobilizációjára vonatkozó döntést, valamint az ellentmondó kérelmek esetén hozandó döntéseket a Bizottság hozza meg, a segítséget kérő és a segítséget nyújtó tagállamokkal szoros együttműködésben.

A rescEU képességek nemzeti, azaz hazai célokra is használhatóak, ebben az esetben az összes felmerülő költséget az adott tagállam viseli.

Annak biztosítása érdekében, hogy a rescEU teljes körű kialakításáig is elegendő képesség álljon rendelkezésre, 2025. január 1-jéig átmeneti időszakot alkalmaznak. Az átmeneti időszak elsődleges célja (volt) a 2019-es erdőtüzes időszakot megelőzően biztosítani a nemzeti képességek rescEU részeként történő működését. Az átmeneti időszak Görögország, Franciaország, Horvátország, Olaszország, Spanyolország és Svédország tevékeny részvételével indult.

A rescEU létrehozására, igazgatására és fenntartására nyújtandó uniós támogatás aránya legalább a képességek elérhetősége és bevethetősége teljes becsült költségének 80 százaléka és legfeljebb 90 százaléka. A költségek fennmaradó részét a képességet befogadó tagállamok viselik. Minden egyes képesség teljes becsült költsége végrehajtási jogi cselekedetek révén kerül meghatározásra, meghatározott, támogatható költségkategóriák figyelembevételével. A pénzügyi támogatások többéves munkaprogramok alapján is végrehajthatók.

Az alacsony valószínűséggel bekövetkező nagy hatással járó veszélyekre történő válaszadás céljából létrehozott kapacitások elérhetőségéhez és bevethetőségéhez szükséges teljes költséget uniós forrásból biztosítják.

A rescEU egységei jelenleg tűzoltó repülőgépekből és helikopterekből áll, a jövőben azonban ennek bővítése tervezett nagyteljesítményű szivattyú, CBRN (vegy-biológiai-radiológia-nukleáris) és mobil kórház rescEU képességek létrehozásával.

További célja a megújított mechanizmusnak az is, hogy egyszerűsítse az adminisztratív eljárásokat a minél gyorsabb és magasabb szintű védelem, a katasztrófákra adott válasz hatékonyságának növelése érdekében.

## FELHASZNÁLT IRODALOM

[1.] Európai Parlament: Európának köszönhetjük, Interneten elérhető: https://what-europe-does-for-me.eu/data/pdf/social/X07_26001_hu.pdf (letöltés: 2020.02.20.)
[2.] Az Európai Parlament és a Tanács (EU) 2019/420 határozata (2019. március 13.) az uniós polgári védelmi mechanizmusról szóló 1313/2013/EU határozat módosításáról, Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019D0420&from=HU (letöltés: 2020.02.20.)
[3.] Európai Bizottság: rescEU – Európa katasztrófavédelmi egysége, amelyre számíthat. Interneten elérhető: file:///C:/Users/pjack/Downloads/rescEU_Backgrounder-HU-HD.pdf (letöltés: 2020.02.20.)
[4.] MABISZ: Közelgõ nyári erdõtüzek: már az EU is készül rájuk, Interneten elérhető: https://mabisz.hu/szemle/?p=8998 (letöltés: 2020.02.20.)
[5.] Index: Katasztrófavédelmi központot állít fel az EU, Interneten elérhető: https://index.hu/kulfold/eurologus/2017/11/23/katasztrofavedelmi_kozpontot_allit_fel_az_eu/ (letöltés: 2020.02.20.)
[6.] Európai Bizottság: Harc az európai erdőtüzekkel – hogyan működik az uniós mechanizmus?, Interneten elérhető: https://ec.europa.eu/commission/presscorner/detail/hu/MEMO_15_5411 (letöltés: 2020.02.20.)
[7.] San-Miguel-Ayanz, J., Durrant, T., Boca, R., Liberta`, G., Branco, A., De Rigo, D., Ferrari, D., Maianti, P., Artes Vivancos, T., Pfeiffer, H., Loffler, P., Nuijten, D., Leray, T. and Jacome Felix Oom, D., Forest Fires in Europe, Middle East and North Africa 2018, EUR 29856 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11234-1 (online),978-92-76-12591-4 (print), doi:10.2760/1128 (online),10.2760/561734 (print), JRC117883.
[8.] Európai Bizottság: European Civil Protection and Humanitarian Aid Operations Emergency Response Coordination Centre (ERCC), Interneten elérhető: file:///C:/Users/pjack/Downloads/emergency_response_coordination_centre_ercc_2020-02-10.pdf (letöltés: 2020.02.20.)
[9.] European Court of Auditors: Special Report: Union Civil Protection Mechanism: the coordination of responses to disasters outside the EU has been broadly effective, Interneten elérhető: https://www.eca.europa.eu/Lists/ECADocuments/SR16_33/SR_DISASTER_RESPONSE_EN.pdf (letöltés: 2020.02.20.)
[10.] Összefoglaló: 1313/2013/EU határozat az uniós polgári védelmi mechanizmusról: A katasztrófák megelőzésére, valamint az azokra történő felkészülésre és reagálásra való kollektív képesség fokozása, Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:2009_2 (letöltés: 2020.02.20.)
[11.] A Bizottság (EU) 2019/1310 végrehajtási határozata (2019. július 31.) az európai polgári védelmi eszköztár és a rescEU működtetésére vonatkozó szabályok megállapításáról (az értesítés a C(2019) 5614. számú dokumentummal történt) (EGT-vonatkozású szöveg.), Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019D1310&from=HU (letöltés: 2020.02.20.)
[12.] A Bizottság (EU) 2019/570 végrehajtási határozata (2019. április 8.) az 1313/2013/EU európai parlamenti és tanácsi határozat végrehajtására a rescEU-képességekkel összefüggésben alkalmazandó szabályok megállapításáról, valamint a 2014/762/EU

bizottsági végrehajtási határozat módosításáról (az értesítés a C(2019) 2644. számú dokumentummal történt) (EGT-vonatkozású szöveg.) C/2019/2644, Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019D0570&from=HU (letöltés: 2020.02.20.)
[13.] Európai Bizottság: Javaslat: Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Decision No 1313/2013/EU on an Union Civil Protection Mechanism
[14.] Javaslat - az uniós polgári védelmi mechanizmusról szóló 1313/2013/EU határozat módosításáról COM/2017/0772 final - 2017/0309 (COD), Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017PC0772&from=EN (letöltés: 2020.02.20.)
[15.] Lisszaboni Szerződés: az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (HL C 306., 2007.12.17.), mely 2009. december 1-jén lépett hatályba. Interneten elérhető: http://www.europarl.europa.eu/factsheets/hu/sheet/5/a-lisszaboni-szerzodes (letöltés: 2020.02.20.)
[16.] 43rd meeting of the Directors-General for Civil Protection of the European Union, of the European Economic Area and of the candidate countries, Helsinki, 9-10 October 2019 – Belső dokumentum
[17.] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, and the European Maritime and Fisheries Fund and financial rules for those and for the Asylum and Migration Fund, the Internal Security Fund and the Border Management and Visa Instrument COM/2018/375 final - 2018/0196 (COD), Interneten elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018PC0375&from=EN (letöltés: 2020.02.20.)

# DATA MANAGEMENT ON MASTERS LEVEL: BIOMETRICS AND THE LEGAL BACKGROUND

# ADATKEZELÉS MESTERFOKON: A BIOMETRIKUS AZONOSÍTÁS ÉS A JOGSZABÁLYI HÁTTÉR

UJHEGYI Péter[1], KUN Tamás[2]

**Abstract**

This article aims to provide a brief overview of the development of biometric identification solutions over the past decade. At the same time, the development of the legal environment is typically presented in the European Union and Hungary, but the international regulatory framework is also mentioned. Authentication has become a key area in the issue of applying IT technologies, which demanded procedures of the development side of processes, that could use most likely unique identifiers and could be use without difficulty. However, these solutions still give rise to public concern about the conditions under which companies and institutions using biometric procedures are entitled to collect data, and in many cases only years later it became clear that data collection proved to be unauthorized. At state-of-the-art procedures and technologies regulatory that influencing processes and societal attitudes has been reviewed, which could hinder or support diffusion.

**Keywords**

security, biometric identification, biometrics development, biometrics legal environment, authentication trends

**Absztrakt**

Jelen cikk rövid áttekintést kíván nyújtani az elmúlt évtized biometriai azonosítási megoldásainak fejlődéséről. Ezzel párhuzamosan bemutatásra kerül a jogi környezet fejlődése, jellemzően az Európai Unióban és Magyarországon, de említésre kerülnek a nemzetközi szabályozási keretek is. Az informatikai alkalmazások térnyerésével az azonosítás kulcsfontosságú területté vált, és olyan eljárások alkalmazását követelik meg a fejlesztői oldalon, amelyek többnyire egyediek, valamint könnyedén használhatók. Azonban ezek a megoldások a társadalomban aggályokat eredményeznek ma is, hogy milyen körülmények között jogosultak adatok gyűjtésére a biometriai eljárásokat alkalmazó vállalatok, intézmények, számos esetben csak évekkel később derült fény arra, hogy az adatgyűjtés jogosulatlannak bizonyult. Áttekintésre kerülnek a legmodernebb eljárások és technológiák, a szabályozásokat befolyásoló folyamatok és azok a társadalmi attitűdök, amelyek gátolják vagy támogatják az elterjedést.

**Kulcsszavak**

biztonság, biometrikus azonosítás, biometria fejlődése, biometria jogi környezet, azonosítási trendek

[1] ujhegyi.peter@phd.uni-obuda.hu | ORCID: 0000-0001-9143-6712| PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kun.tamas@phd.uni-obuda.hu | ORCID: 0000-0002-6620-7157| PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Az elmúlt évszázadok biometriával kapcsolatos fejlődését nagyobb részben az egyértelmű személyazonosítás területén megnövekedett igények alakították. Biometrikus azonosítás során mérjük és rögzítjük, lehetőleg automatikus technikákkal és eljárásokkal egy személy egyedi fizikai, testi jellemzőit, viselkedésbeli jellemvonásait és ezeket azonosítási és hitelesítési célra használjuk. A megoldást lehet személyazonosítás (identification) céljára használni, amikor egy adatbázis állományából keressük a megegyező mintát és azonosítjuk a személyt a csoport valamelyik tagjával. Vagy lehet használni ellenőrzésre, hitelesítésre (verification), amikor a rendszer hitelesít egy személyt az előzőleg felvett minta alapján és megállapítjuk, hogy a személy az e, akinek vallja magát. Hosszú út vezetett el az azonosítási megoldások tekintetében a mai sokrétű megoldásokig

A személyazonosítás a korai kezdetektől megjelenik történelmünkben. A becslések szerint is legalább 31 000 évvel ezelőtti Pech Merle barlangrajzokon olyan kézlenyomatokat találtak, melyek feltételezhetően a készítők azonosítása céljából aláírásként szolgáltak. [1] Hammurapi babilóniai király [2] törvénygyűjteményében a szerződéseket hitelesítő eljárásként ujjnyomatot használtak. Marcello Malpighi [3] 1684-ben az ujjak bőrléc-mintázatainak különbözőségeit tanulmányozta. Innen ered a Malpigi réteg elnevezés, ami a bőrfelület felső rétegére utal, ahol a fodorszálszerkezet található. 1685-ben az ujjnyom dermatoglífiai mintázatának elemzésével egy holland orvos, Bidloo foglalkozott behatóan és eredményei meghatározók a biometria tudományában.

A modern korban a népesség erőteljes növekedésének folyamata megkövetelte, hogy a bűnügyi nyomozati eljárások is haladjanak a korral, és olyan módszerek kerüljenek kidolgozásra, amelyekkel a bűnüldöző szervek egyértelműen beazonosíthatják az elkövetőket. Ebben az időben a migrációs folyamatok is adtak egy erőteljes lendületet a szakterületnek. Az 1800-as évek közepére, ahogy a városok népessége és az ipar fejlődött, egyre nagyobb igény merült fel az emberek pontosabb és gyorsabb azonosítására. A városok népességének bővülése magával hozta az emberek nagyobb mobilitását, a hatóságok már nem támaszkodhattak saját tapasztalataikra és helyi ismereteikre. Tudatosabb és kodifikáltabb lett az igazságszolgáltatás, ami egyre jobban igényelte az elkövetőkkel szembeni hatékonyabb fellépést és ezzel az egyértelmű azonosítási eljárások szükségszerűségét. Olyan formális rendszerek kidolgozására lett igény, mely nyilvántartja a bűncselekmények és elkövetők személyi jellemzőit. Az első rendszer a különböző testméretek mérésén és összehasonlításán alapuló Bertillon-rendszer volt, mely Franciaországból származott. A második módszer is a bűnüldözés területén indult fejlődének. Hivatalos eljárásokban a rendőri szervek az elkövetők azonosításában az ujjlenyomatokat kezdték használni.

Hazánkban a kriminalisztikai szakirodalom egységes abban, hogy a személyazonosítás új módszerének a magyar gyakorlatba történő bevezetése dr. Pekáry Ferenc kerületi rendőrkapitánynak (későbbi budapesti főkapitány-helyettesnek) köszönhető. [4] Vélhetően az 1902-ben Londonban töltött szabadsága alatt látottakat összegezve és az akkori szakirodalom (pl. Endrődy 1989-es nyomozati tankönyve) nyomon követésének hatására azt a következtetést vonta le, hogy az ujjnyomat alapú biometrikus azonosítási eljárás a gyakorlatban jobban alkalmazható és megbízhatóbb, mint az akkori korban inkább elterjedtebbnek számító Bertillon módszer. A Budapesti Rendőrfőkapitányságon kidolgozásra került az ujjnyomat alapú azonosítási módszertan [5] és 1904-ben bevezetésre került a daktiloszkópia. 1909. január 1. napján pedig megalakult az Országos Bűnügyi Nyilvántartó Hivatal és a

daktiloszkópiai részlege is, köszönhetően annak, hogy a dánosi rablógyilkosság felderítésénél az ujjnyomat azonosítás módszerével sikerült egyértelmű bizonyítékot szolgáltatni és az ügyet sikeresen lezárni.

Az 1900-as években a migrációs folyamatok indukálták az azonosítási módszerek fejlődését a bűnüldözési módszerekre fókuszálva és ahogy az törvényszerű, ezt lekövetve pedig az évezred végére a kereskedelmi forgalomban is egyre jobban elkezdtek terjedni a különféle biometrikus azonosításon alapuló megoldások. A továbbiakban kitérek az elmúlt évtizedben a biometrikus azonosítási technológiáinak fejlődésére és bemutatom a legújabb technológiák és tendenciák elterjedésének körülményeit.

## A TECHNOLÓGIÁK FEJLŐDÉSE

Visszatekintve az alapokhoz, a biometria egy görög eredetű kifejezés, a bio, mint élet és a metron, mint mérés szavakból tevődik össze. [6] Általánosságban, valamilyen élőlény valamilyen élettani jellemzőjét mérjük. A biometrikus azonosítás esetében az élőlény általában egy adott ember. A biometrikus jellemzői pedig az ember saját személyi jellemzőinek tekinthető, amelyek alapját képezik a személyazonosságának és velük együtt a jogosultságai meghatározásának. „Definíciószerű megfogalmazással a biometrikus azonosítás olyan automatikus technikát igénylő eljárás, amely „méri és rögzíti egy személy egyedi fizikai, testi jellemzőit, viselkedésbeli jellemvonásait, és ezeket azonosítás és hitelesítés céljára használja fel. A biometrikus felismerés alkalmazható személyazonosítás céljára, amikor a biometrikus rendszer azonosítja a személyt, az egész lajstromozott adatállományból kikeresve a megegyezőt, valamint használható ellenőrzés céljából, amikor a rendszer hitelesít egy személyt az előzőleg róla felvett és eltárolt minták alapján.” [7]

A biometrikus azonosítási technikákat az általuk vizsgált jellemzők alapján két nagyobb csoportba sorolhatjuk. Egyik a fizikai, fiziológiai alapú vizsgálatokon alapuló technikák csoportja, ide tartoznak az ujjnyomat, tenyérnyomat alapú azonosítások, az íriszazonosítás, a retinaelemzés, az arcfelismerés alapú megoldások, a geometriai felismerésen alapuló technikák, mint a kézkörvonal és a fülforma felismerés. Ide sorolható még a testszagészlelés, a hangazonosítás, a verejtékpórus-elemzés és a DNS mintázat elemzés. A másik csoportba a viselkedési minta elemzésén alapuló azonosítási megoldások tartoznak, mint a gépelési ritmus és kézírás elemzés, valamint a járás és mozgás elemzés. Elterjedőben vannak a pszichológiai alapú technikák ma még gyerekcipőben járó területei. Ahogy a profilozási megoldások, az összekapcsolt adatbázisok és az AI (mesterséges intelligencia alapú) technológiák egyre jobban teret nyernek, úgy ezek egyre jobb hátteret adnak az új irányzatok térhódításának.

Multimodális rendszereknek nevezzük a fenti technikák megoldásainak összevonását és integrálását. Ezekkel olyan komplex megoldásokat kapunk, melyek során többféle cél is teljesülni tud. Ezek a rendszerek több biometrikus adatot használnak párhuzamosan (például többféle mozgási jellemzőt mérnek), ezzel csökkentve a biometrikus rendszerek hibás elfogadási arányát, illetve növelik a kényelmet, a biztonságot és a hatékonyságot. Képesek arra, hogy nagyobb távolságról, az egyén hozzájárulása vagy célirányos tevőleges cselekedete nélkül is adatot gyűjtsenek, és ezzel nagyon jó lehetőséget biztosítanak másodlagos felhasználási területeknek, ahol már nem csak az azonosítás a fő cél. A többféle biometrikus jellemző összetettsége miatt, az ilyen rendszerek nagyobb tömegekkel kapcsolatos azonosítási igények kiszolgálására is alkalmas, mert nem csak azonosítani, hanem követni is lehet

az egyéneket. Az azonosítás megtörténhet egy arcfelismerő kamera által, de a tömegben való mozgás is (elvegyülési szándék esetén) követhető az alany járásképének elemzésével, de ha a megfigyelt személy esetleg napszemüveg mögé rejtőzik, fülformája alapján is azonosítható. Speciális esetben, például éjszaka, azonosítható a személy hőkép alapján is. Az ilyen rendszerek megtévesztése nagy felkészültséget igényel és a visszaélések során is több biometrikus jellemzőt kellene megszereznie, vagy korrumpálnia egy támadónak. A jobb megértéshez érdemes pontosan megismerni, hogy zajlik egy azonosítási folyamat.

A biometrikus azonosítási folyamat az egyén biometrikus adataiból képzett kód, a sablon létrehozásával kezdődik, mely a regisztrációhoz szükséges. A sablont jogi értelmezésben személyes adatnak kell tekinteni és a biometrikus adatok kezelésére vonatkozó előírások betartása kötelező érvényű rá. A sablon létrehozásakor egyirányú kódolással, nem visszafejthető módon, automatizált felhasználás céljára az egyén személyes mérhető adatait és jellegzetességeit dolgozzák fel olyan módon, hogy a sablonból a korábbi adattartalom nem állítható vissza semmilyen módszerrel. Erre a személyes adatok célhoz kötött kezelése érdekében, illetve az osztott információs rendszerekre vonatkozó adatvédelmi követelmények miatt van szükség. Fontos az is, hogy a sablon létrehozása után már nem lehet leválogatni az adatbázisból valamilyen speciális tulajdonságnak megfelelő jellemzőkkel rendelkező egyéneket, de az adatbázis ugyanakkor alkalmas arra, hogy referencia adatforrásként összehasonlító eljárásokkal személyazonosítást végezzenek vele. Az azonosítási módszerek sokfélesége a felhasználási területek fejlődésében mutatkozik meg igazán, mely módszerek az utóbbi 20 évben a kriminalisztikai felhasználási területeken kívül is rengeteget fejlődtek.

**Testalkat alapú azonosítás**

Az antropomorf jellemzők, azaz az emberi testi méretek különbözőségét mérő eljárások adják az alapját a testalkat alapú azonosítási megoldásoknak. A mai felhasználási megoldásokban ezek az eljárások önállóan nem, vagy csak nagyon speciális esetekben alkalmasak egyértelmű azonosításra. Ezért is szorult háttérbe a Bertillon módszer az elmúlt 100 évben, de kiegészítve egyéb távoli azonosítási eljárásokkal pontosítható az azonosítás eredménye. Minél több testalkattal összefüggő paramétert mérünk, annál pontosabb az azonosítás. Példaként említve a testmagasság adatokból még nem tehetünk egyértelmű becslést az alany származására, hiába tudjuk, hogy az ázsiaiak átlagosan alacsonyabbak az európai embereknél. De ha ezeket az adatokat kiegészítjük fejforma adatokkal és végtagokra vonatkozó adatokkal, akkor arányaiban máris pontosabb eredményt kapunk.

**Járás alapú azonosítás**

A járás alapú azonosítás (gait recognition) az egyik legígéretesebb kiegészítő azonosítási megoldás, hiszem távolról is végezhető, tömegek ellenőrzésére is alkalmazható és viszonylag kevés dolog befolyásolja az eljárás hatékonyságát. Már az 1900-as években is végeztek kísérleteket (gait-humact), amikor az emberi testekre csatolt fényforrások mozgását mérték és elemezték különböző testmozgások közben. A képfeldolgozáson alapuló technológia két modell alapján működik, az egyik a holisztikus, mely során a körvonalakat vizsgáljuk statisztikai módszerekkel, a másik a modell alapú parametrikus módszer, mely során fiziológiai paramétereket hasonlítunk össze. [8]

A hazai kutatások közül szeretném kiemelni Gálai Bence és Benedek Csaba 2017-ben végzett kutatását, többszenzoros LiDAR rendszerrel végzett, járás alapú személyazonosítás és cselekvésfelismerés témában. Eljárásuk többszereplős kültéri jelenetekből nyeri ki a felismeréshez szükséges jellemzőket, a személyek egyidejű mozgása mellett. Kölcsönös kitakarások és egyéb háttérmozgások zaja mellett sikeres, nagy hatékonyságú azonosításokat végeztek, mely a technológia további felhasználhatóságát támasztja alá. [9] Nemzetközi porondon a kínai Watrix cég megoldása 50 méteres távolságon belül képes nagy (94%-os) hatékonysággal az azonosításra, és a rendszerrel nem szükséges az alanynak együttműködni. Nagy tömegben, eltakart arccal, hátat fordítva, szándékosan sántikálva, görnyedt tartással sem téveszthető meg a rendszerük, mely természetesen AI támogatással működik. A technológia egyelőre nem real-time, azaz nem valós időben azonosítja a személyeket. [10]

**Hőkép alapú azonosítás**

Az amerikai hadsereg harci képességeinek fejlesztéséért felelős részlege, a Hadseregkutató Laboratórium tudósai együttműködtek a Polaris Sensor Technologies céggel, hogy kifejlesszenek egy speciális infravörös kamerát. Az elektromágneses sugárzás által kibocsátott fény tulajdonságai alapján minden tárgy sajátos polarizációs jelzéssel rendelkezik, az objektum felületének tulajdonságaitól és alakjától függően. Az IR polarimetrikus kamera, az úgynevezett Pyxis, képes megkülönböztetni az ember alkotta tárgyak polarizációs jelét a természetes háttérétől. A hő polarimetria lehetővé tette a kutatók számára az emberi azonosítás és arcfelismerés teljes sötétségben történő elvégzését, ahogy a kapott adatokat összevetették más biometrikus adatbázisokkal. Ezt kihasználva a katonaság számára olyan AI-val támogatott arcfelismerési megoldást fejlesztettek, mely teljes sötétben, hőkép alapján képes személyek azonosítására, vagy speciális felhasználási területen könnyűszerrel végzi személyek követését. A Polaris által kifejlesztett polarimetrikus IR kamera drónokra szerelve már bizonyított, de a katonáságon kívüli egyéb kereskedelmi felhasználási területen is eredményeket hozott. Kikötők, kereskedelmi vízi útvonalak, olajfúró platformok megfigyelésére és az olajszennyezett területek észlelésére is alkalmazható. [11]

**Viselkedésalapú megoldások (behavioral biometric)**

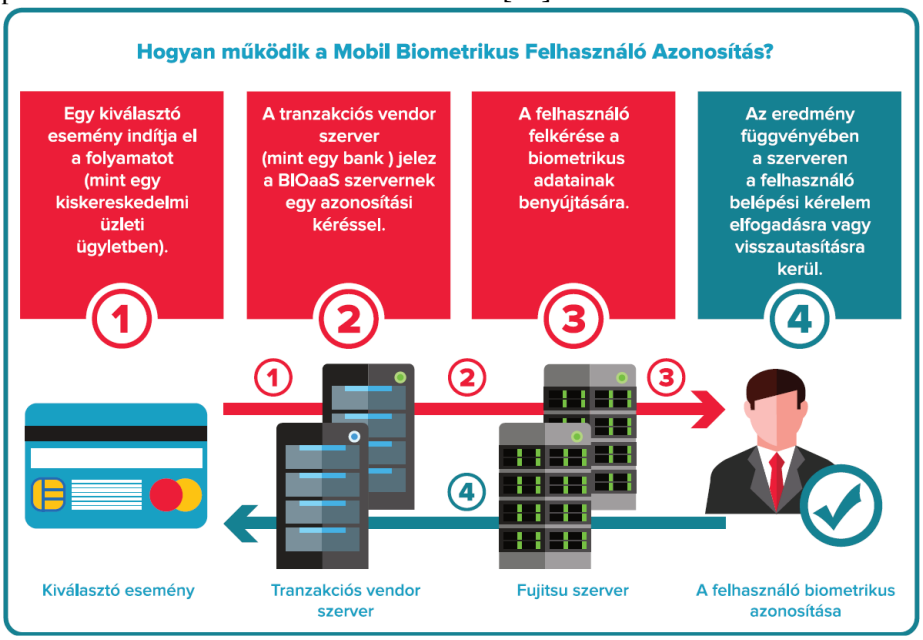
A viselkedés alapú biometria olyan emberi tulajdonságokkal kapcsolatos azonosítási megoldás, mely az egyedi képességek, stílus vagy motorikus képességek napi, rutinszerű feladatvégzés közbeni mérésén, összehasonlításán alapul. Ilyen lehet például minden számítógép használattal összefüggő tevékenység, mint a jellemző gépelési szokások, vagy az egér használattal összefüggő jellemző minták. De akár a telefonálás, az autóvezetés mintái, vagy a beszéd, sőt még a járás dinamikája és módja is ide tartozik.

„Az emberi viselkedésben rejlő különbözőségek elemzésére eddig is léteztek módszerek, melyek nem igényeltek gépi analízist: írásdinamika elemzése, beszédelemzés stb. Nagyon jó példa erre, hogy a második világháború során a Brit hírszerzés operátorai, a német Morse-kódok küldőiről képesek voltak anonim profilokat kialakítani, a gépelési sebesség és a vétett hibák alapján." [12] Ezek a megoldások, vagyis inkább adatok, nem használhatók egy beléptetés során elvégzendő hitelesítésre, de kiválóan alkalmasak profil alkotásra és a háttérben futó algoritmusok segítségével a folyamatos azonosításra, valamint a referen-

cia mintától való eltérés esetén riasztás életbe léptésére. A technológia természetesen alkalmas rejtett feltérképezésre és titkos profilozásra, hiszen interneten keresztül gépelési szokásainkat észrevétlenül rögzíthetik, vagy éppen rejtett kamerákkal és az arcfelismerés kombinálásával, járásunk módja egy adatbázisban összerendelhető.

## Legújabb technológiák

Zártan működő és védett rendszer felhasználóinak védelmére fejlesztett proaktív, végponti viselkedéselemző megoldást a BlackBerry Cylance. A Cylance Persona folyamatosan figyeli és elemzi a védett rendszer felhasználóinak viselkedését, azaz a beviteli perifériák használatát, mely során észleli a korábban felvett referencia adatoktól való eltérést és életbe lépteti az előre definiált cselekvési terveket. [13]

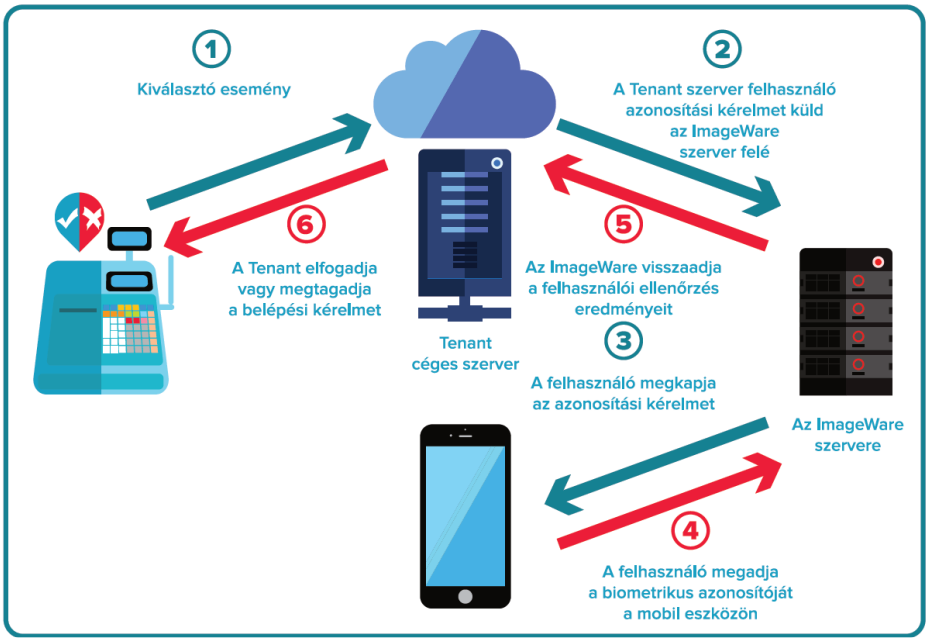



*1. ábra: Mobil biometrikus felhasználói hitelesítés [14]*

## Biometric as a Service (BIOaaS)

Vezető ICT szolgáltatóként a Fujitsu egy felhőalapú biometrikus platform kifejlesztését tervezi az ImageWare® Systems (IWS)-el kötött partnerség keretein belül. Az IWS a mobil és felhő alapú multimodális, biometrikus identitáskezelő megoldások egyik élenjáró szakértője, a Fujitsu pedig felhőalapú infrastruktúra szolgáltatásaival (IaaS) és szoftver szolgáltatásaival (SaaS) piacvezető. A Fujitsu a megoldásaival már régóta előkészíti a terepet a BYOD (Bring Your Own Device) jellegű környezetekhez és az ilyen üzleti igények kiszolgálásához. A szolgáltatásuk középpontjában a GoCloudID® áll, az IWS felhőalapú, biometrikus kezelési és azonosítási szolgáltatása. Ezt a Fujitsu felhőjéből igénybe véve, viszonylag gyorsan integrálni lehet az üzleti alkalmazásokkal, a pay-as-you-go modellen működő plug-n-play biometria segítségével. Az IWS GoCloudID® által a felhasználó személye gyorsan azonosítható, és így hozzáférés nyerhető a biztonságos digitális tartalmakhoz. Természetesen, mindezekhez szükséges a szolgáltató biztonságos alkalmazáskiszolgálója a

GoMobileInteraktiv®, mely a gyors és pontos személyazonosság ellenőrzést végzi. [14] Amikor a GoVerifyID alkalmazás rögzíti a felhasználó biometrikus adatait, azt továbbítja az IWS GoCloudID® platformjára, átalakítja digitális biometrikus sablonokba, és névtelenül tárolja a Fujitsu felhőalapú, Software-as-a-Service (SaaS) rendszerén keresztül.




*2. ábra: Felhő alapú azonosítás és hitelesítés folyamata [16]*

**Viselkedés alapú azonosítás**

A Fujitsu nem csak az egyike a felhő infrastruktúrában élen járóknak, de az ő nevéhez fűződik az első, tenyér érhálózat alapú, biometrikus azonosító szenzor, a PalmSecure szenzortechnológiája is. Erre az eszközre épül a Groupama Arénában bevezetett, „véna-szenzor" néven elhíresült, tenyérérhálózat alapú azonosító megoldás is. De a gyártónál az évek alatt nem álltak meg a fejlesztéssel, mert az új trendeknek megfelelően, olyan mesterséges intelligencia alapú –rögzített video tartalomban az emberi viselkedést elemző – eljárást fejlesztett ki, mely egyaránt képes a szinte alig észrevehető gesztusok és a komplex viselkedés arzenál felismerésére. „A szoftver mintegy 100 alap „cselekvés" segítségével képes modulárisan azonosítani összetettebb viselkedésmintákat, mint pl. a vásárláson való rágódás, vagy bűncselekményre készülődés. Mint azt a fejlesztő kifejtette, a „hagyományos", mélytanuláson alapuló eljárások jelentős méretű tanító adatbázisok segítségével, több hónapos munkával készíthetők fel az éles tevékenységre, melyet a Fujitsu megoldása szükségtelenné tehet. A szoftverbe alapként integrált 100 cselekvést/gesztust a rendszer 90% feletti hatékonysággal ismeri fel a fejlesztők állítása szerint. A cég tervei szerint, az Actlyzer a japán piacon debütál még az idén, majd az így beszerzett tapasztalatokra építve fejlesztik, mielőtt a Fujitsu Human Centric AI Zinrai termékcsomag részeként a globális piac számára is elérhetővé válik." [16]

**Érintés nélküli, ujjlenyomat alapú azonosítás**

Nedves vagy sérült ujjlenyomat azonosítására képes eszközök és megoldások, melyek érintés nélkül végzik el nagy sebességgel az azonosítást. Jellemzőjük a nagy pontosság és a nagy sebesség. Érintés nélküli technológiát használ, tehát higiénikus, egy másodpercen belüli gyors azonosítást tesz lehetővé, négy ujj menet közbeni azonosításával. Az azonosítás során a mintavétel folyamat így nem igényel külön időt, és az azonosítási eljárás elfogadásának cselekedete sem szükségszerű többé, hiszen a folyamat nem igényel a felhasználótól ráutaló magatartást. Az ilyen, rejtett azonosításon alapuló megoldások, a felhasználó hozzájárulását nem igénylő, vagy észrevétlenül kikényszerített azonosítást igénylő megoldások egyre jobban terjednek és ilyen eljárás egyre több várható a világban. 2020-ban a londoni Metropolitan Rendőrség nagy számban fog arcfelismerő kamerákat beüzemelni a kedvelt turistahelyszíneken és a bevásárló központokban. [17] Eddig az arcfelismerést Angliában csak sporteseményeken és koncerteken használták, de viszonylag magas számú téves azonosítással. Az új módszer szerint a rendszer csak megjelöli a gyanús egyéneket és a járőröző rendőrök pedig igazoltatják. Ugyanakkor az adatvédelmi szakemberek a polgári szabadságjogok elleni támadásnak veszik a bejelentést és felhívják a figyelmet, hogy könnyű a rendszerrel visszaélni.

**Közösségi médiából gyűjtött képek elemzése**

A Clearview AI, amerikai startup cég azzal került a figyelem központjába, hogy olyan szolgáltatóktól gyűjtött be publikusan elérhető képeket, mint a Facebook, a Youtube, az Instagram vagy a Twitter. Adatbázisában 3 milliárd kép található. [18] Maga a technológia ugyanúgy működik, mint bármilyen másik arcfelismerő algoritmus: az arcvonások elemzésével az adatbázisukban szereplő minden arcot matematikailag értelmezhető vektorokká alakítanak és a hasonló értékek alapján csoportokba rendezik őket. Amikor a rendszer egy azonosítandó arcot lát, azt is átalakítja, és összeveti a már tárolt értékekkel, majd kidobja a leginkább hasonló találatokat, azaz minden keresett személy képe mellé a leginkább releváns Facebook, Instagram vagy egyéb közösségi média találatokat párosítja. Ez a mélymerítés olyan széleskörű azonosítást tesz lehetővé, amelyhez foghatót nemcsak egyetlen másik technológiai vállalat, de az amerikai kormány se rakott még össze soha, legalább is mai ismereteink szerint. A cég megoldását több mint 600 bűnüldöző szerv használja. A szoftvercég nagyon sok ellenséget gyűjtött, és ezzel az arcfelismerés technológiára is rányomta a bélyeget. A megoldást úgy használja hatóságok sora, hogy az nem esett át független ellenőrzésen, például a technológiai sztenderdekre ajánlásokat megfogalmazó kormányzati ügynökség, a NIST vizsgálatán, illetve magát a céget és adatkezelési szabályzatait és azok betartását sem auditálta senki.

A hírek alapján a cég az adatbázist engedély nélkül állította össze. A közösségi médiában megtalálható képek tömeges leszűrését minden érintett cég saját adatkezelési szabályzatában tiltja. Valamint a bűnüldöző és állami szervek eddig csak hivatalos, hatósági forrásból származó képeket használhattak, nem pedig a polgárok közösségi médiában megosztott magánfotóit. Technológiailag úttörő, de jogi és adatkezelési szempontból kifejezetten aggályos, hogy a Clearview AI technológiája úgy képes azonosításra, hogy nem profilképeket használ, hanem bármilyen szögben készült kép, vagy apró képrészlet alapján képes azonosítani. Fő probléma, hogy nem ismert a cég adatkezelési szabályzata, az adatbázisok

védelmi szintje és a harmadik fél hozzáférésének lehetősége, kockázata sem. Mindez egyébként azért is problémás, mert az arc alapján történő biometrikus azonosítás több nagy technológiai cégnél is már évekkel ezelőtt kikutatott és elkészült technológia. A Facebook is készített arcfelismerő alkalmazást, a Google is kész már a technológiával (pl. GoogleGlass), de végül nem, vagy nem úgy dobták piacra a terméket ahogy eredetileg tervezték. A hírek szerint azért, mert az átfogó, nemzetközi szabályozási irányelvek még nem készültek el és nem akarták a technológiát ideje korán úgy bevetni, hogy az komoly ellenérzést vált ki a nagy tömegekből, vagy azért, hogy az esetleges visszaélések miatt a technológia ne szenvedjen hátrányt. [19]

**A biometria elterjedésének összefüggései**

Az elsietett megoldások piacra dobása nagyban rontja a technológia megítélését és elfogadottságát. Olyannyira, hogy az EU átmenetileg betiltaná pár évre az arcfelismerő rendszerek publikus helyeken való használatát az EU-n belül, hogy megelőzzék a lakosság megfigyelését és az ezzel járó ellenállás növekedését. Az egyelőre vázlat formájában létező, várhatóan a 2020-as év elején megszilárduló javaslat a GDPR adatvédelmi szabályozásból indul ki, melynek fő célja, hogy az EU polgárai ne legyenek kitéve a személyes profilt alkotó, automatizált rendszerek döntéseinek. A kamerákra azért vezetnék be az ideiglenes tiltást, hogy legyen idő mérlegelni a mesterséges intelligencián alapuló automatikus személyazonosítás kockázatait, és kidolgozni a szükséges finomhangolásokat és szabályozásokat. [20]

Eközben az USA kormányzata nyilvánosságra hozta saját, AI szabályozási irányelveit, amelyeknek célja a hatóságok túlzott mértékű korlátozására vonatkozik, és sürgette az EU-t, hogy kerülje el az agresszív megközelítéseket. [21]

Az arcfelismerő technológiák ellentmondásosak a világ többi részén is. Magyarországon a Parlament 2019. december 10-én megszavazta az "egyes eljárások egyszerűsítése és elektronizálása érdekében szükséges" salátatörvényben a rendőrségi törvény módosítását, aminek egyik pontja a biometrikus arcfelismerést szabályozza. [22] Eszerint az olyan esetekben, ahol a rendőr az igazoltatás során nem tudja hitelt érdemlően azonosítani a személyt, ott lehetséges az arcfelismerő szoftver használata. Sőt, további lehetőségként a rendőr ujjnyomtatot vehet a személytől és más biometrikus adatát is rögzítheti, melyek segítségével ott a helyszínen biometrikus azonosítást végezhet a megfelelő rendszerben. [23]

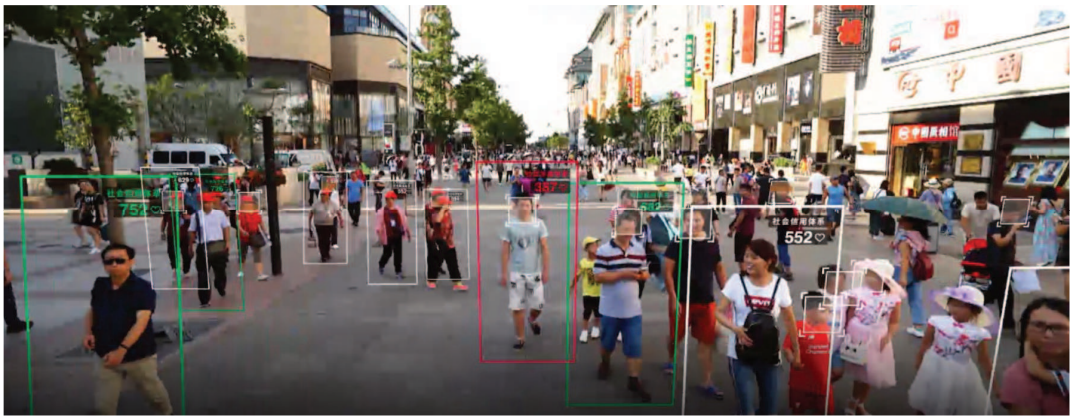
Megoldások szempontjából a kormányzati szektor mindig is a biometria korai alkalmazói közé tartozott, ideértve a határellenőrzésben használt technológiákat, a nemzeti azonosító megoldásokat vagy a bűnüldöző szervek által bevett eljárásokat. A mobil eszközök és alkalmazások növekvő elterjedésével várható, hogy az iparágakban egyre növekszik a biometrikus alkalmazások iránti igény az identitások hitelesítésére az online tranzakciókban. A magas kockázatú iparágak, mint a bankszektor is, jelentős beruházásokat végeznek a biometria területén. Csak a hangbiometria felhasználására már 2015-ben is 350 millió dollárt költött a szektor, aminek a következő időszakra a többszörözését várhatjuk, bár ebben a statisztikában majd érdekes lesz megfigyelni a koronavírus okozta, egyelőre ismeretlen mértékű hatásokat. Globális értelemben a közepes méretű biztosítótársaságok 70-80%-a már elfogadja a BYOD stratégiát, és ennek eredményeképpen a biztosítási üzletág jövőbeli kiadásai várhatóan mobilitási megoldásokat, biztonsági és vállalati alkalmazásokat céloznak meg. Különösen igaz lehet ez abban az esetben, ha a koronavírus okozta otthoni

munkavégzés megszokottá válik, mert ez lökést ad a távoli azonosítási megoldások fejlődésének.

A viselkedési minták integrálása biometrikus adatokkal, már napi szinten jelen van életünkben, amikor személyre szabott hirdetéseket kapunk. Ezeket hitelesítési eljárásokkal összekapcsolva sokkal magasabb szintre lehet emelni a biztonságot. Azonban nem szabad elfelejtkezni arról, hogy a nagyobb biztonság minden esetben a nagyobb szabadság rovására megy.

A pekingi Normal Egyetem kampuszán már évek óta arcfelismeréssel és kártya használatával lehet bejutni, amit nemcsak a diákok azonosítására használnak, de a viselkedési szokásaikat (éjszakai kimaradás) is elemzik. [24] Hangcsou 11. számú középiskolájában pedig a teremben tanuló diákokat figyelik meg arcfelismerő kamerákkal, melyek képesek az emberi arckifejezéseket értékelni. Így, ha egy diák tekintete sokáig elkalandozik, vagy ásítozik, azt a rendszer észleli. A tapasztalati visszajelzések alapján a tanulmányi teljesítmény javult, persze, ki merné az asztalra hajtani a fejét, ha közben tudja, hogy több kamera folyamatosan figyeli és értékeli. A rendszer egyébként nem rögzíti a képeket és nem tölt fel adatokat a felhőbe, csak a belső rendszer számára készít statisztikákat. [25]

Mindemellett, Kínában a digitális diktatúra csúcsra járatása történik éppen. [15] A Kínai kreditrendszer alapja a több százmillió arcfelismerést támogató kamera, mely segítségével totális megfigyelést hajt végre a kormány. A megfigyelésből gyűjtött adatok segítségével az embereket állami pontrendszerben pontozzák. A fizetési megoldásokat összekötik arcfelismerést használó mobil alkalmazásokkal. A bolti vásárlási szokásokat elemzik, a túl sok alkohol vásárlása pontlevonással jár, pelenka, vagy trendi és egészséges termékek vásárlásért plusz pontokat lehet szerezni. Az állam által kívánatos szolgáltatások igénybevételéért, vagy magán adatok megadásáért szintén plusz pontok járnak, akárcsak, ha valaki pontosan fizeti a hiteleit. De egy bebukott hitel akár le is nullázhatja a társadalmi kreditpontokat, amivel az illető egzisztenciája is semmivé foszlik, legvégső esetben a rendszer peremére sodródik. Nem ér el szolgáltatásokat, nem utazhat szabadon, nem vehet meg bármit, mert a társadalmon kívülre került. A népnevelés ilyen formája könnyen megy az autoriter rezsim állami propagandájának nyomása alatt, a közbiztonság igénye mögé bújva elveszi a magánszférát és digitalizálja a diktatúrát.




*3. ábra: Kínai megfigyelőrendszer. Forrás: HVG [26]*

Kínában a rendszer segítségével, algoritmusokkal kormányoznak. A laza, csak a központi állami szervek igényeire kialakított adatkezelési szabályzatok teljes mértékben támogatják a személyes adatok gyűjtését, profilozást és ezzel a magánszféra durva megsértését. Itt vissza is jutottunk a technológia fejlődéséhez és annak fontosságához, hogy a technikai fejlődéssel szorosan együtt kell, hogy járjon a jogi szabályozás fejlődése és a felhasználók megfelelő oktatása. A következőkben a nemzetközi jogszabályi környezetet vizsgáljuk.

## A BIOMETRIKUS AZONOSÍTÁS NEMZETKÖZI ÉS MAGYAR JOGSZABÁLYI HÁTTERÉNEK ÁTTEKINTÉSE

### General Data Protection Regulation (GDPR)

A GDPR azon felül, hogy az Európai Unió tagállamaira vonatkozóan speciális adatkezelési szabályokat határoz meg, attól az érintettek körébe tartoznak az Unión kívüli országok is, ezáltal a rendelet hatálya globális, mert EU adattal kapcsolatos tárgykörben is folyik adatkezelés. A rendelet deklarálja, hogy az adatgyűjtés megkezdése előtt a hozzájárulásnak explicit módon meg kell lennie. Nagy volumenű sajátossága a rendeletnek az elfeledtetéshez való jog, amely a kezelt adatokra vonatkozó visszaállíthatatlan törlés lehetőségének megvalósítását szorgalmazza. [27]

### Az Európai Adatvédelmi Testület ajánlása biometrikus adatkezelésre vonatkozólag

„A biometrikus adatok felhasználása és különösen az arcfelismerés fokozott kockázatot jelent az érintettek jogai szempontjából. Alapvető fontosságú, hogy az ilyen technológiák igénybevételére a GDPR-ben rögzített jogszerűség, szükségesség, arányosság és az adatok minimalizálása elveinek kellő tiszteletben tartásával kerüljön sor.” [28]

### UK Data Protection Act

Az Egyesült Királyságban 2018-ban elfogadott adatvédelmi törvény számos alkalommal említi a biometrikus adat kifejezést, a jogos érdek és a törvényes eljáráson felül a „sensitive processing”, azaz érzékeny adatkezelés meghatározáson belül is definiálja. Az általános rendelkezésekről e téren a 205. szakasz rendelkezik részletesen. [29]

### California Consumer Privacy Act (CCPA) módosítása AB-375

A törvénymódosító szerint a személyes adat kategóriájába a nyilvánosan elérhető információk nem tartoznak bele. Rögzíti továbbá, hogy a nyilvánosan elérhető adatok körébe kizárólag a törvényesen elérhető adatok tartoznak, amelyek a központi kormányzattól, az állami vagy helyi kormányzatok nyilvántartásaiból származnak. A biometrikus adatokra vonatkozólag úgy rendelkezik, hogy azok nem tartoznak nyilvánosan elérhető információk körébe és nem gyűjthetők a fogyasztó tudomása nélkül. [30]

Összegezve tehát elmondhatjuk, hogy a nemzetközi gyakorlatban a szabályozás arra törekszik, hogy legyen az állampolgár/magánszemély/fogyasztó besorolásokban egy olyan kapaszkodó pont, amely védi az egyéneket az akaratukon kívüli adatgyűjtéstől, valamint attól, hogy ha ezek mégis megtörténnének, legyen mozgásterük azoknak a kiküszöbölésére, módosítására, semmissé tételére. A különleges adatkategóriába tartozó biometrikus

adatok kezelése azért is kockázatos, mert olyan területeket képes kiszolgálni, mint a bűnüldözés, a személyre szabott marketing, politikai és vallási konfliktusok és számos más terület, ahol a személy pontos beazonosítása közel tökéletes azonosító jegyek alapján megvalósítható, az intézkedések és eljárások pedig személyre szabhatók. Ennek tudatában a szabályozás a jogos érdeket és a törvények szerinti eljárást különösképpen hangsúlyozza a jogszabályi keretekben.

## A BIOMETRIAI AZONOSÍTÁS SZABÁLYOZÁSÁNAK NEMZETKÖZI PÉLDÁI

### Iskolai keretek között rögzített ujjnyomatok miatt kiszabott bírság

A lengyelországi Gdańsk városában lévő 2.-es számú Általános Iskolában az iskolai ebédbefizetés ellenőrzése során alkalmazott ujjnyomatazonosítási eljárás miatt történt jogosulatlanul adatgyűjtés és adatkezelés. Ennek következtében a lengyel adatvédelmi hatóság bírságot szabott ki a tanintézmény számára, 20 000 lengyel zloty tételben (megközelítőleg 1,6 millió magyar forint). Az iskola 2015 áprilisa óta a 2019/2020-as tanévig 680 diák biometrikus adatát kezelte jogosulatlanul, és mindösszesen 4 tanuló választotta az alternatív megoldást az azonosításra. [31]

### Növekvő jogi és szabályozási követelmények a biometrikus adatok gyűjtésével kapcsolatban

Az elmúlt években a biometrikus azonosítás az ujjnyomat-ellenőrzéstől az arcfelismerésig, széles körben került elterjedésre a mindennapi használatban, elég, ha a fizetési megoldásokra gondolunk, vagy a reptéri beléptetésre a csomagellenőrzésnél. Ezek a megoldások, bár egyszerűsített azonosítási módszereket jelenthetnek a felhasználói oldalon, azonban adatvédelmi szempontból (és védelmi szempontból is) komoly elvárásokat támasztanak az adatkezelők számára ezeknek az adatoknak a gyűjtése során. Az Egyesült Államokban 2008 óta érvényben lévő Biometric Information Privacy Act is az egyik megjelenési formája ezeknek. 2019 januárjában egy iskolai kirándulás során egy fiúnak felvették az ujjnyomatát, mellyel igénybe vette a szabadidős parkba a belépőkártyáját. Azonban az azonosítást végző vállalat nem kötött ki határozott időt a felvett különleges adat kezelésével kapcsolatban, ezzel jogosulatlan adatgyűjtés miatt megszegte a BIPA rendelkezéseit. A vállalat szándéka a biometrikus azonosítással az volt, ha netán egy vendég elveszíti a papír alapú belépőkártyáját, a csalási szándék ezáltal kizárható legyen, tehát csak az az egyedi azonosítóval együttesen rendelkező személy használhassa a belépőt, akinek a regisztrációkor azt rögzítették. Viszont a cég a jogos érdekét az adatkezelés időtartamát tekintve nem tudta igazolni, ezért a per során veszített. [32]

### Biometrikus adat – a permanens személyes adat kockázatai

Néhány terület, ahol alkalmazásra kerülnek a biometrikus azonosítási eljárások:

- Munkaerőgazdálkodás
- Kórházak
- Bankszektor
- Kereskedelem
- Járműipar

Az Egyesült államokban az Illinois-i BIPA alapján 1000 dollártól 5000 dollárig terjedhet a bírság annak függvényében, hogy milyen természetű szabályszegés történt (szándékosság tényállása). Ezek a rendelkezések azonban 2018 februárjában módosítva lettek olyan kizáró tényezőkkel, mint hogy:

- az adott entitás a biometriai adatkezelést és adatgyűjtést biztonsági okokból, csalás megelőzés céljával vagy munkaerőgazdálkodási szempontból alkalmazza,
- nem folytat kereskedést ezekkel az adatokkal,
- illetve ezeknek az adatoknak a tárolása, cseréje, valamint védelme a magánszektorra jellemző alapvető módon vagy még hatékonyabb szinten történik, hasonlóan a bizalmas és érzékeny információkra tekintettel [33]

**Biometrikus azonosítás a munkahelyen**

A biometrikus azonosítás munkahelyi környezetben való alkalmazása világszerte elterjedőben van, a munkavállalóknak a vállalati eszközökhöz való hozzáférését, vagy elzárt területekre való bejutását szolgálhatja ki. A módszertan bevezetésével a csalások redukálhatók, a biztonsági szint számottevően emelkedik, amellett, hogy egyéb területek biztonsági költségein még spórolni is tudunk. Azonban fontos szem előtt tartani, mivel különleges adatok kezeléséről van szó, ezért adatvédelmi szempontból kellő gondoskodással kell eljárnunk mind a rendszerek, mind az adatok védelmével kapcsolatban. További fontos elemként jelenik meg, hogy a kezelt adat természetéből fakadóan jellemzően a tökéletesen egyedi felé tendál, azoknak esetleges kiszivárgása a rendszerekből, illetve egyéb okból jogosulatlan kézbe kerülésük esetén komoly gondokat okozhatnak. Ezeket még a bevezetés előtt célszerű felmérni, ezzel is elkerülve a kontraproduktív hatást. A jogszabályi háttér során két alapelvet mindig biztosítani kell, ez pedig az előzetes önkéntes hozzájárulás, valamint a jogos érdek biztosítása. Ezekről már a korábban említett GDPR részletesen rendelkezik. Fontos továbbá az is, hogy a biometrikus eljárások alkalmazása során kellő körültekintéssel rendelkezzenek a munkavállalók is, hiszen ők maguk is felelősek az általuk kezelt adatokért. [34]

**Arcfelismerési szabályozás az Egyesült Királyságban, Kanadában és az Egyesült Államokban**

A döntéshozók szerte a világban vagy várakozási álláspontot, vagy védekezési módban állnak a technológiai megoldással kapcsolatban. A kanadai tartományok közül az atlanti térségben elhelyezkedő mind a négy tartományban közös nevezőn vannak a járművezetési engedély kiadásához kötődő arcfelismerési eljárások bevezetésében a szabályozást illetően. A közlekedésügyi miniszter megjegyezte, hogy 2007 óta már rendelkezésre áll a technológia és az engedély nélküli autóvezetés területén már volt néhány fogás annak alkalmazásával. Skóciában a liberális politikai erők azért emeltek szót, hogy a rendőrségi nyilvántartásban szereplő ártatlan emberek arcképmásai legyenek eltávolítva, mert nincs jogos érdek tárolásukra. Az Egyesült Államokban egy korábban a New York Police Department biztosaként dolgozó szakember, Bill Bratton szerint a szabályozásnak nem kellene tiltania a biometrikus eljárásokat. Álláspontját azzal igyekezett alátámasztani, hogy a magánszektor már régóta foglalkozik és fejleszti ezeket az eljárásokat, attól függetlenül, hogy

ezt a Szenátus szeretné vagy sem. Továbbá kiemelte, hogy a technológiai megoldás az ártatlan embereket igyekszik védeni a börtönbüntetéstől, szembe állítva ezt a szemtanúi vallomás alapján történő ítélkezési eljárással. [35]

2015-ben a skót parlamenti képviselők kritikával illették a szabályozási gyakorlatot, valamint a skót kormány által létrehozott biometriai biztosi pozíciót, melyről azt vélték, hogy nem lesz olyan hatékony, mint az elvárt lenne. Mathew Rice, az Open Right Group Scotland igazgatója a problémát a beszámolási kötelezettségekben találta, érvelésében az információügyi biztos pozíciójával vonta párhuzamba, ahol a probléma a tájékoztatás szűkösségében van, mert a biometriai biztos csak a parlament irányába szolgáltathat adatot. [36]

## A magyar jogszabályi környezet fejlődésének vizsgálata a biometrikus azonosítás szabályozásának szemszögéből

A hazai szabályozás első körben a (1. táblázat) szereplő bűnügyi nyilvántartó rendszer (rendelkező jogszabály a bnytv). keretein belül rendelkezik a biometrikus azonosítás, mint eljárás és különleges adatgyűjtési módszerről, valamint annak meghatározott céljáról. Kiindulópontként az ujjnyomat felvételi eljárás, valamint annak (a) személyhez kötött eljárás rendjét definiálja.

| Kihirdetés ideje | Jogszabály neve |
|---|---|
| **2009. VI. 19.** | 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről |
| **2011. VII. 26.** | 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról |
| **2013. IV. 25.** | 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról |
| **2016. IV. 27.** | AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE |
| **2018. XI. 28.** | AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1860 RENDELETE<br>AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1861 RENDELETE<br>AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1862 RENDELETE |
| **2018. XII. 12.** | 2018. évi CXXXV. törvény a sportról szóló 2004. évi I. törvény módosításáról |
| **2018. XII. 20.** | 2018. évi CXXI. törvény egyes belügyi tárgyú és más kapcsolódó törvények módosításáról |

*1. táblázat: A jogszabályi háttér időrendi változása (Saját szerkesztés)*

A növekvő igényre mind az azonosítás, mind az adatgyűjtés területén, szükség volt nemzeti szabályozási keret megteremtésére is, a már meglévő Uniós ajánlásokon és az akkor még hatályban lévő 95/46/EK irányelven felül, ennek következtében született meg a köznyelvben infotörvényként ismert jogszabály. Az infobiztonsági törvény (ibtv.) az állami és önkormányzati hatáskörben gyűjtött és kezelt adatokkal kapcsolatosan fogalmazott meg alapelveket, valamint eljárást ezeknek az adatoknak a kezeléséről. 2016-ban jelent meg ajánlás az Általános Adatvédelmi Rendelet (GDPR) tekintetében, amely egy 2 éves periódust kínált fel a tagállamok számára, hogy a jogharmonizációt érvényre juttassák a nemzeti jogszabályi keretrendszerükben. Az illegális migráció okozta közigazgatási nyomás következtében, 2018-ban az Európai Parlament és a Tanács rendeletben korlátozta a kiutasítás és a schengeni övezetben jogosulatlanul tartózkodó személyek mozgását, ezeknek a szemé-

lyeknek azonosítását részben biometrikus módszerek alkalmazásával is kiszolgálta (pl. ujjnyomat-, arcfelismerés alapú azonosítás). Sportrendezvényekre való könnyebb beléptetés gyanánt, valamint az ilyen eseményeken gyakran előforduló rendbontás következtében a 2004-es sporttörvény módosítására került sor, melynek során bevezetésre kerültek biometrikus azonosítási eljárások is.

## KONKLÚZIÓ

Vészhelyzetben, vagy amikor biztosságérzetünk bármilyen szempontból gyengül, könnyen lemondunk bizonyos szabadságfokokról annak érdekében, hogy az életünk visszazökkenjen a megszokott kerékvágásba. A koronavírus idején (2020) könnyen indokolható közösségi érdekekkel, hogy a mobiltelefonunk lokációs információi alapján visszakövethető legyen, kikkel érintkeztünk az elmúlt időszakban, és ezzel gátoljuk a vírus terjedését. Vagy megosszuk utazási információinkat a hatóságokkal. Ehhez jó alapot ad a környező országok és hazánk kormánya által meghirdetett rendkívüli helyzet és különleges jogrend, ami itthon amúgy is igen széles lehetőségeket biztosít. De mi garantálja, hogy ezek az információk nem kerülnek illetéktelenek kezébe, vagy, hogy az állami szervek nem használják fel biometrikus azonosítóinkat, kapcsolati adatainkat, szokásainkat profilozásra és a kinyert adatokat később saját céljaikra? Szükség lenne egy ilyen helyzethez illeszkedő, kétharmados törvényekkel és rendkívüli helyzetekben sem felülírható szabályozásra, mely védi a polgárok személyes adatait és jogait, ugyanakkor a biztonság növelése mellett sem ad lehetőséget a visszaélésre. Ha hallgatunk a vészjósló hangokra, a jövőben is fel kell készülni a koronavírushoz hasonló, globális katasztrófahelyzetekre. Az ilyen helyzetekben a biztonság megnövelése mellett szólnak a fokozódó munkanélküliség miatt szaporodó bűnesetek, vagy az újra felerősödő terrortámadások. Mi történne, ha terrorszervezetek, kihasználva a zavaros időszakot támadást indítanának mondjuk közművek ellen? Erre idejében fel lehetne készülni, minden technológia adott, könnyen kialakítható lenne olyan AI-val támogatott arc és járás felismerő megoldás, amelyekkel automatizáltan védhetők lennének eddig nem fókuszban lévő közművek, például nagyobb települések vízbázisai, vagy víztisztító, vízellátást biztosító telepek. A jövő legnagyobb kincse a víz lesz, ezért ezek védelmére kiemelt figyelmet kellene fordítani! De könnyen belátható, hogy amíg nincs egységes, a demokratikus értékrendekhez jobban igazodó (pl. Európai Uniós) szabályozás és kontroll, addig azokban az országokban, ahol a biometrikus adatok gyűjtése és felhasználása elterjedőben van, ott a visszaélések száma is várhatóan magas lesz.

A koronavírushoz hasonló epidemiológiai események jó táptalajt adhatnak a biometria terjedésének, mely kihat majd más területekre is. Gondoljunk bele, milyen egyértelmű lehetőség lenne biometrikus azonosítási elven működő országgyűlési választási rendszert fejleszteni (online állampolgári azonosító elve), vagy az egészségügyben betegazonosításra, recept kiváltásra vagy távoli ügyintézésre használni az ilyen rendszereket. Persze a világ számos pontján már sziget megoldásként történtek ilyen területen fejlesztések, de ezek elterjedése és az egységes szabályozás még várat magára. A kockázatok figyelembevételével, ha magasabb szintű biztonságra van szükség vagy az elvárás nagyobb, akkor többféle azonosító faktor használata a megoldás a megfelelő szabályozás és kontroll mellett.

## HIVATKOZÁSOK

[1] J. Renaghan, „Etched in stone," The Zoogoer, 1997.
[2] 13 Kr. e. 1792-1750 vagy Kr. e. 1728-1686 között uralkodott.
[3] Marcello Malpighi a Bolognai Egyetem anatómiaprofesszora, (1628-1694).
[4] K. FÖLDESI, „A DAKTILOSZKÓPIA FUNKCIONÁLIS TÖRTÉNETE," [Online]. Available: hadmernok.hu/153_01_foldesik.pdf. [Hozzáférés dátuma: 16 december 2019].
[5] d. H. A. T. dr. GÁBOR Béla, Dactyloscopia, Budapest: Országos Központi Nyomda Részvénytársaság, 1905.
[6] M. I. O. C. KOVÁCS Tibor, „A biztonságtudomány biometria aspektusai," [Online]. Available: http://www.pecshor.hu/periodika/XIII/kovacsti.pdf. [Hozzáférés dátuma: 10 november 2019].
[7] G. KETSKEMÉTY, Biometrián alapuló személyazonosító rendszerek, Budapest: Budapest Műszaki Főiskola Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2008.
[8] GUARDWARESYSTEMS, „Távoli személyazonosítási technikák," [Online]. Available: http://oldweb.mit.bme.hu/eng/research/search/downloads/tst/Irodalomkutatas.pdf. [Hozzáférés dátuma: 21 február 2020].
[9] B. C. GÁLAI Bence, „Járás alapú személyazonosítás és cselekvés felismerés LIDAR szenzorokkal," [Online]. Available: https://eprints.sztaki.hu/9175/1/Galai_1_3239040_ny.pdf. [Hozzáférés dátuma: 10 március 2020].
[10] „Chinese 'gait recognition' tech IDs people by how they walk," [Online]. Available: https://apnews.com/bf75dd1c26c947b7826d270a16e2658a. [Hozzáférés dátuma: 5 március 2020].
[11] „US Army infrared drone camera," [Online]. Available: https://www.army.mil/article/230293/researchers_tackle_challenges_of_tomorrow_with_new_infrared_drone_camera. [Hozzáférés dátuma: 13 február 2020].
[12] Securinfo, „Viselkedés alapú biometria," [Online]. Available: https://www.securinfo.hu/termekek/biometria/3735-behavioral-biometrics-viselkedesalapu-biometria.html. [Hozzáférés dátuma: 29 január 2020].
[13] SecuriFocus, „BlackBerry viselkedés alapú biometria," [Online]. Available: https://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=6965. [Hozzáférés dátuma: 11 Március 2020].
[14] „Fujitsu BIOaaS solution," [Online]. Available: https://www.fujitsu.com/ca/en/Images/Biometrics-as-a-Service_BIOaaS-Flyer.pdf. [Hozzáférés dátuma: 10 február 2020].
[15] F. &. Sullivan, „Biometric As a Service," [Online]. Available: https://www.fujitsu.com/caribbean/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf. [Hozzáférés dátuma: 11 március 2020].
[16] F. &. Sullival, „Cloud-based Identity and Authentication," [Online]. Available: https://www.fujitsu.com/caribbean/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf. [Hozzáférés dátuma: 16 január 2020].

[17] SecuriFocus, „Fujitsu viselkedés alapú biometria AI támogatással," [Online]. Available: https://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=7786. [Hozzáférés dátuma: 17 február 2020].
[18] „Londoni arcfelismerés bevezetése," [Online]. Available: https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment. [Hozzáférés dátuma: 20 március 2020].
[19] „Clearview közösségi média alapú arcfelismerési megoldása," [Online]. Available: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing. [Hozzáférés dátuma: 4 február 2020].
[20] „Google arcfelismerés," [Online]. Available: https://www.cnet.com/news/google-vows-not-to-sell-its-facial-recognition-technology-for-now/. [Hozzáférés dátuma: 22 február 2020].
[21] „EU drops idea of facial recognition ban in public areas," [Online]. Available: https://ca.reuters.com/article/idUSKBN1ZS37Q. [Hozzáférés dátuma: 14 március 2020].
[22] „Guidance for Regulation of Artificial Intelligence Applications," [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. [Hozzáférés dátuma: 15 március 2020].
[23] MagyarországKormánya, „T/7690. számú törvényjavaslat," [Online]. Available: https://www.parlament.hu/irom41/07690/07690.pdf. [Hozzáférés dátuma: 26 február 2020].
[24] „Az igazoltató rendőr akár arcfelismerő szoftvert is használhat," [Online]. Available: https://index.hu/belfold/2019/12/10/az_igazoltato_rendor_akar_arcfelismero_szoftvert_is_hasznalhat/. [Hozzáférés dátuma: 24 február 2020].
[25] „Beijing Normal University facial scanner," [Online]. Available: http://www.xinhuanet.com//english/2017-09/12/c_136604144.htm. [Hozzáférés dátuma: 14 március 2020].
[26] Techjuice, „Intelligent Classroom Behavior Management System," [Online]. Available: https://www.techjuice.pk/this-school-scans-classrooms-every-30-seconds-through-facial-recognition-technology/. [Hozzáférés dátuma: 13 március 2020].
[27] „A Kínai kreditrendszer," [Online]. Available: www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html?utm_source=reddit.com. [Hozzáférés dátuma: 20 február 2020].
[28] https://hvg.hu/tudomany/20180919_kina_tarsadalmi_kreditrendszer_hogyan_mukodik_pontszam_megfigyeles_digitalis_diktatura, A Kínai kreditrendszer, HVG, 2018.
[29] „Biometric data and data protection regulations (GDPR and CCPA)," 27 02 2020. [Online]. Available: https://www.gemalto.com/govt/biometrics/biometric-data. [Hozzáférés dátuma: 25 03 2020].
[30] European Data Protection Board, „Guidelines 3/2019 on processing of personal data," 10 07 2019. [Online]. Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf. [Hozzáférés dátuma: 01 04 2020].
[31] United Kingdom Parliament, „Data Protection Act," UK, 2018.
[32] H. S. Chau A., „n act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.," California, 2018.
[33] Office for Personal Data Protection, „School with students' fingerprints," 05 03 2020. [Online]. Available: https://uodo.gov.pl/pl/138/1453. [Hozzáférés dátuma: 01 04 2020].

[34] Forrester Research, „The growing legal and regulatory implications of collecting biometric data," 17 05 2019. [Online]. Available: https://www.zdnet.com/article/the-growing-legal-and-regulatory-implications-of-collecting-biometric-data/. [Hozzáférés dátuma: 25 03 2020].
[35] A. S. Wernick, „Biometric Information – Permanent Personally Identifiable Information Risk," 14 02 2019. [Online]. Available: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/. [Hozzáférés dátuma: 25 március 2020].
[36] P. Kovacsics, „Biometric Authentication at the Workplace: Risks and Legal Challenges," 28 08 2019. [Online]. Available: https://www.hrtechnologist.com/articles/hr-compliance/biometric-authentication-at-the-workplace-risks-and-legal-challenges/. [Hozzáférés dátuma: 25 03 2020].
[37] C. Burt, „Legal issues around facial biometrics use examined in U.S., Canada, and UK," 03 02 2020. [Online]. Available: https://www.biometricupdate.com/202002/legal-issues-around-facial-biometrics-use-examined-in-u-s-canada-and-uk. [Hozzáférés dátuma: 25 03 2020].
[38] A. Tibbitt, „Biometrics watchdog will lack powers, say critics," The Ferret, 23 07 2018. [Online]. Available: https://theferret.scot/scottish-biometrics-commissioner-enforcement-powers/. [Hozzáférés dátuma: 31 március 2020].

# SOCIAL ENGINEERING AND MANIPULATION TECHNIQUES AND METHODS - RESEARCH REPORT

# A SOCIAL ENGINEERING ÉS A MANIPULÁCIÓS TECHNIKÁK ÉS MÓDSZEREK - KUTATÁSI JELENTÉS

KOLLÁR Csaba[1], ZAKAR Ákos[2]

**Abstract**

In the first part of our study [1], we reviewed the theoretical summary of the topic, focusing on the manipulation methods and techniques that can be related to the human soul, psychology, interpersonal communication, and also appear in the field of information security. The techniques and methods were presented along the human and IT-based divisions, and we also covered the criminal law aspects of the topic. In the second – present – part we present the results of our own research. Based on the responses to our online, large-sample questionnaire, we first provided a demographic description of the sample, then presented the responses by questions, and then analyzed the responses by group composition. In our research, we examined three hypotheses aimed at the use of passwords, the use of operating systems, and the recognition of the dangers inherent in phishing emails. After examining the relationship between the questions, we concluded our study with conclusions on the achievement of safety awareness, focusing on survey, regulation and knowledge transfer.

**Keywords**

information security, social engineering, manipulation, research report

**Absztrakt**

Tanulmányunk első részében [1] a téma elméleti összefoglalását tekintettük át, s elsősorban azokkal a manipulációs módszerekkel és technikákkal foglalkoztunk, melyek az emberi lélekhez, a pszichológiához, a személyközi kommunikációhoz köthetőek, s megjelennek az információbiztonság területén is. A technikákat és módszereket a humán, illetve IT alapú felosztás mentén mutattuk be, s kitértünk a téma büntető törvénykönyvi vonatkozásaira is. A második – jelen – részben saját kutatásunk eredményeit ismertetjük. Az online, nagymintás kérdőívünkre kapott válaszok alapján először a minta demográfiai leírását adtuk meg, majd a kérdésenkénti válaszokat mutattuk be, ezt követően pedig a csoport összetétele szerinti válaszokat elemeztük. Kutatásunkban három hipotézist vizsgáltunk, melyek a jelszavak használatára, az operációs rendszerek használatára, illetve az adathalász e-mail-ekben rejlő veszélyek felismerésére irányultak. A kérdések közötti kapcsolat vizsgálata után tanulmányunkat a biztonságtudatosság elérésére vonatkozó, felmérésre, szabályozásra, ismeretátadatásra fókuszáló következtetésekkel zártuk.

**Kulcsszavak**

információbiztonság, social engineering, manipuláció, kutatási jelentés

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | associate professor/egyetemi docens | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] zakarakos85@gmail.com | ORCID: 0000-0002-3919-4098 | information security expert/információbiztonsági szakértő | állami tulajdonú gazdasági társaság

## KUTATÁSMÓDSZERTANI ALAPVETÉS

Primer kutatásunk célja az volt, hogy egy közel kétszáz fő részvételével az információbiztonság tudatossággal kapcsolatos felhasználói véleményeket ismerjünk meg, s ezek feldolgozása és kielemzése után megalapozott következtetéseket vonjunk le, illetve, hogy szervezeti szinten is alkalmazható javaslatokat fogalmazzunk meg. A kvantitatív kutatási módszerek közül a kérdőívet választottuk, ennek elkészítésénél módszertanában többek között Babbie [2], Cseh-Szombathy és Ferge [3], Freedman és szerzőtársai [4], Moksony [5], Sajtos és Mitev [6], Scipione [7], Malhotra [8] műveire hagyatkoztunk. A kérdőív feldolgozásánál és az eredmények értékelésénél nevezett szerzők mellett elsősorban Bornemissza [9], Reidmacher [10] és Tóthné [11], [12] javaslatait és ajánlásait vettük figyelembe. Kérdőívünk kérdéseinek összeállításánál egyebek mellett Oroszi [13] 2008-ban végzett szekunder kutatását tanulmányoztuk, s így egy 40+1 kérdésből álló kérdőívet készítettünk a Google Űrlapok (Forms) segítségével. A 41. kérdés egy nyitott kérdés volt, melyben a kitöltők szöveges formában írhatták le véleményüket a kérdőívvel, illetve a témával kapcsolatban. A kérdőív kérdéseinél egyaránt alkalmaztunk nyitott, zárt és hibrid kérdéseket, így a válaszadási lehetőségeknél a feleletválasztós, a jelölőnégyzetes és a szabad szöveges mezők egyaránt szerepeltek lehetőségként. Az elkészült kérdőív linkjét – a GDPR előírásainak figyelembe vételével – saját ismeretségi körben (levelezőlista, telefonkönyv, Facebook ismerősök) osztottuk meg. A kitöltésre 2020. március 31. és 2020. április 8. között adtunk lehetőséget. A lekérdezési szakasz zárásakor 216 érvényes kérdőívet számoltunk össze.

## KÉRDÉSENKÉNTI VÁLASZOK (KIVONAT)

A kérdésekre adott válaszoknál – terjedelmi okok miatt – bizonyos kérdésekre adott válaszokat nem, vagy csak lényegesen rövidebb terjedelemben (összegezve) ismertetünk.

### Általános és demográfiai kérdések

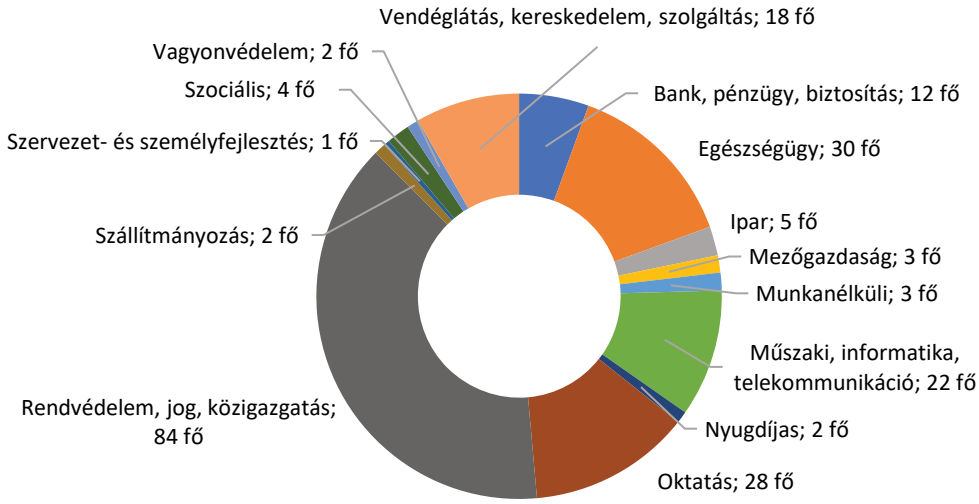
A kutatásmódszertani alapvetésben már leírtuk, hogy összesen 216 érvényes kérdőívet számoltunk össze. A mintánk demográfiai leírását a nem, az életkor, a végzettség, a munkaviszony és a munkahely ágazati besorolása alapján adjuk meg.

| Generációk | | Nők | | Férfiak | |
|---|---|---|---|---|---|
| *elnevezés* | *életkor* | *%-os arány* | *fő* | *%-os arány* | *fő* |
| Baby boomer | 56-74 | 10,2 | 22 | 2,3 | 5 |
| X generáció | 41-55 | 20,8 | 45 | 21,2 | 46 |
| Y generáció | 26-40 | 23,1 | 50 | 18,5 | 40 |
| Z generáció | 11-25 | 1,8 | 4 | 1,8 | 4 |
| Összesen | | 56 | 121 | 44 | 95 |

*1. táblázat: a válaszadók neme és életkora közötti megoszlás (saját szerkesztés)*

Válaszadóink többsége (66%) felsőfokú végzettséggel (főiskola, egyetem) rendelkezik, ezt követi a szakközépiskola és gimnázium (30%). A vizsgált csoportnak valamivel több, mint a fele (50,5%-a) közszférában dolgozik, a versenyszférában 31,9%-uk vállal munkát alkalmazottként. 6,9%-uk közép- és felsővezető, 4,2% cég ügyvezetője vagy tulajdonosa valamely társas vállalkozásnak. Egyéni vállalkozóból 6 fő van, tanulóból 2 fő, al-

kalmi munkavállalóból 1 fő, valamint 5-en vannak, akik valamilyen oknál fogva nem aktívak a munkaerőpiacon. A válaszadók munkahelyének ágazati megoszlása az első ábrán látható.




*1. ábra: a válaszadók munkahelyének ágazati besorolása (saját szerkesztés)*

A válaszadók több, mint egyharmada (38,8%-a) a rendvédelem, jog, közigazgatás területén dolgozik. 13,8%-a az egészségügyből jött, 12,9%-uk oktató, nevelő tevékenységet végez. 10,2%-a műszaki, IT, telekommunikációs szektorból, 8,3%-uk vendéglátás, kereskedelem és szolgáltatás területéről, 5,5%-uk a pénzügyi világból érkezett. A fennmaradó 10,5% megoszlik a mezőgazdaság, ipar, vagyonvédelem, szállítmányozás, szociális dolgozók és az 5 fő inaktív között.

**Jelszóhasználat**

A jelszóhasználattal kapcsolatban öt kérdést tettünk fel, úgymint: (1) Használ-e ugyanolyan jelszavakat magán és munkahelyi fiókjaihoz? (2) Ismeri-e más a privát vagy munkahelyi fiókjai jelszavát? (3) Hogyan választja meg a használni kívánt jelszavait? (4) Milyen gyakran változtatja a jelszavait? (5) Hol tárolja a jelszavait?

A kérdésekre adott válaszok alapján megállapítottuk, hogy szinte azonos eredményt kaptunk a jelszavak megválasztása és a jelszavak másokkal való megosztása vonatkozásában. A válaszadók 30%-a használ ugyanolyan jelszavakat a magán és munkahelyi fiókjaihoz, míg 28,7%-uk másokkal meg is osztja ezen jelszavakat. A fennmaradó többség már óvatosabb e tekintetben, más jelszavakat használ privát és munka célra, valamint ezek bizalmasságára is vigyáz. A jelszó megválasztásánál a legkockázatosabb verziót, miszerint alapértelmezett jelszavakat használ, csak 2,3%-uk, mindössze 5 fő választotta. Bár hozzá kell tenni, hogy ez nagyon sok alkalmazás esetén csak ideiglenes opció. Egy új rendszerhez történő hozzáférés esetén két út áll a felhasználó előtt. Így a másik két tábor közel azonos arányban képviselteti magát. Személyhez köthető, rövid, könnyen megjegyezhető jelszavakat 51,4%-uk használ. Bonyolult, egyedi, hosszú jelszavakat különféle típusú karakterekkel

46,3%-uk alkalmaz. A jelszó megváltoztatás gyakoriságára tekintettel három táborra oszthatók a válaszadók. Lényegében minden második ember (56%-uk) csak kötelező jelleggel, a rendszer által előírt időközönként változtatja jelszavát. 28,7%-uk csak akkor változtatja meg, ha elfelejtette, vagy ha újat kell igényelni. A legkevesebben, (15,3%) azok vannak, akik tudatosan, rendszeresen saját maguk által meghatározott gyakorisággal változtatják jelszavukat. A jelszavak tárolására vonatkozóan túlnyomó többségük (közel 60%) a hagyományos tárolást választotta, vagyis az emlékei közt, saját memóriájában tárolja jelszavait. A realitások talaján maradva további négy lehetőséget kínáltunk fel. A legveszélyesebb tárolási módot 2,3%-uk alkalmazza, vagyis akiknél a számítógépük mellett van felírva a jelszavuk. A maradék három opciót, a biztonságos megoldást választók jelölték be. Nagy különbség nem mutatkozik a jelszómanagert használók 10,6%-a, és a titkosított megoldást választók közt. Utóbbinál fájlban vagy mobiltelefonon történő jelszótárolást 8,6%-uk használja. Kevésbé biztonságos, ugyanakkor hagyományos módszert választott 18,5%-uk a válaszadóknak, akik elrejtett, elzárt füzetben felírva őrzik jelszavaikat az illetéktelenek elől.

**Informatikai védelem**

Az informatikai védelemmel kapcsolatban összesen tizenegy kérdést tettünk fel, az ezekre adott fontosabb válaszokat alább foglaljuk össze. A válaszadók rendszerint fontosnak tartják a vírusvédelmi eszközök meglétét a különböző eszközeiken, ugyanakkor a három alapvető eszközfajta (számítógép, tablet, mobiltelefon) együttes védelmét csak közel 18% jelölte be. A vírusvédelmi szoftverek kiválasztásánál a válaszadók harmada (35,5%) kizárólag ingyenes programokat használ, míg kicsivel kevesebb, mint harmaduk (31,8%) olyan megoldás mellett dönt, ami a szokásainak leginkább megfelelő. 15,2%-uk törekszik rá, hogy ár/érték arányban a legtöbb tudást nyújtó megoldást válassza és 17,5%-uk megbízik ismerősei ajánlásában. A munkahelyi vírusvédelmi szoftverekkel kapcsolatban a válaszadók közel 60%-a nem tudta megnevezni, hogy milyen védelmi szoftvereket használ az adott szervezet/vállalat. A munkaállomástól rövid időre való felállást követő egyszerű biztonsági mozdulat[3] betartását 59,2%-uk veszi komolyan, míg 31,9%-uk semmit nem tesz annak érdekében, hogy más nem nyúljon a felügyelet nélkül hagyott számítógépéhez. A maradék 8,9% megoszlik az olyan választ adók közt, akik operációs rendszerén be van állítva az automata zárolási funkció. A válaszadók többsége (60,6%-a) már használt saját pendrive-ot munkahelyi számítógépben, vagy fordítva: vállalati pendrive-ot saját gépben. A többi 39,4%-uk ennek elkerülésére figyelmet fordít. Az informatikai eszközök (laptop, tablet, mobiltelefon) és adathordozók elvesztésével, ellopásával kapcsolatban a megkérdezettek közül 35-en már voltak áldozatai lopásnak. 24 főnél mobiltelefon, 9 főnél adathordozó, 1 főnél laptop, 1 főnél mobiltelefon és adathordozó bánta a gazdája nem megfelelő figyelmét. Köztük 42,8%-uk nem használt semmiféle titkosítási eljárást, így adataik mások számára is ismertté válhattak. A szervezeti információbiztonság szempontjából kényes kérdés, hogy mit tesz a munkavállaló, amikor a munkahelyén gazdátlan adathordozót talál. A válaszadók túlnyomó többsége (78,8%-a) még nem találkozott ilyen esettel. 18,1%-a becsületes és óvatos megtalálóként leadta egy olyan személynek a cégen belül, aki meg tudta tenni a szükséges intézkedéseket, hogy az adathordozó – feltéve, hogy szervezeten belül

[3] A leggyakrabban használt Windows operációs rendszeren az automatikus zárolás funkció, WINDOWS gomb + „L" billentyű kombinációval kiléptet az adott fiókból.

kell keresni – visszajusson a gazdájának. A válaszadók 1,9%-a teljes passzivitást tanúsított, nem foglalkozott a talált tárggyal, míg 1,4%-a, azaz 3 fő volt olyan bátor és megnézné annak tartalmát a céges vagy az otthoni számítógépen. Utóbbiak a csalizás áldozatai, mellyel akár egy komplett vállalati infrastruktúrát is lefertőzhetnek kártékony programmal.

Kíváncsiak voltunk arra is, hogy a megkérdezettek hogyan viszonyulnak a vezeték nélküli (WiFi) kommunikáció biztonságához. A válaszadók közel fele (46,3%) az otthoni router gyárilag beállított jelszavait használja, míg az egy fokkal jobb megoldást választók (41,7%) legalább az eszköz telepítésekor megváltoztatták az eszköz alapértelmezett jelszavát. A biztonságot szem előtt tartók mindössze 12%-kal vannak, ők azok, akik rendszeresen megváltoztatják WiFi jelszavukat. A nyilvános WiFi hálózatra történő csatlakozásnál a vizsgált minta több mint fele (51,9%) nem használja ezt a fajta megoldást, inkább a mobil internet adta lehetőségekre támaszkodik. Teljesen egyforma azon válaszadók száma, akik különösebb aggodalom nélkül felcsatlakoznak nyilvános hálózatokra, ők 20,8%-nyian vannak. Akik abban a hiszemben vannak, hogy egy jelszóvédelem – a titkosítás ismerete nélkül – megvédheti őket, szintén ugyanennyien képviseltetik magukat. Az IT biztonsághoz értőknek neveznénk azt a 6,5%-nyi 14 fős csoportot, akik felcsatlakoznak ugyan nyilvános WiFi hálózatra, de ezt követően egy biztonságos VPN csatornán keresztül élvezik az ingyenes internet adta lehetőségeket.

A mobiltelefonos applikációk, vagy számítógépes programok frissítésével, törlésével kapcsolatban 53,2%-uk automatikusan a rendszerre bízza az update-et, 42,6%-uk manuálisan hajtja végre a telepítést és törlést. A válaszadók 4,2%-a azonban felesleges dolognak tartja a szoftverek frissítését, e biztonsági műveletben csak az alkalmazás kinézetének esetleges megváltoztatása tölti el aggodalommal.

**Fizikai biztonság**

A fizikai biztonsággal kapcsolatos kérdések a beléptető rendszerre és az otthon felejtett belépésre jogosító kártyára/kulcsra vonatkoztak. A munkahelyükön lévő beléptető rendszerrel kapcsolatban a kulccsal nyitható ajtózár (61%) mellett sokan megjelölték még az élőerős védelmet (41,2%), a mágneskártyát (24,7%), valamint a belépőkód alkalmazását (20,8) és az ujjlenyomat olvasót is (2,3%). Az aktív dolgozók közül 6 személy semmiféle védelmet nem jelölt be, ami a belépést biztosítaná a munkahelyén. Mivel a jelölő négyzetes választási módok mellett egyéb lehetőséget is kínáltunk a válaszadásra, így páran beírták még a kulcsdoboz, proxy, vagy a riasztó használat mellett a „semmilyen” és „nincs” válaszokat. A válaszadók 63,9%-ával fordult már elő, hogy belépésre jogosító kártyáját, kulcsát otthon hagyta. A következő ráépülő feltételes válaszban arra voltunk kíváncsiak, hogy ezen személyek hogyan jutottak be ezt követően a munkahelyükre. A feledékeny dolgozók közül 39,7%-a más kolléga jogosultságával, vagy kulcsával jutott be a munkahelyére. Jóval többen (57,7%) választották a hivatalos utat, azaz a portaszolgálathoz fordultak. 2,6%-uk azonban olyan bejáratot választott, ahol ilyen jellegű intézkedések nem voltak szükségesek.

**Biztonságtudatosság**

A válaszadók biztonságtudatosságát öt kérdés segítségével vizsgáltuk meg. A válaszolóknak szinte a fele (49,5%) már elolvasta a munkahelyük információbiztonsági szabályzatát, míg 39,8%-uk nem. 6,5%-uk kategorikusan kijelentette, hogy náluk ilyen nincs, míg

4,2% volt azok aránya, akik nem tudták miről van szó, számukra ismeretlen ez a dokumentum. A megkérdezettek 17,6%-a már használta munkahelyi e-mail címét magánjellegű levelezésre, valamint 10,2%-uk ezzel a címmel már regisztrált is különböző weboldalakon, feliratkozott hírlevelekre. A nagy többség azonban ilyen módon nem ossza meg munkahelyi email címét másokkal. A közösségi oldalak használatát illetően a Facebook és a LinkedIn weboldalakat szándékosan egy kérdésbe tettük bele, mivel egy social engineering támadás információszerzési fázisa szempontjából nincs relevanciája, hogy a célszemély ellen melyik platformról szerzi be az adatokat a támadó. Egy-egy válaszadó volt, aki nem rendelkezik ilyen profillal, kamu profilt használ vagy tanulmányait, illetve szakmai önéletrajzát a LinkedIn-en megosztja, a Facebook-on viszont nem. Legtöbben nevüket (85,2%), fényképüket (68,5%), jelenlegi (27,8%) és korábbi munkahelyüket (15,7%), telefonszámukat (9,3%), valamint lakcímüket (2,8%) is közzéteszik.

**Szoftverhasználat**

Az otthoni és munkahelyi operációs rendszerek használatánál közel azonos eredmény született a két környezetnél. A Windows 10 vezet mind az otthoni (71,7%), mind a munkahelyi (74,5%) felhasználásnál. A Windows 8 esetén a munkahelyi területen több, mint háromszor annyian használják (11,1%), mint az otthoni környezetben, ahol csak 3,2%. Munkahelyükön 9,2% használja még a kockázatos Windows 7-es operációs rendszert. A Linuxot használók aránya szinte azonos, munkahelyen 3,7%-uk, otthon 3,2%-uk használja. A macOS nem számít elterjedt rendszernek, mindössze 3-an használják otthoni, köztük 1 fő pedig munkahelyi célra is. Volt néhány olyan válaszadó, aki több lehetőséget is bejelölt. Legtöbben, mintegy 73,1% saját tapasztalás útján, valamint 32,4%-uk ismerősök által tanulták meg a szoftverek használatát. Munkahelyi oktatás keretében szinte minden ötödik fő szerepelt, de találkozhatunk még a használati útmutató, könyvek, videók alapján történő tanulással is, ők 14%-al voltak. A legkevesebb jelölés az iskolai oktatás mellett szólt. Az ismeretlen hibaüzentre való reagálási helyzetet vizsgáló kérdésnél két közel azonos nagyobb és egy kis táborra oszlik meg a válaszadók aránya. 44,9%-uk a rendszergazdát értesíti első körben, míg 46,3%-uk megpróbálja rá megkeresni a megoldást – akár a kollégák bevonásával is – és csak végső soron jeleznék azt a help desk személyzetnek. Közel minden tízedik ember nem foglalkozik vele, mivel szerinte nem az ő dolga az ilyen jellegű informatikai problémák kezelése.

**Veszélyhelyzetek felismerése**

A válaszadóknak egy harmada, azaz 33,3%-a nem foglalkozik vele, ha a kollégája mögötte áll meg, miközben egy adott rendszerben megpróbál bejelentkezni. 39,8%-uk már felismeri az ebben rejlő kockázatot és inkább a másik elől takarva, gyorsabban gépelve próbálja megóvni jelszavát társa elől. Kb. egynegyedük pedig nem bízza a véletlenre a saját hitelesítő adatainak megismerését mások részére, megkéri kollégáját, hogy álljon arrébb, ezzel elejét véve a váll fölötti leskelődésnek. A munkahelyi témákról való beszélgetést vendéglátóhelyeken vagy tömegközlekedési eszközökön 52,8%-uk kerüli, 41,2%-uk pedig igyekszik rövidre fogni és halkan átadni a szükséges információkat. 6%-uk (13 fő) viszont ilyen jellegű dologgal nem foglalkozik, így hallgatózással könnyen bizalmas információk

juthatnak illetéktelenek fülébe. A munkahelyi szükségtelen iratok megsemmisítésére vonatkozóan is több válaszadási lehetőséget lehetett bejelölni. A kitöltök közel kétharmada a kötelező iratmegsemmisítő használatát választotta, őket követik azok, akik külön zsákba teszik a selejtes iratokat (22,7%). A felelőtlen megoldást választóknak két szintje van, akik a kommunális szemetesben dobják ki (17,1%), valamint akik hazaviszik elégetés vagy papírgyűjtés céljából (8,3%). Utóbbi két megoldás egyike sem nyújt biztonságot a kukabúvárkodás ellen. A munkaállomás takarítás közbeni védelmére vonatkozóan a válaszadók mintegy fele, 47,7%-a megteszi a szükséges intézkedést, azaz lezárja a szekrényeivel, fiókjaival együtt. Jóval biztonságtudatosabb az a 9,7%, akik a fizikai eszközei védelme mellett folyamatosan nyomon követik a takarító személyzetet munka közben. 21,3%-uk lezárja a számítógépét, de a dokumentumai elzárására nincs lehetősége. Ugyanennyien vannak teljes bizalommal a kisegítő személyzet iránt, nem hiszi, hogy az ő irataival foglalkozna, így nem is tesznek semmilyen óvintézkedést. Az ő esetükben könnyű lehetőség mutatkozik akár egy hardveres keylogger telepítésére, akár dokumentumok fotózására is. A belső információk gondatlan kiszivárogtatására vonatkozó kérdésünk egy ismeretlen kollégával szembeni telefonos kommunikációra utalt, aki konkrét információt szeretne megtudni. Tipikusan ilyen lehet egy megszemélyesítéses támadás. A válaszadóknak pontosan a fele választotta azt, hogy elérhetőséget és visszahívást kér. Minden ötödik, vagyis 19,4%-uk a hívás közbeni ellenőrzés módját választotta, míg szinte azonos aránnyal 19,9%-kal vannak azok, akik elhiszik, hogy valóban a munkatársukkal beszélnek. A fennmaradó 10,7% megoszlik az egyedi válaszokat adók közt. Ide sorolhatóak azok, akik semmilyen ügyben nem adnak tájékoztatást, ismerik kollégájukat, hivatalos megkeresést vagy belső e-mailt kérnek, továbbkapcsolják a vezetőjüknek stb. közt. Azzal kapcsolatban, hogy végrehajtanának-e felettesük nevében e-mailen kapott sürgős pénzügyi műveletet, közel minden tízedik megkérdezett igennel válaszolt, nem lát benne semmi veszélyt, ezzel potenciális résztvevői egy BEC (Business Email Compromise) típusú támadásnak. A válaszadók több mint fele (52,8%) más csatornán is megerősítést kérne és 38,9%-a pedig felismerné a jogtalan próbálkozást és jelentené az illetékeseknek. Az ismeretlen feladótól érkező vagy közüzemi szolgáltatóktól kapott mellékletekre 13,9%-uk azonnal rákattintana, letöltené őket, ezzel adathalász támadásnak téve ki magát. 10,2%-uk csak biztonságos zárt környezetben nyitná meg az e-mailt és mellékleteit. Meglepő, hogy közel háromnegyedük, 72,2%-uk pedig alapos elemzés után valószínűleg a törlés mellett döntene. A válaszadók maradék 3,7%-a is a biztonságos megoldást választaná, azaz a törlést, valamint figyelmen kívül hagyást választaná.

## A CSOPORT ÖSSZETÉTELE SZERINTI VÁLASZOK

Annak érdekében, hogy a válaszok, illetve a válaszok kapcsolódásának rejtett dimenzióit is meg tudjuk vizsgálni, mintánkat több szempont szerint is összehasonlítottuk, s a válaszok meghatározott szempont (pl.: nem, életkor) szerinti bontása után a fontosabb kérdésekre adott válaszok hasonlóságát-különbségét vizsgáltuk rendszerint kereszttáblával. A fontosabbak megállapításokat alább közöljük.

## Nemek szerinti vizsgálat

| Kockázatok / Nemek | Nők (%) | Férfiak (%) |
|---|---|---|
| Ugyanolyan jelszavak használata magán és munkahelyi fiókoknál | 57 | 43 |
| Más által is ismert jelszavak használata | 61,3 | 38,7 |
| Érdeklődési körhöz tartozó rövid vagy alapértelmezett jelszavak használata | 62 | 38 |
| Soha vagy csak felejtés miatti jelszóváltoztatás | 81 | 19 |
| Számítógép mellé vagy füzetbe felírt jelszavak | 50 | 50 |
| Vírusvédelmi szoftverek használatának kerülése | 100 | 0 |
| Csak ingyenes (nem a felhasználói igényekhez, vagy ár/érték arányhoz szabott) vírusvédelmi szoftverek használata | 70,6 | 29,4 |
| Munkaállomások zárolásának kerülése a géptől való felállást követően | 64,7 | 35,3 |
| Pendrive munkahelyi és magán célú használata | 55,8 | 44,2 |
| Adathordozók titkosítás nélküli védelme | 65,3 | 34,7 |
| Talált adathordozó csatlakoztatása otthoni vagy céges számítógépre | 66,7 | 33,3 |
| Gyári jelszó használata otthoni WiFi routeren | 66 | 34 |
| Nyilvános, ingyenes WiFi használata | 64,5 | 35,5 |
| Automatikus rendszer, program frissítések mellőzése | 66,7 | 33,3 |
| Munkahelyi beléptető rendszer hiánya | 88,8 | 22,2 |
| Más belépési jogosultságának használata | 46 | 54 |
| Információbiztonsági Szabályzat szándékos el nem olvasása | 58,1 | 41,9 |
| Munkahelyi e-mail cím használata magáncélú levelezésre | 42,1 | 57,9 |
| Munkahelyi e-mail cím regisztrálása magáncélból hírlevelekre, webáruházba stb. | 45,4 | 54,6 |
| Közösségi oldalakon személyes információk megadása (pl. lakcím, telefonszám, munkahely) | 63,1 | 36,9 |
| Windows 7 vagy régebbi operációs rendszer otthoni használata | 58,1 | 41,9 |
| Bankkártya adatok, bejelentkezési adatok elmentése | 51,3 | 48,7 |
| Windows 7 vagy régebbi operációs rendszer munkahelyi használata | 80 | 20 |
| Ismeretlen számítógépes hibaüzenet figyelmen kívül hagyása | 68,4 | 31,6 |
| A belépési adatok leskelődéssel történő megismerésének figyelmen kívül hagyása | 54,2 | 45,8 |
| Nyilvános helyeken munkahelyi témákról való beszélgetés | 46,2 | 53,8 |
| Munkahelyi selejtes iratok kommunális hulladékként való kezelése vagy hazavitele | 77,4 | 22,6 |
| Számítógép le nem zárása takarítás alatt | 74 | 26 |
| Munkahelyi telefonon magát kollégának kiadó személy azonosságának nem ellenőrzése | 67,5 | 32,5 |
| Vezető nevében érkezett e-mail utasításának ellenőrzés nélkül végrehajtása | 63,2 | 36,8 |
| Ismeretlen feladó vagy közüzemi szolgáltató nevében érkezett email linkjének vagy mellékletének azonnali megnyitása | 70 | 30 |

*2. táblázat: nemek szerinti felosztás (saját szerkesztés)*

A táblázat adataiból jól látható, hogy a nők jobban ki vannak téve a social engineering típusú támadásoknak. Ha a fenti felsorolásból kiveszem azon kockázatos fenyege-

téseket (beléptetési rendszer hiánya, elavult operációs rendszer használat), melyek kiküszöbölése nem egy alkalmazott felelőssége, akkor a nők átlagosan 62,6%-a, a férfiak 37,4%-a tekinthető potenciális áldozatnak ebből a szempontból.

### Életkor szerinti vizsgálat

Az életkor szerinti vizsgálatot – ahogy arra korábban már utaltunk – a generációk szerinti felosztás szerint vizsgáltuk meg. Megállapítottuk, hogy az X generációs korosztály szerepel első helyen átlag 41,5%-kal, őket követi szorosan az Y generáció átlag 40,8%-kal. A Baby boomerek kockázatos válaszainak aránya 14,2% volt, a Z generációnál mindössze 3,4%. Nyikes [14] 2017-es kutatásában a 35 éves kort, mint vízválasztó vonalat húzta meg az informatikai eszközök és alkalmazások magabiztos használatában. Fontos megkülönböztetni a magabiztos és a biztonságtudatos használatot. Míg az előző gyakorlással elsajátítható képességet jelent, addig az utóbbi tudatos, veszélykerülő magatartás, melyet előzetes információszerzés nélkül nem lehet megvalósítani.

### Végzettség szerinti vizsgálat

Az iskolai végzettség és a kockázatos magatartás összefüggésének vizsgálata során megállapítottuk, hogy a kockázatos magatartást tanúsítóknál a felsőfokú szakképesítéssel rendelkezők közül kerülnek ki a legtöbben. Ennek okát abban látjuk, hogy esetükben rendszerint nem választódik élesen külön a hivatali- és a magánélet, az alacsonyabb végzettségűekhez képest sokkal többször, sokkal komolyabb döntést kell hozniuk, s emiatt (is) stresszesebb a munkájuk. A végzettség szerinti öt legnagyobb különbség felsőfokú végzettséggel rendelkezők, illetve nem rendelkezők között az egyes kérdések vonatkozásában csökkenő aránnyal a következő: talált adathordozó csatlakoztatása otthoni vagy céges számítógépre (100%), munkahelyi e-mail cím használata magáncélú levelezésre (81%), ugyanolyan jelszavak használata magán és munkahelyi fiókoknál (78,8%), pendrive munkahelyi és magán célú használata (77,9%), automatikus rendszer, program frissítések mellőzése (77,8%).

### Ágazatok szerinti vizsgálat

Az ágazatok szerinti bontás eredményéből megállapítható, hogy a 31 kockázatos viselkedési formából 23-ban a „rendvédelem, jog, közigazgatás” szektor áll a legrosszabb helyen, egy területen pedig az egészségüggyel azonos arányban szerepel. Ez az elkeserítő kép azt sugallja, hogy az állam működése szempontjából legnagyobb jelentőséggel bíró szektorból származott a legtöbb olyan válasz, mely a biztonságtudatos viselkedés hiányát mutatja a szervezeten belül.

## HIPOTÉZISVIZSGÁLAT

A nem, kor és munkahelyi adatoknak a kockázatokhoz való viszonyításán felül többféle relációban is vizsgáltuk az eredményeket, melyek során tanulságos megállapítások születtek. Kíváncsiak voltunk, hogy különböző magatartási viselkedési minták hogyan viszonyulnak egymáshoz, megállapítható-e köztük bármilyen összefüggés. Viszonyítási alapnak így több csoportot is meghatároztunk, majd hipotéziseket állítottunk fel, melyek statisztikai értékelése után levontuk belőlük a következtetést. A skálázást 25%-os léptékben 4

részre osztottuk fel. A felétől nagyobb előfordulást mutató, 50% feletti eredményeket már igaznak vettük a bizonyítás során.

**1. hipotézis**

*Azok, akik egyszerű jelszavakat használnak, az információ- és informatikai biztonság több területén is hanyag hozzáállással rendelkeznek.*

Definíciók és kérdéskör tisztázása: egyszerű jelszavak alatt a személyhez köthető vagy alapértelmezett jelszavak használatát értjük. Hanyag hozzáállás alatt a kérdőívünkben megfogalmazott szituációk mögötti kockázatos viselkedésformákat értjük, melyhez egyéni felelősség társítható. Így nem vettük figyelembe az értékelésnél a munkahelyi beléptető rendszer, illetve az elavult munkahelyi operációs rendszer használatát sem.

Értékelés: 28 db kérdés esetén a kockázatos válaszok megoszlása

| Arány (%) | 0 - 25 | 25 - 50 | 50 - 75 | 75 - 100 |
|---|---|---|---|---|
| Előfordulás (db) | 15 | 9 | 4 | 0 |

*3. táblázat: 1. hipotézis kérdéseinek megoszlása (saját szerkesztés)*

Következtetés: Mivel a 28 kérdésből csak 4 kérdésre kaptunk kockázatos választ – mely nem éri el az 50%-os határt – feltevésünk nem bizonyult igaznak. A kockázatos válaszok az alábbiak voltak: adathordozók titkosítás nélküli védelme (64,8%), pendrive munkahelyi és magán célú használata (61%) gyári jelszó használata otthoni WiFi routeren (60%), valamint a munkaállomás zárolásának kerülés a géptől való felállást követően (51,4%). Összefüggésként kiemeljük, hogy akik könnyű jelszavakat választanak maguknak, azok nagy többsége még arra sem veszi a fáradtságot, hogy megváltoztassák otthoni vezeték nélküli hálózatuk gyári jelszavát. Ennek oka az lehet, hogy a könnyű jelszavakat használókat nem foglalkoztatja sem a felhasználói nevükhöz köthető adott alkalmazás, sem a saját hálózatuk biztonsága.

**2. hipotézis**

*Azok, akik magáncélra elavult operációs rendszert használnak, nem védik kellően hálózatukat, eszközüket és felhasználói fiókjaikat sem.*

Definíciók és kérdéskör tisztázása: elavult operációs rendszer alatt Windows 7 és korábbi verziót értjük, mivel a gyártói támogatása 2020.01.14-én megszűnt, így használata kockázattal jár [15]. Véleményünk szerint elavultnak számít egy újabb kiadású, de nem frissített operációs rendszer is. A nem kellő védelem alatt a hálózat vonatkozásában a nyilvános WiFi hozzáférési pontokra való csatlakozást és az otthoni WiFi hálózat gyenge jelszóval történő védelmét értjük. Eszközvédelem alatt az adathordozók titkosítását és a vírusirtók használatának mellőzését, de már a nem megfelelően kiválasztott termék használatát is ide vettük. Továbbá a munkahelyi végpontvédelmi megoldásokkal szembeni érdektelenség is kapcsolódik az eszközvédelem témájához. Felhasználói fiókvédelemnél a gyengén

megválasztott, vegyes használatú, másnak is tudomására hozott és tárolási módjából eredően könnyen megismerhető jelszavak kérdéseire adott válaszok tartoznak a régóta használt jelszavak mellett.

Értékelés: 12 db kérdés esetén a kockázatos válaszok megoszlása

| Arány (%) | 0 - 25 | 25 - 50 | 50 - 75 | 75 - 100 |
|---|---|---|---|---|
| Előfordulás (db) | 4 | 4 | 3 | 1 |

*4. táblázat: 2. hipotézis kérdéseinek megoszlása (saját szerkesztés)*

Következtetés: Mivel a 12 kérdésből 4-re kaptunk kockázatos választ a csoporttól, feltevésünk teljes mértékben nem bizonyult igaznak, de több területen is megállta helyét. A kockázatos válaszok az alábbiak voltak: munkahelyük vírusvédelmi szoftvere nevének nem ismerete (80,6%), gyári jelszó használata otthoni WiFi routeren (67,7%), érdeklődési körhöz tartozó rövid vagy alapértelmezett jelszavak használata (61,3%), adathordozók titkosítás nélküli védelme (54,8%). Összefüggésként megállapítható, hogy akik elavult operációs rendszert használnak, túlnyomó többségük nem ismeri, hogy munkahelyük melyik cég termékével védekezik a kártékony programok ellen. Ennek oka lehet, hogy még a saját rendszerük védelmére sem fordítanak kellő figyelmet, nemhogy érdeklődést tanúsítanának a munkahelyükön használt szoftvereket illetően.

### 3. hipotézis

*Azok, akik felismerik egy adathalász e-mailben lévő veszélyeket, felelősséggel vannak a munkahelyük információ bizalmassága és saját munkaállomásuk védelme iránt, tehát tisztában kell lenniük szervezetük információbiztonsági szabályzatával is.*

Definíciók és kérdéskör tisztázása: felismerés alatt értjük a gyanús levél törlését, csak megbízható környezetben való megnyitását vagy elemzését és összevetését korábbi hasonló e-mailekkel. A munkahelyi információk bizalmasságát nyilvános helyeken való csevegéssel, selejtes iratok nem megfelelő kezelésével és természetesen illetéktelenek részére történő adatok megadásával is meg lehet sérteni. De szintén információ kikerülésnek minősülhet, ha munkahelyi – gyengén megválasztott, másnak által ismert és felírt – jelszavunkat privát célra használjuk vagy azzal különböző weblapokra regisztrálunk. Kockázatos cselekménynek minősül továbbá más személyt saját azonosítónkkal beengedni egy objektumba. Amennyiben közösségi oldalakon munkahelyünket megemlítjük, azzal is információt teszünk közzé, bizonyos területeken (pl. rendvédelmi szervek) ez tiltva is van. Saját munkaállomásunk védelméhez a váll feletti kifigyelés elleni védelmet, valamint a takarítás vagy egyéb ok miatti zárolást vettük. Ide sorolható még az is, ha a felhasználó figyelmen kívül hagy egy számára ismeretlen hibaüzenetet.

Értékelés: 16 db kérdés esetén a kockázatos válaszok megoszlása

| Arány (%) | 0 - 25 | 25 - 50 | 50 - 75 | 75 - 100 |
|---|---|---|---|---|
| Előfordulás (db) | 1 | 1 | 7 | 7 |

*5. táblázat: 3. hipotézis kérdéseinek megoszlása (saját szerkesztés)*

Következtetés: mivel 16 kérdésből 14-re kaptunk kockázatkerülő, figyelmes hozzáállást tanúsító válaszokat, feltevésünk egyértelműen igaznak bizonyult. A biztonságtudatos válaszok aránya elérte a 87,5%-ot. Több megállapított összefüggés közül felsorolás szinten kiemeljük azokat, melyek olyan felhasználókra jellemzők, akik helyesen járnak el egy adathalász levél érkezését követően. Ők azok, akik ellenőrzik az idegen kollégájuk személyazonosságát, nem hagyják figyelmen kívül, ha hibaüzenet jelentkezik számítógépükön, munkahelyi e-mail címükkel nem regisztrálnak magáncélból hírlevelekre, webáruházakba. Továbbá közösségi oldalakon nem adnak meg munkahelyi információkat, munkahelyi e-mail címüket nem használják privát célra, nem írják fel jelszavukat számítógép mellé és füzetbe sem. Ennek oka lehet, a részletek felismerésének és a higgadt gondolkodásnak a képessége egy óvatos, ösztönös szabálykövető szemlélettel társul annak ellenére, hogy csak valamivel több, mint minden második ember olvasta el munkahelyük információbiztonsági szabályzatát.

## A KÉRDÉSEK EGYMÁSHOZ VISZONYÍTOTT ÉRTÉKELÉSE

Hipotéziseink vizsgálata után kíváncsiak voltunk arra, hogy a kockázatos viselkedésformák hogyan viszonyulnak egymáshoz, vagyis van-e korreláció az erre vonatkozó kérdések között, s ha van, akkor hol tapasztalunk erős korrelációt. Értelmezésünkben az alábbi képlet alapján állapítottuk meg a kapcsolatot (a KVASZ a kockázatos választ adók száma):

$$\frac{viszonyított\ kérdésnél\ KVASZ}{bázis\ kérdésnél\ KVASZ} * 100$$

Az így kapott értékek besorolását az alábbiak szerint határoztuk meg: 0-25% (nincs kapcsolat), 25-50% (gyenge kapcsolat), 50-75% (közepes kapcsolat), 75-100% (erős kapcsolat). Az elemzést elvégezve a következő összegző megállapításokat fogalmaztuk meg.

- Akik ugyanolyan jelszavakat használnak magán és munkahelyi fiókjaiknál 76,9%-ban ugyanazt a pendrive-ot használják magán és munkahelyi célra is.
- Akik kerülik a vírusvédelmi szoftverek használatát, 90%-ban nem használnak titkosítást adathordozóikon és 80%-ban nem biztonságosan semmisítik meg a munkahelyi selejtes iratokat sem.
- Akik talált adathordozót behelyeznek otthoni vagy céges számítógépbe, köztük 100%-uk csak ingyenes vírusvédelmi szoftvereket használ és a pendrive-ját magán és munkahelyi célra is használja.
- Akik mellőzik az automatikus rendszer és programfrissítéseket, 88,9%-ban talált adathordozót behelyeznek otthoni vagy céges számítógépbe.
- Akik olyan munkahelyen dolgoznak, ahol nincs beléptető rendszer, 100%-ban nem biztonságosan semmisítik meg a munkahelyi selejtes iratokat, 77,8%-ban adathordozóikat titkosítási védelem nélkül használják, és gyári jelszavakat használnak otthoni WiFi routerükön.
- Akik munkahelyi e-mail címüket használják magáncélú levelezésre, 86,8%-ban pendrive-jukat magán és munkahelyi célra is használják.
- Akik elmentik bankkártya adataikat és belépési adataikat hordozható eszközeiken, 79,5%-ban pendrive-jukat magán és munkahelyi célra is használják.

- Akik munkahelyén Windows 7 vagy régebbi operációs rendszer üzemel, 80%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik ismeretlen számítógépes hibaüzenetet figyelmen kívül hagynak, 89,5%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nyilvános helyeken munkahelyi témákról is beszélgetnek, 84,6%-ban gyári jelszavakat használnak otthoni Wifi routerükön és 76,9%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik munkahelyi selejtes irataikat kommunális hulladékként kezelik vagy hazaviszik, 77,4%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nem zárják le számítógépüket munkahelyükön takarítás alatt, 80,4%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nem ellenőrzik telefonon keresztül magukat kollégájuknak kiadó személy azonosságát, 79,1%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik ismeretlen feladótól vagy közüzemi szolgáltató nevében érkezett e-mailben lévő linkre vagy mellékletére azonnal rákattintanak, 83,3%-ban használnak nyilvános helyeken ingyenes WiFi hálózatot.

A fentiek alapján azt a következtetést vonjuk le, hogy amennyiben a munkahelyek vezetői – az operációs rendszer és beléptető rendszer korszerűsítéssel kapcsolatban – valamint felmérésben részt vevő személyek a többi kérdés vonatkozásában biztonságtudatosabb viselkedésre váltanának át, az pozitív változásokat idézhetne elő az erős kapcsolódással rendelkező kérdéseknél is.

**Pozitív megállapítások**

Az utolsó hipotézisünkben felállított pozitív gondolatmenetet tovább folytatva, a biztonságtudatos szemléletet követő felhasználók szokásait is elemeztük, mely során a bázis és viszony kérdések kiválasztását egyéni preferencia alapon döntöttük el. Ennek alapján a következő megállapításokat fogalmaztuk meg.

- Akik különböző jelszavakat használnak magán és munkahelyi fiókjukhoz, 72,8%-ban nem osszák meg másokkal jelszavukat, továbbá 56,3%-ban bonyolult, összetett jelszavakat alkalmaznak.
- Akik odafigyelnek, hogy más mögöttük állva ne láthassa meg begépelt hitelesítő adataikat, köztük 79,3%-ban nem osszák meg másokkal jelszavukat, továbbá 60,3%-ban bonyolult, összetett jelszavakat alkalmaznak.
- Akik tudatosan válasszák meg vírusvédelmi szoftverüket, 50,5%-uk meg tudta nevezni a munkahelyükön használt vírusirtójuk nevét is. Akik ismerős ajánlása alapján választanak otthonra ilyen védelmi programot, csak 37,8%-uk volt tisztában a munkahelyükön használttal. Míg, akik nem használnak semmiféle vírusvédelmet csak 10%-ban ismerték a munkahelyi vírusvédelmi programjuk nevét.
- Akik rendszeresen naprakészen karbantartják operációs rendszerüket, a szükségtelen programokat törlik, 53,2%-uk tudatosan választja ki vírusirtóját is. 56,5%-uk soha nem használ ingyenes WiFi hálózatot.
- Akik elolvasták munkahelyük IBSZ-ét, 83,2%-uk nem használja munkahelyi email címét magán célra és 89,7%-uk semmilyen weboldalra, hírlevélre nem regisztrált

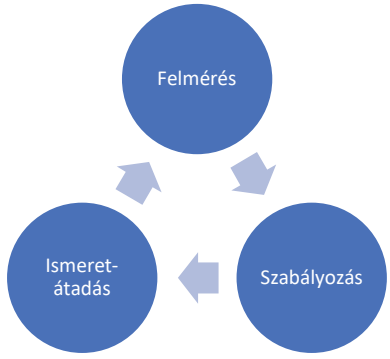
vele. 73,8%-a zárolja munkaállomását miután feláll tőle, 86,9%-uk pedig takarítás közben is vigyáz a bizalmas munkahelyi adataira. Köztük csak 14,9%-uk oszt meg magáról közösségi oldalakon olyan adatokat, mely alapján személyük beazonosíthatóvá válik és csupán 12,1%-a engedné be kollégáját saját azonosítójával. Munkahelyi témákról is 4,7%-uk beszélne nyilvános helyeken.

## KÖVETKEZTETÉSEK

Kérdőíves kutatásunk eredményeként, valamint a tanulmányunk első részében nevesített hazai és nemzetközi szakirodalom feldolgozása alapján az alábbi javaslatokat teszszük az emberi jellemből fakadó social engineering típusú támadások elkerülése, felismerése és megakadályozása érdekében.

### Javaslatok a biztonságtudatosság elérésére

Mint ahogy az alfejezet címe is mutatja, az elérendő cél a szervezet dolgozóiban a biztonságtudatos gondolkodás és viselkedés kialakítása, megteremtése. Hogy mi is az a fajta gondolkodásmód, ami felé terelni akarjuk a dolgozókat, ezáltal a szervezetet, mindenképp tisztázni szükséges. Az ISACA [16] definíciója a tudatosság alatt azt érti, hogy „értesültnek lenni, figyelembe venni, tudatosnak és jól informáltnak lenni egy olyan szakmai tárgykörben, mely magába foglalja az adott témakör tudását és megértését és az annak megfelelő cselekvést.” Nemeslaki és társa [17] az információbiztonsági tudatosságról alkotott fogalmában konkretizálja ezt a kérdéskört, miszerint az tulajdonképpen „egy munkavállaló általános tudása az információbiztonságról és az információbiztonsági szabályzat tudomásul vétele a szervezetben”. A fentiek tükrében megfogalmazott módszert különböző megközelítés szerint osztályoztuk, melyek egymással szoros kölcsönhatásban lévén, egymásra épülő elemeknek tekinthetőek. A kérdőív válaszaiból megállapított problémák, hiányosságok alapján egy komplex egymásra épülő megoldást javasolunk a 2. ábrán, Oroszi [13] munkájára alapozva.




*2. ábra: biztonságtudatosítási folyamat körforgása (saját szerkesztés)*

**Felmérés.** A fejlődési igénynek mindig felülről kell jönnie, azaz amíg a szervezet vezetősége nem határozza meg ezt az utat maga előtt, addig a dolgozóktól is hiú ábránd ilyet elvárni. Egy adott szervezet biztonságtudatosságát először fel kell mérni, melynek eredménye kiindulópont lesz a továbbiakban. Ez történhet kérdőívekkel, külsős személy

általi váratlan ellenőrzéssel (penetration test) vagy audit által is. Bármelyiket is választjuk, mindenképp az adott szervezetre kell szabni a kérdéseket. Ehhez a vállalat szervezeti felépítését, infrastruktúráját, bizonyos belső szabályozásait ismerni kell, hogy minél inkább életszerűbb, személyre szabottabb kérdéseket lehessen alkotni. A fentebb említett vezetőség általi támogatottság nyújtása így rendkívül fontos. Azonban nem szabad figyelmen kívül hagyni azt a tényt, hogy a felmérés tulajdonképpen már a befejezésével elavulttá válik. A kiértékelés közt eltelt időben egy új alkalmazott felvétele, új technológia bevezetése, mint eddig ismeretlen tényező, olyan kockázat megjelenését jelenti, ami nem ismert sebezhetőséget rejt magában. Fontos elérnünk a munkavállalókban, hogy egy kérdőíves felmérés kötelező jellegű kitöltését kellő komolysággal hajtsák végre, hiszen ellenkező esetben fals eredmények születhetnek. A dolgozóknak tehát meg kell érteni a social engineering jelentőségét, amivel támadás érheti egyénüket, családjukat és a szervezetüket is. Manapság egy kis családi vállalkozástól kezdve egy multinacionális cég ügyvezetője is célponttá válhat. A leghatékonyabb ellenintézkedés így az oktatáson keresztül valósulhat meg. Ismerniük szükséges a gyakori social engineering támadásokat és amennyiben találkoznak egy gyanús szituációval, kövessék az alapvető biztonsági intézkedéseket. A social engineerek ugyanis az emberi hiszékenység mellett a korlátozott mennyiségű információkra hagyatkoznak, amik az idegen emberek azonosságának ellenőrzését elősegítik. Ez utóbbi információk hiányában az áldozat el fogja hinni, hogy a támadó az, akinek kiadja magát. Felkészültnek kell lenni a gondolkodás terén is, ehhez a szkepticizmus mellett folyamatos éberség kifejlesztése is szükséges.

**Szabályozás.** A felmérések kiértékelését követően a már meglévő szabályzatok, előírások felülvizsgálata – vagy amennyiben nem léteznek ilyenek, akkor elkészítésük – következik. Visszautalva a kérdőívünkre a válaszadók 6,5%-a szerint a munkahelyük nem rendelkezik információbiztonsági szabályzattal. Amennyiben olyan újfajta sebezhetőségeket tárt fel a felmérés, melynek megelőzéséről eddig nem rendelkezett a szervezet, ennek megfelelő módosítása szükséges. Saját kutatásunk alapján a következő területeket szükséges szabályozni: jelszókezelés, elektronikus levelezés, munkaterület védelme, adathordozók védelme, számítógép használat, beléptetés rendje, hulladék kezelése, információk továbbítása, kommunikációs csatornák használata. Szakmailag az egyik legkézenfekvőbb választás az MSZ/EN ISO 27001:2014-es szabvány „A” mellékletét ajánlani, mely a szervezet valamennyi területét lefedi.

**Ismeretátadás.** Egy munkahelyi oktatási sorozat felépítésének az előzetesen elvégzett felmérések eredményein kell alapulnia, hivatkozva a szervezet aktuális szabályozásaira. Egy köremailben kiküldött szabályzatváltozásnak, újfajta rendelkezés ismertetésének a gyakorlati szinten a hatékony tudásátadás szempontjából meglátásunk szerint nem sok értelme van. Ezek az üzenetek rendszerint a napi munkamenet közben érkező levelek közé vegyülnek, kevesen vannak, akik alaposan, nyugodt körülmények közt át is olvassák őket. Így mindenképp a példákkal színesített, élő személy általi oktatást tartjuk az egyik jól bevált módszernek. E mellett persze számos másfajta lehetőséggel is élhetünk úgymint e-learning oktatás, kiscsoportos tréningek, vagy a figyelem fenntartását szolgáló kampányok és programok. Mindezek célja az ismeretterjesztés, melyet meghatározott időközönként ismételni

szükséges. A képzéseket a célcsoport igényeire és veszélyeztetettségi szintjéhez kell igazítani. Gondolunk itt a felsővezetésre, adminisztratív feladatot ellátó titkárnőkre, IT-ra, kiváltképp az üzemeltetésre valamint bármilyen speciális munkaterületre, ahol eltérő kockázatok merülhetnek fel. Az oktatást követően – rendhagyó módon – pár nappal érdemes lehet egy gyors ellenőrzés gyanánt rövid teszt kitöltése is, mely a megmaradt tudás visszamérését szolgálja. Meghatározott időközönként – amennyiben incidens nem következett be – ismételten elő kell venni az ellenőrzés eszköztárát (felmérés, pentest, audit) annak megállapítására, hogy a mindennapi munkavégzés során a dolgozókba mennyire ivódott bele az új ismeretek elméleti szinten való befogadása és implementálása a gyakorlatban. Amint látszik, ahhoz kétség sem férhet, hogy egy szervezet védekezése a social engineering ellen – annak összetettsége miatt – több dimenziós folyamat. Csak a hardveres és szoftveres védelem ez esetben nem elegendő, azonban sok esetben segítség lehet. Vírusírtók, tűzfalak, IDS/IPS-ek, honeypot-ok, phishing oldalakat észlelő böngésző bővítmények, beléptető és megfigyelő rendszerek, mind-mind hasznosak lehetnek, de a támadások középpontjában végső soron az ember áll.

## FELHASZNÁLT FORRÁSOK

### Irodalom

[1] Cs. Kollár, Á. Zakar, „A social engineering és a manipulációs technikák és módszerek” *Biztonságtudományi Szemle*, 2. évf. 2. szám, pp. 23-38, 2020.
[2] E. Babbie, „A társadalomtudományi kutatás gyakorlata”, Budapest: Balassi Kiadó, 2017.
[3] L. Cseh-Szombathy és Z. Ferge, *„A szociológiai felvétel módszerei”*, Budapest: Közgazdasági és Jogi Könyvkiadó, 1971.
[4] D. Freedman, R. Pisani és R. Purves, *„Statisztika”*, Budapest: Typotex, 2005.
[5] F. Moksony, *„Gondolatok és adatok”*, Budapest: Osiris Kiadó, 1999.
[6] L. Sajtos és A. Mitev, *„SPSS Kutatási és Adatelemzési Kézikönyv”*, Budapest: Alinea Kiadó, 2007.
[7] P. A. Scipione, *„A piackutatás gyakorlata”*, Budapest: Springer-Verlag, 1994.
[8] N. K. Malhotra, *„Marketingkutatás”*, Budapest: KJK-Kerszöv, 2002
[9] Zs. Bornemissza, *„Microsoft Excel függvényei a gyakorlatban”*, Budapest: Szalay Könyvkiadó, 2003.
[10] H. P. Reidmacher, *„Excel közgazdászoknak”*, Budapest: Aula Kiadó, 2000.
[11] K. L. Tóthné, *„Összefüggés vizsgálatok”*, Gödöllő: Gödöllői Innovációs Központ, 2009.
[12] K. L. Tóthné, *„Következtetés statisztika”*, Gödöllő: Gödöllői Innovációs Központ, 2009.
[13] E. Oroszi, *„Social engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője”*, Budapest: Corvinus Egyetem, 2008.
[14] Z. Nyikes, „A biztonságtudatosság fejlesztésének egyes lehetőségei”, *XXII. Fiatal Műszakiak Tudományos Ülésszaka*, Kolozsvár, 2017.
[15] https://support.microsoft.com/hu-hu/help/4057281/windows-7-support-ended-on-january-14-2020 (letöltve: 2020.04.12.)
[16] ISACA: Glossary of terms, Rolling Meadows, IL 60008 USA, ISACA 2015.
[17] A. Nemeslaki, P. Sasvári, *„Empirical Analysis of Information Security Awareness in the Business and Public Sectors in Hungary”* Central and Eastern European e|Dem E|Gov Days 2015, Conference Proceedings

# PROTECTION OF MEDICAL BUILDINGS

# OBJEKTUMVÉDELEM AZ EGÉSZSÉGÜGYBEN

LIEBMANN Gábor[1]

**Abstract**

The medical buildings fraught with considerable security risk, because of its' special curative care. The healing of the patients – on the basis of the new medical recommendations – a large open area and the possibility of free and unrestricted entry helps. It contains special security risks, to reduce them a well prepared and designed building protection system could be a solution. The integrated electronic security systems alone are not sufficient for effective protection, because it gives only alarm signals for the security centers. It is always needed to be there a human person to prevent or solve any incidence. The well designed optimal co-operation of the systems can provide a well prepared complex safety, and security system, which has to integrate the various emergency strategies, too. It's not enough to design, to install the safety and security system, it must be operate, too. It can't be a useful and efficient complex system without well educated and trained human staff.

**Keywords**

medical, complex security system, access control, video surveillance, gate phone, burglar alarm system, security staff

**Absztrakt**

Az egészségügyi létesítmények a speciális gyógyító-, betegellátási feladatuk miatt jelentős biztonsági kockázatot rejtenek magukban, mert a gyógyulást - az orvosszakmai javaslatok alapján - a tágas nyitott területek és a szabad, korlátozás nélküli, belépés lehetősége elősegíti. Vagyonvédelmi szempontból a fentiek miatt adódó veszélyek csökkentésére egy jól átgondolt objektumvédelmi rendszer kialakítása jelenthet megoldást. Az elektronikus vagyonvédelmi rendszerek önmagukban nem elegendőek a hatásos védelemhez, mert a prevencióhoz, a bekövetkezett rendkívüli események megoldásához szükséges a hatékony beavatkozó személyzet jelenléte is a területen. A rendszerek optimális együttműködését egy komplex biztonsági védelmi rendszer biztosíthatja, melynek a vagyonvédelmi szempontokon túl a különféle válsághelyzeti stratégiák integrálását is tartalmaznia kell. Nem elég a rendszerek tervezése, kidolgozása, telepítése, azokat üzemeltetni is kell és biztosítani a személyzet képzését, gyakorlatát.

**Kulcsszavak**

objektumvédelem, egészségügy, komplex biztonsági rendszer, beléptető, video megfigyelő, kaputelefon, behatolásjelző, élőerős védelem

[1] liebmann.gabor@gmail.com | ORCID: 0000-0002-0726-862X | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Az egészségügyi területen az elsődleges gyógyító ellátás mellett a közelmúltig a vagyonvédelemre kevés figyelmet fordítottak. Napjainkban azonban mind az írott, mind az elektronikus sajtóban egyre több olyan eset jelenik meg, amelyben egészségügyi intézményekben történik vagyon elleni bűncselekmény, vagy a létesítmény nevét, ismertségét kihasználva, azzal visszaélve követnek el csalásokat. A Covid-19 pandémia tovább növelte az egészségügyi létesítmények jelentőségét, növelve ezzel egyben a kockázatokat is. Az egészségügyi területen dolgozók és a betegek - az előzőekben említett okok miatt - egyre növekvő veszélyérzete előtérbe helyezi az objektumvédelem kialakításának szükségességét.

Az egészségügyi ellátásban résztvevő létesítményekben jelentős a beteg- és a látogató forgalom. A fekvőbeteg ellátó intézményekben pedig sok a magáról gondoskodni csak segítséggel képes, gyógyulni vágyó ember, ezért a területek vagyonvédelmi kockázata magas. Sajnos egyre több elkövető tekinti ezt könnyű vagyonszerzési lehetőségnek, amelyeket igyekeznek egyre jobban kiaknázni. Az egészségügyi ápoló személyzet alacsony száma, illetve a folyamatos túlterheltsége nem teszi életszerűvé, hogy feladataikon túl, a felügyeletük alá tartozó osztályon még a vagyonvédelemmel is foglalkozzanak. Az egészségügyi létesítményben elkövetetett személy-, vagy vagyon elleni cselekmények - a morális kérdéseken túl - a betegek gyógyulási folyamatát is megakaszthatják, lelassíthatják, esetlegesen újabb betegség kialakulását okozhatják.

A fenti kockázatok jelentősen csökkenthetők egy megfelelő és hatékonyan együttműködő elektronikus jelző-, mechanikai-, élőerős-, biztosítási-, azaz komplex védelmi rendszer kialakításával.

## EGÉSZSÉGÜGYI OBJEKTUMOK ÁLTALÁNOS JELLEMZŐI ÉS KOCKÁZATAI

„A kórházbiztonság egy speciális objektumvédelem, melyet az ott dolgozók, az ott kezeltek, és az oda látogatók tesznek speciálissá, az összetett feladatok mellett. Egészségügyi létesítmények védelmének előkészítése és tervezése, valamint az ezzel összefüggő feladatok végrehajtása néhány terület tekintetében meghatározóan sajátságos. Az egyik és talán a legfontosabb az, hogy akár szakrendelőről, akár kórházról beszélünk, számításba kell venni a következőket:

- az objektumot látogató csoport heterogén összetételű
- a személyforgalom meglehetősen nagy és
- az objektumon belüli tevékenység szerteágazó.„ [1]

Az egészségügyi létesítmények az épületek széles spektrumát alkotják, az egyszerű orvosi rendelőktől kezdve, a rendelőintézeteken, a klinikákon keresztül, az összetett nagy kiterjedésű, hatalmas méretű oktató kórházakig. A kockázatok figyelembevételével ennek megfelelően kell az egyre bonyolultabb és komplexebb rendszereket kialakítani és működtetni. Az orvosi rendelőnél már egy behatolásjelző rendszer kiépítése, és annak kiegészítése távfelügyeleti és kivonuló szolgáltatással biztosítja a kockázatokkal arányos védelmet. A méretek növekedése, a védendő értékek hatványozott növekedését vonja maga után. Mindemellett a nagy betegforgalom és a modern orvosi felfogás, a területekre, épületekbe történő szabad bejutást, a nyilvánosságot, a nagyméretű barátságos közösségi területeket preferálja, mert ez jó hatással van mind a betegek, mind a kísérők közérzetére, mentális állapotukra,

ezzel segítve a gyógyulást. A vagyonvédelemre a felsorolt tulajdonságok összessége azonban nagy feladatot ró, mert ebben a környezetben a biztonságérzet kialakításához szükséges védelem megvalósításának-, üzemeltetésének költsége exponenciálisan növekszik, mivel a fenyegetéstől és veszélytől való mentesség és biztonság érzése az ember alapvető szükséglete. [2]

Egy egészségügyi létesítményben a biztonsági kockázatok között a kisebb eszközök, tárgyak eltulajdonításától kezdve (telefon, pénztárca, személyes értéktárgyak), a nagy értékű orvosi eszközök rongálásán, az informatikai hálózaton lévő szenzitív adatok illetéktelen hozzáférésén keresztül, akár az öngyilkosságot és sajnos az emberölést is számon kell tartani, mert ezek mind az egészségügyi elláttás összetettségében és specialitásában rejlő és bekövetkező események. A kezeltek heterogén összetételéből adódóan előfordulhat, hogy büntetésvégrehajtási intézményekből is érkeznek ide ellátásra szorulók, akikre a fentieken túl, szintén speciális védelmi protokollok vonatkoznak.

A háziorvosi rendelőknél nagyobb épületek felépítése a modern kor orvosszakmai kívánalmainak eleget téve tágas nyitott területekkel rendelkezik, ahová bárki korlátozás nélkül, anonim módon beléphet. Időszakosan egyszerre nagy számú ember tartózkodhat ezekben a terekben, mely az előzőekben említett veszélyeket nem csökkenti, hanem tovább növeli. Az anonimitás ahhoz vezet, hogy a közösségi területeken tartózkodók a „nem az én problémám, nem az én feladatom” viselkedési modellt követik, amely a zsebtolvajok számára ideális. [3]

Az épületek általában központi-, jól megközelíthető, nagyforgalmú helyeken találhatók, mely a professzionálisabb bűnelkövetők figyelmét is könnyen felkelti.

Mindezen tényezők mellett még számolni kell az épületben, vagy annak közvetlen közelében előforduló hagyományos veszélyforrásokkal is, mint például a víz, a tűz, a robbanás, valamint a földrengés. [4]

## MEGELŐZÉS ÉS VÉDELEM

Az épület üzemeltetőjének a feladata, hogy technikai-védelmi eszközökkel, rezsimintézkedésekkel a veszélyeket redukálja. A biztonsági szintet a folyamatosan változó külső tényezők időről-időre csökkentik, ezért nagyon fontos, hogy az üzemeltető az épületben dolgozókkal folyamatosan párbeszédet folytasson, rendszeresen kérje ki a biztonsággal kapcsolatban is a véleményüket. Szervezzen fórumokat, ahol megismerheti az épületben található különféle szervezetek működését, időrendjét, a várható forgalmat és annak összetételét.

Az üzemeltetőnek a hatásos védelem kialakításához a biztonsági kockázatok feltérképezése után, ismernie és alkalmaznia kell a hatályos jogszabályi előírásokat.

### Az egészségügyi létesítmények vagyonvédelmének törvényi szabályozása

Az egészségügyi létesítmények területe két részre osztható, az egyik terület a magánterület, de vannak olyan létesítmények, melyekben előfordulnak közforgalom számára megnyitott magánterületek is. Az objektumvédelmi rendszert az előzőekben írtaknak megfelelően meg kell feleltetni a hatályos jogszabályoknak. A magyarországi közintézményekben az alábbi törvények és rendelkezések előírásait kell alkalmazni:

- 1994. évi XXXIV. törvény a Rendőrségről - a közforgalom számára megnyitott magánterület miatt.
- 1999. évi LXIII. törvény a közterület-felügyeletről – a megközelítés közforgalom számára megnyitott magánterület miatt
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban: Vagyonvédelmi Törvény) - több területre való érintettsége okán.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Információs Törvény) – a video megfigyelő és a beléptető rendszerben keletkező szenzitív adatok kezelése miatt.
- 2012. évi I. törvény a munka törvénykönyvéről - a dolgozók megfigyelése miatt,
- Az Európai Parlament és a tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (továbbiakban: GDPR)

Az üzemeltetőnek rendelkeznie kell a GDPR, illetve a harmonizált Információs Törvényben meghatározott saját adatkezelési szabályzattal és a törvényben kötelezően előírt nyilvántartásokkal, melyeket folyamatosan naprakészen kell tartani és a jogszabály változásoknak megfelelően meghatározott időközönként felülvizsgálni, szükség esetén módosítani. A területen létesítendő beléptető és video megfigyelő rendszer felügyeletét külső vagyonvédelmi szolgáltatóval, vagy saját szervezeten belül (egészségügyi létesítmény saját alkalmazottjával) is lehet biztosítani.

Abban az esetben , ha a megfigyelési terület magánterület, akkor az objektumvédelmi rendszerek kiépítésénél és műszaki paramétereinek meghatározásánál a Vagyonvédelmi Törvényben megfogalmazott előírásoknak megfelelően kell eljárni. [5] Ezzel szemben, ha a megfigyelési terület a magánterületnek a közönség számára nyilvános részén kerül alkalmazásra, úgy azt csak a törvényben meghatározott hivatalos személyek nézhetik, ellenőrizhetik, ellenkező esetben ott video megfigyelés nem folytatható, a meglévő kamerákat le kell szerelni.

A rendelkezésre álló információk alapján lehet elkezdeni a létesítmény védelmi rendszerének tervezését, a szükséges vertikális védelmi szintek meghatározását, azon belül a pedig a horizontális héjak kidolgozását. Egy egészségügyi létesítményben – a korábban megfogalmazott kockázatok figyelembevételével – a hatékony védelemhez komplex rendszer kialakítása szükséges, mely a teljes vertikumot magába foglalja, az építészeti megelőzési lehetőségek kiaknázásától, a mechanikai-, elektronikai jelző-, élőerős rendszereken keresztül a bekövetkezett események okozta károk enyhítésére szolgáló biztosítást is. Létesítményenként az egyes szintek mélységében lesznek különbségek. „Az esetek döntő többségében nem a meglévő erőket és eszközöket hangoljuk össze, hanem a kockázatelemzés és a kockázatértékelés elvégzését követően határozzuk meg, hogy a kívánt védelmi szint eléréséhez milyen mechanikai védelmi eszközöket, elektronikai jelző berendezéseket kell alkalmazni és ezek felügyeletére milyen élőerőt kell alkalmazni. A három védelmi forma egymásra épülése, egymás kiegészítése adja a komplexitást.” [6]

**Beléptető rendszer**

Az épületekben lévő mozgásokat korlátozni kell, hogy a látogatói területekről a gyógyító, kutató, oktató tevékenységgel összefüggő területekre csak szabályozottan és ellenőrzötten történjen a bejutás. A fenti célnak az egyik legmegfelelőbb eszköze a jól megválasztott beléptető rendszer kialakítása és üzemeltetése. A beléptető rendszer az épületen belüli mozgásokat szabályozza, korlátozza. Egy egészségügyi létesítményben ennek különös jelentősége van, mert nem csak az előre meghatározott csoportok térbeli korlátozását szükséges megvalósítani, hanem a rendelési és látogatási időkben a jogosultsággal nem rendelkezőket is be kell engedni a megfelelő helyekre. A beléptető pontok meghatározását hosszú előkészítési folyamatnak kell megelőznie, melyben a biztonságtechnikai szempontokon kívül figyelembe kell venni az orvosszakmai ajánlásokat és előírásokat is. Fontos, hogy az épületbe történő be- és kijutási lehetőségének száma a lehető legalacsonyabb legyen. A használaton kívüli bejáratokra kerüljenek fel olyan jelzőegységek, melyek az épületben lévő biztonsági szolgálat figyelmét felhívják a jogosulatlan ki- és belépésekre, a szállításra, az esetleges rongálásra.

A helyiségek számát figyelembe véve nem gazdaságos, hogy a létesítmény minden ajtajára önálló beléptető rendszer kerüljön. A beléptető rendszert jól kiegészíti és a hatékony védelmet is szavatolja az egységes fő- kulcsrendszer. Arra kell törekedni, hogy az épületben dolgozó személyzetnek lehetőleg csak kevés számú kulcsot kelljen használnia, azonban ezek a kulcsok egyediek és másolásvédettek legyenek. Tovább növeli a hatékonyságot, ha a kulcs kiadás- és visszavétel naplózása azonosíthatóan és elektronikusan történik.

**Behatolásjelző rendszer**

A létesítményekben vannak olyan kiemelt területek, ahová – a védendő értékek nagysága, veszélyes anyagok tárolása, illetve a szenzitív adatok kezelése miatt - behatolásjelző rendszereket szükséges kiépíteni. Ezen területek lehetnek például az orvosi szobák, a tantermek, a konzíliumi helyiségek, a raktárak, különös tekintettel a pszichotróp-, kábító-, tudatmódosító gyógyszerek tárolására szolgáló raktári területek, valamint a sugárzó anyaggal dolgozó diagnosztikai területek. A behatolásjelző rendszer az épületeken belül található vagyonvédelmileg veszélyeztetettebb helyiségek kiegészítő védelmét szolgálja a mechanikai védelem mellett. A kialakított rendszernek célszerűen együtt kell működni mind a beléptető, mind a video megfigyelő rendszerrel. A behatolásjelző rendszer így a lezárt területekre történő nem azonosított bejutást azonnal jelzi közvetlenül a helyszínen, az épületfelügyeleti központban, valamint biztosítja az átjelzést a távfelügyeleti központba is.

**Video megfigyelő rendszer**

A video megfigyelő rendszer az épületeken belüli, illetve az épületek közvetlen környezetében bekövetkező események képeit rögzíti és továbbítja az épület felügyeleti központjába, a nagy kockázatú létesítményeknél egy külön távfelügyeleti központba. A video megfigyelő rendszer a behatolásjelző és a beléptető rendszerek működését teszi hatékonyabbá, mert vizuális visszacsatolást ad a kezelő személyzetnek és a szolgálatot teljesítő járőröknek, biztonsági szolgálatnak. Segítségével eredményesebben felderíthetők az épület működését, vagy működési rendjét veszélyeztető tevékenységek, ezáltal a beavatkozást

végző személyek irányítása is rendkívül közvetlen és sikeres lehet. A megfigyelő rendszereknél minden esetben meg kell határozni a megfigyelés jogalapját, illetve célját. Az egészségügyi létesítményekben ugyanazon eszközök kerülnek felszerelésre vagyonvédelmi-, illetve életvédelmi célból is. A vagyonvédelmi célra használt eszközök nem kerülhetnek felszerelésre olyan területre, ahol az emberi méltóság sérülhet (kórtermek, vizsgálók, stb..). Az intenzív terápiás területeken, ahol a betegek 24 órás folyamatos felügyeletét biztosítani kell, alkalmazható egészségügyi megfigyelő rendszer, azonban az itt keletkező képek rögzítése egyáltalán nem engedélyezett. A Covid-19 pandémia rámutatott arra, hogy a video megfigyelő rendszerek – megfelelően szabályozott módon és a jogszabályi előírások teljeskörű betartásával - alkalmazásával az egészségügyi ellátás biztonsága jelentősen növelhető, a szakszemélyzet munkája hatékonyabbá-, leterheltségük szintje pedig alacsonyabbá tehető.

**Kaputelefon rendszer**

Egy jól megtervezett kaputelefon rendszer a biztonsági szint növekedését is eredményezi. A rendszer célja, hogy az egészségügyi kezelőszemélyzet azonosítani tudja a belépő személyét anélkül, hogy közvetlenül a belépési ponthoz kellene mennie. Ezáltal a munkáját hatékonyabban tudja végezni és úgy tud vagyonvédelmi feladatokat ellátni, hogy az számára nem jelent többlet terhet. A steril-, őrző-, betegellátó terekbe történő azonosított bejutás életvédelmi szempontból is kiemelten fontos, így a komplex vagyonvédelem egyik fontos elemeként is lehet a kaputelefon rendszerekre tekinteni. Mivel a kaputelefon rendszer elemei a beléptető rendszerrel együtt kell hogy működjenek, így összekapcsolásuk, a beléptető rendszerbe történő integrálásuk is kézenfekvő. Ezzel a módszerrel a kaputelefonon keresztül történő beléptetések is naplózásra kerülnek, így visszakereshetővé válnak ezek az események is. Mindezen szempontok figyelembevételével a területek biztonsági szintje növekszik.

**Élőerős védelmi rendszer**

Az egészségügyi épületek biztonsága nem szavatolható hatékony humán erőforrás nélkül. A létesítményekben a fő belépési pontokon a nyitvatartási időnek megfelelő időtartamú portaszolgálatok kialakítása szükséges, valamint az épület területein a létesítmény méretéhez igazodó járőrszolgálat felállítása is javasolt. A feladatuk az épületbe belépők megfigyelése, eligazítása, valamint a nem megfelelő magatartást tanúsító, illetve az épület működésére veszélyt jelentő személyek kiszűrése és az épületből történő eltávolítása, továbbá a vagyonvédelmi rendszer jelzéseire történő reagálás.

A technikai berendezések és a humán egységek összekapcsolására, koordinálására célszerű egy diszpécserszolgálat felállítása, külön erre a célra kialakított épületfelügyeleti helyiségben. A beavatkozások hatékonysága érdekében a szolgálatok minden tagjának rendelkeznie kell olyan kommunikációs eszközzel, mely az épület egészét lefedi és biztosítja az általános, illetve a szelektív kapcsolatot minden résztvevő számára.

A humán erőforrás munkavégzéséhez nem elegendő a műszaki-, technikai feltételek biztosítása, hanem szükséges a feladat ellátási helyének megfelelő elméleti és gyakorlati képzések, rendszeres továbbképzések szervezése is. [7]

Fontos itt is megjegyezni, hogy a komplex rendszer üzemeltetése egy rendkívül összetett és bonyolult folyamat, melynek alapvető szükséglete a megfelelő szaktudással és gyakorlattal rendelkező humán erőforrás használata.

**Speciális védelmi megoldások**

Az egészségügyi jelleg miatt nem elegendő csak a vagyonvédelemmel foglalkozni, az objektumvédelemnek ki kell terjednie az életvédelem sajátos területeire is. A fekvőbeteg ellátás akadályozza az épületek gyors kiüríthetőségét, ezért az épület közelében bekövetkező vészhelyzetekre az evakuációs terveken túl, ki kell dolgozni az elzárkózási terveket is. Mindkét folyamat megvalósítása az objektumvédelmi komplex rendszerek igénybevételével és aktív segítségével történik. Az elzárkózás során a veszélyeztetett területek nyílászáróinak becsukása, az épületgépészeti mesterséges szellőztetés leállítása, az elektromos áramszolgáltatás csak a létfontosságú területre történő biztosítása alatt az épületben tartózkodó személyek, betegek a veszélyforrástól legtávolabbi helyekre történő átköltöztetését is jelenti.

A vagyonvédelmi rendszerek ekkor csak az elzárkózási helyszín felé biztosítják a szabad mozgást, minden mást lezárnak, a központból pedig a megfigyelő rendszerek segítségével folyamatosan ellenőrizhetők az épületen belüli-, illetve az épület közvetlen közelében lévő mozgások.

A magyarországi tapasztalatok azt mutatják, hogy nem elegendő a terveket megalkotni és a legapróbb részletekig kidolgozni, hanem az épületre vonatkozó elzárkózási és evakuációs terveket folyamatosan karban kell tartani és azt évenként legalább egyszer – minden érintett bevonásával - a gyakorlatban is végre kell hajtani. Azon egészségügyi létesítmények, melyek fekvő részleggel, intenzív terápiás részleggel, műtőblokkokkal rendelkeznek, különös fontosságú a protokollok gyakorlatban történő alkalmazása, hiszen havaria helyzetben már nincs mód a válságtervek olvasására. Nem elég azonban csak a saját tervek ismerete, mert egy válsághelyzet megoldása elképzelhetetlen a mentőszolgálat, a katasztrófavédelem, valamint a rendvédelmi szervek részvétele nélkül. Meg kell ismerni ezen szervezetek beavatkozási metódusait is, melyre a legalkalmasabb módszer a közös gyakorlatok szervezése és lebonyolítása. A gyakorlatok tapasztalatai alapján pedig a terveket felül kell vizsgálni és szükség esetén javítani, valamint ennek folyamataként az épületben feltárt technikai hiányosságokat ki kell javítani, vagy azokat meg kell oldani.

## ÖSSZEGZÉS

Az adott egészségügyi létesítményt üzemeltető feladata, hogy a biztonsági kockázatokat azonosítsa, azokat csoportosítsa és ezek felhasználásával a kockázatelemzést elvégezze. Az elemzés adatait felhasználva lehet a komplex vagyonvédelmi rendszert kidolgozni és azt a létesítmény védelmére bevezetni. Az elemzés során a vagyonvédelmi kockázatokon kívül, az egészségügyi ellátás specialitásából eredő életvédelmi kockázatok felmérésének is meg kell történnie. A rendszer komplex védelmének kialakításakor pedig mindkét aspektus figyelembevételével lehet csak az optimális védelmet meghatározni. Nem létezik olyan mértékű védelem, mely minden típusú fenyegetettségre 100%-os megoldást nyújt. Az objektumvédelem optimális szintjének meghatározásakor azt kell figyelembe venni, amikor a kiépítésre kerülő integrált rendszer hatékonyságának további növelése már

jelentős költségráfordítást igényelne, ezzel szemben sem az épület használói, sem az üzemeltető már nem érzékelné ezt a különbséget. Az élőerős védelem nélkülözhetetlen a rendszer üzemeltetése és működtetése szempontjából, az optimális védelmi szinthez azonban a munkavégzéshez megfelelő szakképzettségű és gyakorlattal rendelkező humán erőforrás alkalmazása szükséges. A védelmi rendszer fennmaradó kockázataira pedig egy olyan biztosítást kell választani, mely a bekövetkező események okozta károkat megfelelő mértékben fedezi.

A tervezést, kiépítést követően a védelmi rendszereket üzemeltetni kell, a tapasztalatok felhasználásával pedig rendszeres időközönként felülvizsgálni, szükség esetén beavatkozni, esetleg módosítani a működésüket. Az egészségügyi létesítményekben különös fontossága van a válsághelyzeti terveknek. A tervekben megfogalmazott protokollok rendszeres, legalább évenkénti gyakorlatban történő végrehajtása szükséges a valós védelmi szint eléréséhez.

## HIVATKOZÁSOK

[1] L. Berek, T. Berek és L. Berek, Személy és Vagyonbiztonság, Budapest: Óbudai Egyetem, 2016.
[2] A. Maslow, Motivation and personality, New York: Addison Wesley Longman , Inc., 1954.
[3] D. Challinger, „CRISP Report: From the Ground Up: Security for Tall Buildings," ASIS Foundation, Inc., Alexandria, VA, 2008.
[4] European Interagency Security Forum, Office Opening: A Guide For Nn-Governmental Organisations, London: EISF Secretariat, 2015.
[5] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, 2005.
[6] L. Berek, Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014.
[7] M. W. Green, The Appropriate and Effective Use of Security Technologies in U.S. Schools, Washington: National Institute of Justice, 1999.
[8] D. Mann, „Facility Management," in Human Outsorcing Solutions to Clients, New Delhi, Global India Publications Pvt Ltd., 2009, pp. 43-44..

# EXAMINATION OF THE HISTORY OF INFORMATION SECURITY – DEVELOPMENT OF ERP SYSTEMS

# AZ INFORMÁCIÓBIZTONSÁG FEJLŐDÉSTÖRTÉNETI VIZSGÁLATA – AZ ERP RENDSZEREK FEJLŐDÉSE

BABOS Tibor[1] - ZÁHONYI Lajos[2]

**Abstract**

Today, the most common corporate decision support systems are Enterprise Resource Planning (ERP) systems. In this, IT systems are based on corporate processes and incorporate the principles of information security.

The present study takes stock of the history of corporate governance systems, presents some aspects related to corporate information security, and briefly summarizes the ERP system vendors that "dominate" the data of larger than average firms and companies today.

Without Enterprise Resource Planning systems, the operation of corporate processes is practically unthinkable, and the protection of the information data in the system is key.

The study also has interdisciplinary aspects: starting from the foundations of security science, it also touches the fields of informatics and history.

**Keywords**

information security, Enterprise Resource Planning, ERP, history of information security, SAP, ORACLE

**Absztrakt**

Napjaink legelterjedtebb vállalat-vezetői döntéstámogató rendszerei a vállalatirányítási rendszerek (Enterprise Resource Planning – ERP). Ezen az informatikai rendszerek a vállalati folyamatokra épülnek rá és beépítik magukba az információbiztonság alapelveit.

Jelen tanulmány sorba veszi a vállalatirányítási rendszerek fejlődéstörténetét, bemutat néhány - a vállalati információbiztonsághoz - kapcsolódó aspektusát és röviden összefoglalja melyek azok az ERP rendszer gyártók, amelyek globális viszonylatban „uralják" a közepesnél nagyobb cégek és társaságok adatait, napjainkban. A vállalatirányítási rendszerek nélkül a vállalati folyamatok működtetése gyakorlatilag elképzelhetetlen, a rendszerben lévő információs adatok védelme pedig kulcsfontosságú. A tanulmánynak interdiszciplináris vonatkozásai is vannak: biztonságtudományi alapokról indulva érinti az informatika, és a történettudomány területeit is.

**Kulcsszavak**

információbiztonság, vállalatirányítási rendszerek, ERP, információbiztonság története, SAP, ORACLE

[1] babos@uni-obuda.hu | ORCID: 000-0001-7459-8349 | director/igazgató | Óbudai Egyetem Biztonságtudományi Központ

[2] zahonyi.lajos@phd.uni-obuda.hu | ORCID: 0000-0001-9999-9624 | PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

„A biztonság és napjaink nemzetközi kapcsolatai tempójára, időbeli korlátjaira és egyben kilátásaira jelentős hatással van a globalizáció és a modernizáció. E két tényező új, eddig soha nem tapasztalt sebességre lendítette a fejlődés kerekét. [1] A tradicionális rend dinamikus liberalizálódása következtében hallatlanul fokozódik a gazdasági és technológiai szabadverseny. A gazdasági dimenzióváltás, a termelés, a fogyasztás és a szolgáltatások új struktúrái, a nemzetközi pénzügyek, a tudomány és az információ univerzálissá válása egyre erőteljesebben és radikálisabban alakítja át a nemzetközi rendet." [2]

A 20. század végére hihetetlenül felgyorsuló technikai fejlődés magával hozta az egyre nagyobb méretű és egyre nagyobb perspektívába gondolkodó ipari létesítmények, globális szolgáltatók és globális kereskedelmi vállalatok létrejöttét. A termelés, vagy szolgáltatás során kialakult információs dömping, azaz „kitermelt" és feldolgozandó adatok mennyisége és az ezzel párhuzamosan másik oldalon megjelenő adat-vákuum, amely azt az igényt fedi le, hogy a cég-irányítás minél több releváns információval rendelkezzen a vállalkozás folyamatairól, szinte törvényszerűen magába hordozta a vállalatirányítási rendszerek (ERP [3]) megjelenését és komplex fejlesztését. Manapság a közepes, vagy annál magasabb besorolású vállalkozások 99%-a használ valamilyen vállalatirányítási rendszert a munkája során. [4]

A tanulmány tézise, hogy az információ-biztonság fejlődéstörténetének súlyponti elemeiből kirajzolódó tendencia, meghatározó befolyást gyakorol a vállalatirányítási informatikai rendszerek fejlődésére. Másként fogalmazva: a jelenlegi ERP-rendszerek fejlődési alternatívái, az információbiztonság fejlődéstörténetébe beágyazottan alakulnak. A tanulmány – e tézis szellemében – amellett érvel, hogy az ERP-rendszerek fejlődéstörténetének valós súlyponti elemeinek meghatározása, kulcsfontosságú a tendencia vázolása és a további fejlődési alternatívák előrejelzése tekintetében. A tézis bizonyítása érdekében a tanulmány először általánosan bemutatja az ERP-rendszereket, azok elemeit, kialakulásuk fontosabb mozzanatait és időszakait. Ezt követően a jelenkor felhő-szolgáltatásait, valamint fontosabb szereplőit tárgyalja.

## ERP RENDSZER

Az ERP (vagy ERP system) egy angol mozaikszó, aminek az eredeti kifejezése az *Enterprise Resource Planning*[5] szavak rövidítése.

A magyar szóhasználatban vállalatirányítási rendszerként terjedt el bár a szó szerinti fordítása „Vállalati Erőforrás Tervezés" lenne.

Az integrált vállalatirányítási (ERP) rendszer alatt az egy vállalaton belül lezajló valamennyi műszaki, termelési, kereskedelmi, raktározási, készletgazdálkodási, pénzügyi, vezetési, irányítási és számos egyéb folyamat egységes, integrált számítástechnikai kezelését megvalósító információs rendszert értünk (Anderson, 2011) [6].

A vállalatirányítási rendszer-szoftver jellemzően több vállalati tevékenységi terület folyamataira terjed ki. A könyveléstől a beszerzésen át egészen a gyártósorokig.

A vállalatiirányítási rendszerek, üzleti menedzsment rendszerek, amelyek magukba foglalnak olyan funkcionális területeket támogató modulokat, mint a tervezés, gyártás, ér-

tékesítés, marketing, disztribúció, számvitel, pénzügyi, emberi erőforrás menedzsment, projekt menedzsment, készletgazdálkodás, szerviz és karbantartás, szállítás vagy éppen az e-business. [7]

Egy jól működő vállalatirányítási rendszer lehetővé teszi a szakmai területeken keletkező adatok gyűjtését, tárolását, kezelését, feldolgozását és értelmezését. Mindezt globális nagyvállalati, vállalatcsoporti, vagy akár vállalati részleg szinten is.


*1.ábra: Vállalatirányítási rendszerek (ERP) felépítése [8]*
*A komplexitás nem zárhatja ki az információbiztonság alapelveinek érvényesülését.*

Egy vállalatirányítási rendszerben folyamatosan frissülő adatokból előállított integrált képet (avagy riportot) kaphatunk a cég folyamatainak valós idejű helyzetéről. Mindezen adatok egy közös adatbázisban tárolódnak, amely adatbázisoknak biztosítani kell az információbiztonság alapelveinek teljesülését.

## ELVÁRÁSOK EGY ERP RENDSZERREL KAPCSOLATBAN

Érdemes megvizsgálni, melyek azok a szempontok, amelyek egy ERP rendszerrel szemben elvárásként megjelennek.

### Az adatok biztonsága

Mindenekelőtt egy ERP rendszer működésével szemben alapvető követelmény, hogy az adott ügyfél biztonságban tudja adatait, folyamatait. Egy modern vállalatirányítási rendszernek kell tudnia kezelnie a jogosultságokat és naprakész információkat kell szolgáltatnia 0-24 órában.

### Jogosultságok

Az ERP rendszerrel szemben elvárás hogy elkülönített és különböző jogosultságokkal „skálázható" szerepek „*userek*" legyenek definiálhatóak. Rendkívül fontos, hogy a rendszert használó szereplőknek „*userek*"-nek a szervezethez igazodva különböző szintű jogosultságokat lehessen beállítani, amely biztosítja az információs adatok védelmét is.

### Kényelem

Biztonságtudományi megközelítésből talán furcsa leírni ezt, de gyakorlatilag a modern ERP rendszerek használóinak és vásárlóinak az adatok biztonságos rendszerbe tartása mellett, komoly súllyal esik latba, hogy az adott rendszer mennyire használható, mennyire „esik kézre". Tudja-e a vezérigazgató vagy HR vezető a maga mobiltelefonján lekérni a számára fontos riportokat. Azt látja-e és úgy ahogy neki az szükséges. Bizony, ez már üzleti szempont is, mind az ügyfél mind a gyártónak.

### Flexibilitás

Az ERP rendszerek bevezetése egy vállalat életében egyfelől komoly pénzbeli beruházás, másfelől komoly időbeli ráfordítást is igényel. Mindezek mellett jogosan elvárható, hogy ezen vállaltirányítási szoftver rendszerek rugalmasan testre-szabhatóak legyenek egy adott vállalat folyamatira. Olyan rendszer legyen, ami a szervezeti változásokat kezelni képes. Fontos ez azért is, mert ezen szoftverek beruházása hihetetlen erőforrásokat kíván a szervezettől. Igaz ezek a befektetések – jobb esetben – megtérülnek.

### Integráltság

A vállaltirányítási rendszerek alapvető tulajdonsága az integráltság. A legideálisabb esetben az összes adat egy szoftver rendszeren keresztül össze van kapcsolva. Ugyanaz a rendszer szolgáltatja az adatot a termelési gyártósorról és akár ezen gyártósoron dolgozó szakmunkás bér adatairól is. Egy ilyen integrált megközelítésből, könnyen megállapítható például egy adott termék bekerülésének és előállításának a költsége. Ezek mind-mind vezetői döntéseket segítő érzékeny üzleti adatok, amelyek alapján üzleti döntések hozhatóak. Az integrálhatóságba beleérthető a további elszigetelt szakmai területek általüzemeltetett sziget alkalmazások adatainak integrálása is.

## ERP RENDSZEREK KIALAKULÁSA

### Kezdetek

Az ERP mai fogalma alatt egy komplex minden vállalati folyamatot magába foglaló rendszert értünk. Így volt ez 60 évvel ezelőtt is, csak azzal a különbséggel, hogy az akkori tudás- és ismereti-határokhoz a korabeli igények párosultak. Azaz kevesebb adatot tudtak kezelni ezért kevesebb igény merült fel.

A vállalatirányítási rendszerek együtt fejlődtek az informatikával, s a különféle technikai lehetőségekkel. Míg a kezdetekben az ERP rendszerek termelésirányítási rendszerekből nőttek ki, addig a XXI. században már a világ legnagyobb vállalatain kívül egészen a mikro-vállalatok is ERP-k segítségével irányítják magukat, optimalizálják az értékesítési, termelési, beszerzési, stb. működésüket.

Kijelenthetjük, hogy az integrált vállalati adatfeldolgozás igénye gyakorlatilag a számítógép megjelenésével majdhogynem egyidejű. Az adott kor eszközrendszerei és technikai határai azonban még nem tették lehetővé az magas szintű adatfeldolgozást.

*2. ábra: The IBM Naval Ordnance Research Calculator (1954), az első „szuperszámítógép" [9]. Az IBM NORC korának a legerősebb számítógépe volt és másodpercenként 15000 műveletet tudott végrehajtani. A fő memoriájában 2000 64 bites szó volt, ami 16 kilobájtnak felel meg. Az információs adatokat külön teremőr vigyázta…*

## A hatvanas évek – leltár ellenőrző rendszerek (Inventory Control System)

Talán nem véletlen hogy a vállaltirányítási rendszerek kialakulásának kezdete a jóléti társadalom kialakulásának és a tömegtermelés megindulásának időszakára esik. A termelés során készletek halmozódnak fel, a gyártáshoz alkatrészek kellenek, amiket szintén készletezni kell. Tömeges és pontos alkatrész-nyilvántartás elengedhetetlen. Kezdetben[10] a legtöbb termelő vállalat a maga sajátos központosított rendszerét használta, amelyekkel próbálták a lehetőségekhez képest maximálisan lefedni a leltározási folyamatokat. Ezek az IC (*Inventory Control System*) rendszerek az 1960-as években alakultak ki és közös jellemzőjük az volt, hogy belsőleg fejlesztették ki őket, valamit az, hogy –tekintve az integráltság hiányát – ritkán lehetet összevetni a havi, vagy negyedéves adatokat.

Ezek a partikuláris fejlesztések a mai szemmel nézve egyszerűnek tűnhetnek hiszen nagyon sok – a mai rendszerekben alapként tekintett – funkció hiányzott. Mégis ezek a kezdetleges számítógépekkel összekapcsolt kezdetleges rendszerek és a belőlük kinyert adatok voltak a termelés és forgalmazás optimalizása céljából kifejlesztett és használt első rendszerek.

## A hetvenes évek és az MRP (Materials Requirements Planning)

A hetvenes évektől megjelent az MRP szoftver amely egyfajta válasz volt a növekvő igényre, hogy minél inkább pontos adatok álljanak rendelkezésre a vállalatoknak. *Materials Requirements Planning* magyarul „anyagkövetelmény tervezés" egy olyan szoftver rendszer amely elsősorban a gyártás anyagszükséglet-számítási feladatokat végzi el. Fontos, hogy itt még nem beszélhetünk komplexitásról hiszen az adatok csak az adott vállalat egy bizonyos folyamatából származtak, mégpedig a termelési területről. Az információbiztonsági aspektusból tekintve, az adatok egy zárt rendszerben jelentek meg és ezen rendszerből készültek a kimutatások. Az információk védelmét inkább a fizikai eszközök és a belső szabályok védték.

Az első MRP rendszer az IBM és a traktorokat és építőipari gépeket gyártó J.I. *Case* közötti együttműködés eredményeképpen jött létre. [11] Case egy olyan megoldást keresett

ahol nyomon tudja követni a gépek gyártásához szükséges anyagszükségleteit. Az együttműködés eredményeképpen, valóban sikerült egy új rendszert kialakítani és működtetni, amelyben az anyagigények egy számítástechnikai rendszeren keresztül „futtatva" valós igényeket és felhasználási trendeket tudott előre jelezni. A szoftver alkalmazásával egy fajta beszerzési ütemezést tudtak elérni, amely egyaránt befolyásolta a nyersanyagok beérkezésének idejét, az áruk kiszállítását a gyárakból, és a készletek felhalmozását. A koprodukció nyomán J.I. *Case* úgy találta, hogy ezen rendszer használatával jelentős előnyre tett szert a versenytársakhoz képest. A hetvenes években az MRP rendszert csak kevés vállalat használta. A vállalatok többsége érezte a számítástechnika korlátait és az elterjedését az is gátolta, hogy az akkori számítástechnikai eszközök költsége rendkívül magas volt.

Érdemes megjegyezni, hogy 1970-ben egy MRP rendszert futtató számítógép mérete egy nagyobb iroda méretével volt összehasonlítható. Az egész szobát elfoglaló rendszer töredéknyi adatfeldolgozási szinttel rendelkezett, mint manapság egy-egy 8x12 cm méretű okostelefon.

**Nyolcvanas évek és az MRP II. (Manufacturing Resources Planning)**

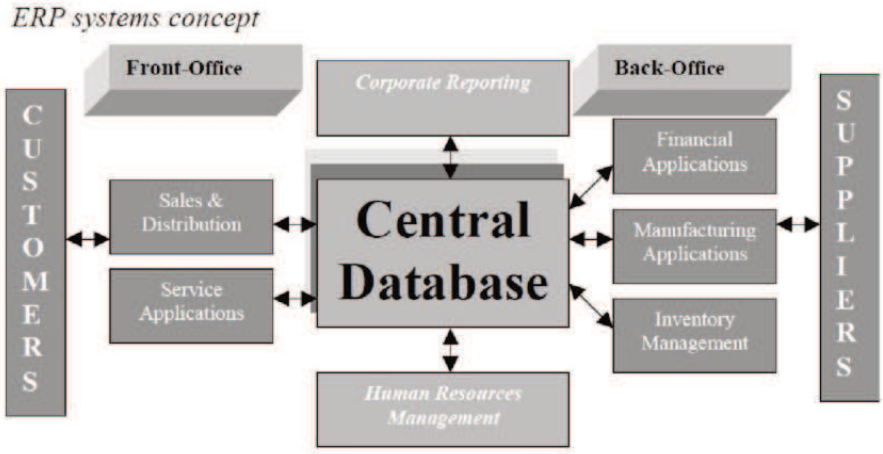
Az „MRP" mozaikszó azért kapta a „II." jelölést, mert fejlődéstörténet szempontjából itt már nem csak anyagkövetelmények kielégítéséről van szó, hanem a komplett gyártási folyamat szoftver szintű leképezéséről beszélünk. Az „MRP II. - *Manufacturing Resources Planning*" kifejezés „Gyártási erőforrás tervezési rendszert" jelent.

Az igények folyamatos emelkedése miatt szükség volt a gyártási folyamatok adatainak komplexebb megismerésére. Ez magával hozta az MRP-rendszerek folyamatos fejlődését, hiszen egyre több képességgel kellett rendelkezniük azért, hogy az egyre komplexebb adatokat pontosan tudja szállítani.

Az ERP-rendszerek ezen közvetlen elődje a gyártás optimalizálására helyezte a hangsúlyt a folyamatok a nyersanyag-igények és a termelési ütemtervek integrálásán keresztül. Az MRP II. tartalmazta a korábbi MRP rendszerek funkcionalitását, de tartalmazott már egyfajta integrációt (integráló funkciókat) amely lehetővé tette a vállalaton belül a különféle szervezetek és szervezeti egységek közötti átfogó koordinációt. A rendszer pénzügyi és munkavállalói adatokat is tartalmazott. [12] A *Manufacturing Resources Planning* rendszert az adatok feldolgozására és integrálására fejlesztették ki, hogy a vállalkozások valós adatokra alapozott döntéseket tudjanak meghozni és ezáltal a hatékonyságukat növelni tudják a termékek előállítása során. [13]

**Kilencvenes évek – az ERP rendszer megjelenése (Enterprise Resource Planning)**

A klasszikus ERP rendszerek immár 30 évesek. Az első komplex vállalati igényeket és vállalati folyamatokat lefedő rendszerek az 1990-es években jelentek meg.




*3. ábra: Az ERP rendszer koncepciója – Komplexitás, integráció és valós idejű adatok. Az információk védelme a rendszer alapvető része. [14]*

A kilencvenes években megjelenő *Enterprise Resource Planning* (ERP) rendszerek már képesek voltak kielégíteni a vállalatok komplex üzleti igényeit. Az ERP rendszerek modulokból épülnek fel. Egy-egy modul egy adott területet fed le. A területekről jövő adatok integráltan kerülnek feldolgozásra. A feldolgozás során egy adatbázist használ a szoftver.
Ezek az 1992-ben megjelenő SAP R/3 rendszer alapvető moduljai [15]:

- AA - Eszközkönyvelés
- CO - Kontrolling
- CS - Vevőszolgálat
- FI - Pénzügyi könyvelés, számvitel
- HR - Emberi erőforrások
- MM - Anyaggazdálkodás
- PM - Karbantartás
- PP - Termeléstervezés és irányítás
- PS - Projekt rendszer
- QM - Minőségbiztosítás
- SD - Értékesítés
- WM - raktárgazdálkodás

A kilencvenes évek elején az ERP-rendszerek még helyszíni partikuláris adatokból dolgozott. Az internet megjelenésével és gyors elterjedésével évtized végére az ERP-rendszerek már nem egy előzetesen kalkulált becsült adatok alapján működtek, hanem valós idejű adatokat tudtak szállítani a lekérdezőnek. Ezáltal lényegesen javult a folyamatok hatékonysága.

Az alapvető különbség az MRP II. és az ERP rendszerek között, hogy míg az MRP II. tradicionálisan a belső erőforrások tervezésére és ütemezésére fokuszált az ERP rendszer már alkalmas volt megtervezni a szállítói erőforrások és a vevői igények és ütemtervek összehangolását.

**Kétezres évek – ERP II. azaz a továbbfejlesztett ERP rendszerek**

Az ERP rendszerek a kilencvenes években „jöttek, láttak és győztek”. A vállalatok egyre másra vezeték be őket és az igény csak folyamatosan nőt. Nem véletlen, hogy a szoftvergyártó óriások ezen évtizedben alapozták meg piaci pozícióikat. A komplex ERP rendszerek megjelenése és az azt követő széleskörű elfogadottsága után számos szoftvergyártó cég kezdte tovább bővíteni az alapvető szolgáltatásait. Az ERP II. rendszerekben további funkciók kaptak helyet, úgymint HR, vezetői döntéstámogatás, beszállítók és vevők kezelése, szerződés nyilvántartás, projekt nyilvántartás, és ügyfélkapcsolati nyilvántartás. Ezek a „kiterjesztett” ERP rendszerek és alkalmazások már tartalmaznak ügyfélkapcsolati menedzsment rendszert, a munkafolyamatok leképezését és speciális iparági (pl.: közmű szektor) megoldásokat is. [16]

**Jelenkor – ERP és a felhő**

A vállalatirányítási rendszerek fejlődésének következő állomása, az SaaS modell elterjedésének hozománya. [17] „*Software as a Service*” azaz magyar kifejezésként „szoftver mint szolgáltatás” vagy „szolgáltatott szoftver” fordítható. Ennek a modellnek a lényege, hogy a szoftver és a kapcsolódó adatok nem a cégnél vagy az igénybe-vevőnél vannak tárolva, hanem egy internet felhőben. Ugyanakkor a felhasználó gyakorlatilag 0-24 időtartamban hozzáfér az adatokhoz egy web-böngészőn keresztül.


*4. ábra: SaaS modell - A fejlődés megállíthatatlan. A „mindent a felhőbe” elv lassan átveszi az ERP rendszerek feletti uralmat, ez újabb információvédelmi kihívásokat jelent.*

A vállalatirányítási rendszerek telepítésének ezen módszere rendkívül sok időt, energiát és nem utolsó sorban pénzt takaríthat meg egy szervezet számára. Ezek a szoftvercsomagok távoli eléréssel leszállíthatóak, telepíthetőek, működtethetőek anélkül, hogy a végfelhasználónak kellene befektetnie a szükséges hardver eszközökbe vagy infrastruktúrába, amelyek biztosítanák számukra a helyszínen a működést. Ez jelentősen csökkenti a vállalkozások beruházási költségeit, ezért az ERP rendszerek piacának terjedése, bővülése egyre inkább gyűrűzik a közép-vállalati szektor felé.

## A LEGNAGYOBB ERP RENDSZER GYÁRTÓK

### SAP AG. [18]

A legnagyobb vállalatirányítási szoftvergyártó céget öt IBM-ből kilépő mérnök alapította 1972-ben Németországban, hogy üzleti szoftvert fejlesszenek a vállalatok számára. Maga az SAP szó egy mozaikszó a „*System, Application és a Product*" szavakból áll össze. 1992-ben adták ki az első ERP rendszerüket az SAP R/2. Az igazi nagy áttörést azonban az első teljesen integrált és minden vállalati kulcsfolyamatot lefedő kiadása jelentettet az SAP R/3. Ezzel a termékkel az SAP gyakorlatilag az ERP piac vezetőjévé vált. Jelenleg világszerte több mint 18 300 ügyféllel és 200 millió felhasználóval rendelkeznek 180 országban.

### JD Edwards & Co [19]

A JD Edwards 1977-ben alakult Denverben (Amerikai Egyesült Államok, Colorado Állam), az IBM szoftver szállítójaként. Az általuk gyártott szoftvereket sok amerikai cég használta. Nevükhöz fűződik a „*OneWorld*" nevű – inkább középvállalat méretű cégeket megcélzó – szoftver termék. Az ORACLE 2003-ban felvásárolta.

### The BAAN Company [20]

Az 1978-ban alapított holland cég már az internet elterjedésének korában lépett az ERP piacra. A BAAN szoftver páratlan kereszt-funkcionalitásáról híres, amelyek könnyen lefedik a különböző üzleti aspektusok és a speciális eszközök közötti kapcsolatot. A bevezetési költségek tervezhetőségét segítő ún. „Orgware" funkció segített abban, hogy piacvezetők legyenek a védelmi szolgáltatások terén és a repülőgépiparban egyaránt.

### ORACLE [21]

Az 1977-es alapítású Oracle Corporation egy amerikai multinacionális számítástechnikai vállalat, amelynek székhelye a *Redwood Shores*-ban, (Amerikai Egyesült Államok, Kalifornia Állam) van. A cég adatbázis-szoftvereket és technológiákat, felhő által tervezett rendszereket és vállalati szoftvertermékeket értékesít. 2019-ben az Oracle a világ második legnagyobb szoftvergyártó cége volt, több mint 430 000 ügyfelével 175 országból.

## ÚJ BIZTONSÁGI TRENDEK ERP TERÜLETEN

### Oracle White Paper - Information Security [22]

Az ORACLE 2011-ben kiadta a „Fehér Könyv"-et, amely a szoftverhez kapcsolódó adatvédelmi és információbiztonsági elveket fekteti le.

Az ORACLE elvek:

- „*Defence in Depth*" - a biztonsági architektúra egyetlen elemének meghibásodása sem veszélyeztetheti az egész informatikai környezetet.
- „*Least Privilege*" – a rendszer felhasználóinak a lehető legkevesebb kivételt engedélyeznek.
- „*Security as a Service*" – az üzleti megoldásokat úgy kell megtervezni, hogy azok minél inkább a közös biztonsági beállítások alapján működjenek. Ahol lehet, törekedni kell az egyedi biztonsági logika elhagyására és a másolatok másolásának elkerülésére.

- „*Identity Federation*" - A biztonsági infrastruktúrának biztosítania kell az identitásleképezést, és a hitelesítő adatok leképezését.
- „*Secure Web Services*" - A webszolgáltatások használata nem veszélyeztetheti a teljes körű rendszerbiztonság és más biztonsági elvek betartását.
- „*Secure Management of Security Information*" Biztonsági információkat, mint például felhasználói adatok, hitelesítő adatok, csoportok, szerepek tulajdonságait, biztonságos és ellenőrizhető módon, központilag (holisztikusan) kell kezelni az egész szervezetben.
- „*Active Threat Detection & Analysis*" A biztonsági infrastruktúrának képesnek kell lennie a rendellenes viselkedés észlelésére és ennek megfelelően alkalmazkodnia kell erőforrások sebezhetőségének védelmében.
- „*Secure, Complete Audit Trail*" - A biztonsági rendszernek képesnek kell lennie arra, hogy azonosítsa a dokumentumok és folyamatok változtatásának időpontját és személyét.
- „*Data Security*" - Az adatok titkosságát, integritását és elérhetőségét mindenkor biztosítani kell
- „*System Availability*" A rendszereket megfelelően védeni kell úgy hogy a védelem szükségtelenül ne akadályozza a tevékenységek végrehajtását.

**SAP Security Information and Event Management [23]**

A vállalatirányítási rendszerek funkcióinak fokozatos bővülése nem kerülte el az ERP rendszerek információbiztonsági vetületeit sem. Az SAP Enterprise *Threat Detection* (SAP Vállalati Fenyegetettség Érzékelés) keretében azonosítja, elemzi és semlegesíti a rendszert ért kibertámadásokat, amint azok bekövetkeznek és mielőtt még súlyos károkat okoznának a rendszerben. Ezt a „*Security Information and Event Management* (SIEM)" eszköz alkalmazásával éri el, amely valós idejű intelligenciát használ a rendszer külső és belső kiberbiztonsági fenyegetésekkel szembeni sebezhetőségének hatékony kezeléséhez és az adatvédelem biztosításához.

## ZÁRÓ GONDOLATOK

Az információbiztonság három alapelvre épül. Az egyik alapelv, hogy az adott információ sértetlen legyen, pontos maradjon és ne torzuljon. A második, hogy az arra felhatalmazott felhasználó mindig hozzáférjen az adott információhoz és kapcsolódó értékekhez. A harmadik elv, a jogosultság, avagy bizalmasság kérdése, vagyis csak az arra jogosult, vagy felhatalmazott személy számára legyen elérhető az adott információ. A vállalati ERP-rendszerek gazdasági igényekre válaszul az információbiztonság ezen három alapelve mentén alakultak ki és fejlődnek napjainkban. A vállalat-irányításban használt informatikai rendszereknek biztosítaniuk kell, hogy a termelésről, a szolgáltatásról és a gyártó sorokról pontos információk érkezzenek be. Hiszen egy-egy rossz adatra épített döntés akár dollár milliókat vehet ki a vállalat költségvetéséből és a tulajdonosok képzeletbeli és valós zsebéből. Alapvető követelmény, hogy ezen vállalati folyamatok során előállított adatok rendelkezésre álljanak. Nem lehet becslésekre és ködös információkra építve felelős vállalati döntéseket hozni. Nem utolsó sorban egy vállalatirányítási rendszernek biztosítani kell a vállalat különböző szintjeihez tartozó jogosultságok beállíthatóságát. Hiszen mást kíván látni

egy vállalat élén álló igazgatósági tag és mást kell látnia egy vállalati pénzügy osztályon dolgozó könyvelőnek.

Egy vállalatra vonatkozóan a tömeges adatok kinyerésének legfőbb eszköze az ERP-rendszer. Ezen döntéstámogató eszközök folyamatos fejlődése tekinthető egyfajta válasznak a kor kihívásaival szemben és ugyanakkor tekinthető az információbiztonság elveire épülő gazdaság igényeket kielégítő eszköz(rendszer)nek is.

## FELHASZNÁLT FORRÁSOK

[1] Thomas L. FRIEDMAN, *The Impact of Globalization on World Peace, Working Paper No. Burkle Center for International Relations*, University of California, Los Angeles, January 1,7 2001, 27, p. 3., Online: http://www.international.ucla.edu/CMS/files/friedman.pdf (2004. január 21.)
[2] Tibor BABOS, *The Five Central Pillars of European Security* 2007 p62
[3] ERP - Enterprise Resource Planning https://dictionary.cambridge.org/dictionary/english/enterprise-resource-planning (letöltés ideje: 2020.05.28.).
[4] Középvállalkozás fogalma: *Európai Bizottság - Felhasználói útmutató a kkv-k fogalom meghatározásához* (p11) (letöltés ideje: 2020.05.28.).
[5] Forrás: https://www.sap.com/hungary/products/what-is-erp.html (letöltés ideje: 2020.05.28.)
[6] Forrás: http://oktato.econ.unideb.hu/domician/Downloads/ppt/sap_alapok.pdf (letöltés ideje: 2020.05.24.)
[7] Mohammad A. RASHID, Liaquat HOSSAIN, Jon David Patrick (2002) - *The Evolution of ERP Systems: A Historical Perspective Chapter* I pp2
[8] Forrás: https://corealm.com/blog/what-is-sap-why-is-it-important (letöltés ideje: 2020.05.28.)
[9] Forrás: https://royal.pingdom.com/retro-delight-gallery-of-early-computers-1940s-1960s/ (letö-ltés ideje: 2020.05.24.)
[10] Piper THOMSON - *The Complete History of ERP: Its Rise to a Powerful Solution* (2020)
[11] Forrás: https://www.erpandmore.com/erp-reference/erp-history/ (letöltés: 2020.05.24.)
[12] Forrás: https://www.omniaccounts.co.za/articles (letöltés ideje: 2020.05.24.)
[13] Piper THOMSON - *The Complete History of ERP: Its Rise to a Powerful Solution* (2020)
[14] Forrás: https://www.researchgate.net/figure/ERP-systems-concept_fig1_309575659 (letöltés ideje: 2020.05.24.
[15] Forrás: https://answers.sap.com/questions/4702151/how-many-functional-modules-in-r3.html (letöltés ideje: 2020.05.30.)
[16] Tamás Fejér - *Vállalkozási informatika* (2013) pp"1.3.2. ERP rendszerek"
[17] Peter LAIRD - *How Oracle, IBM, SAP, Microsoft, and Intuit are Responding to the SaaS Revolution* (2008) http://peterlaird.blogspot.com/2008/06/how-oracle-ibm-sap-microsoft-and-intuit.html (letöltés ideje: 2020.05.24.)
[18] Mohammad A. RASHID, Liaquat HOSSAIN, Jon David Patrick (2002) - *The Evolution of ERP Systems: A Historical Perspective Chapter* I. pp.9
[19] uo. pp.12

[20] uo. pp.11.
[21] uo. pp.10
[22] Oracle White Paper - *Information Security: A Conceptual Architecture Approach* (2011) p25
[23] Forrás: https://www.sap.com/hungary/products/enterprise-threat-detection.html#contact-us (letöltés ideje: 2020.05.28.)

**Online irodalom**


1. Peter LAIRD - How Oracle, IBM, SAP, Microsoft, and Intuit are Responding to the SaaS Revolution (2008) http://peterlaird.blogspot.com/2008/06/how-oracle-ibm-sap-microsoft-and-intuit.html (letöltés ideje: 2020.05.24.)
2. SAP Általános Üzleti Feltételek - https://www.kozbeszerzes.gov.hu/frameagreement?p_p_id=FrameAgreementPortlet_WAR_PubProcPortal&_FrameAgreementPortlet_WAR_PubProcPortal_viewMode=DATA&_FrameAgreementPortlet_WAR_PubProcPortal_frameAgreementId=1404 (letöltés ideje: 2020.05.24.)
3. ERP - Enterprise Resource Planning https://dictionary.cambridge.org/dictionary/english/enterprise-resource-planning (letöltés ideje: 2020.05.28.)
4. https://www.sap.com/hungary/products/what-is-erp.html (letöltés ideje: 2020.05.28.)
5. http://oktato.econ.unideb.hu/domician/Downloads/ppt/sap_alapok.pdf (letöltés ideje: 2020.05.24.)
6. https://corealm.com/blog/what-is-sap-why-is-it-important (letöltés ideje: 2020.05.28.)
7. https://royal.pingdom.com/retro-delight-gallery-of-early-computers-1940s-1960s/ (letöltés ideje: 2020.05.24.)
8. https://www.erpandmore.com/erp-reference/erp-history/ (letöltés: 2020.05.24.)
9. https://www.omniaccounts.co.za/articles (letöltés ideje: 2020.05.24.)
10. https://www.researchgate.net/figure/ERP-systems-concept_fig1_309575659 (letöltés ideje: 2020.05.24.
11. https://answers.sap.com/questions/4702151/how-many-functional-modules-in-r3.html (letöltés ideje: 2020.05.30.)
12. https://www.sap.com/hungary/products/enterprise-threat-detection.html#contact-us (letöltés ideje: 2020.05.28.)
13. https://www.erpandmore.com/erp-reference/erp-history/ (letöltés ideje: 2020.05.28.)
14. https://www.oracle.com/topics/technologies/security.html (letöltés ideje: 2020.05.28.)

# EVENTS IN THE CYBERSPACE UNDER COVID-19

# ESEMÉNYEK A KIBERTÉRBEN A COVID-19 JÁRVÁNY IDEJÉN

KUN Tamás[1]

**Abstract**

In the mists of the pandemic, hackers do not rest. A 'great' opportunity for them to exploit the uncertainty of these days and to sabotage national healthcare systems, that were in combat with the virus, so the protection of IT systems could be fall behind with the priorities, often remains on the theoretical basis, that is because of the criminal activities that happened recently. At the start of the year and the new decade, the Coronavirus Disease (COVID-19) created stressful circumstances all over the world, that took time even for the World Health Organization (WHO) to address that pandemic worldwide. The growth of cyber-attacks against medical institutions are showing ascending tendency, so the development and defense of these systems will be a determining issue for the following years. The successful defence sometimes not only technological issue, rather the quality of the human factor. In most cases, the attackers breaching over the loose ends of top secured systems, so the best practice should be controlling these at organizational level.

**Keywords**

IT security, cyber activities, pandemic, critical infrastructures

**Absztrakt**

A járványhelyzet idején a hackerek nem pihennek. Egy remek lehetőség számukra ugyanis, hogy a kiszámíthatatlan helyzetben, ami jellemzi a mindennapokat államok egészségügyi szervezeteinek működését szabotálják, amelyek éppen a vírus elleni küzdelemmel vannak nagyobb részben elfoglalva, így az informatikai rendszerek védelme nem feltétlenül prioritás, gyakran csak elméleti szinten valósul meg, mert ezt alátámasztják a megtörtént bűncselekmények, amelyek nemrégiben bekövetkeztek. Az új évtized kezdetén a COVID-19 nevet viselő új koronavírus meglehetősen stresszes körülményeket generált szerte a világban, még az Egészségügyi Világszervezet (WHO) is csak késlekedve minősítette világjárványnak azt. Az egészségügyi intézmények ellen elkövetett kibertámadások az utóbbi években növekvő tendenciát mutatnak, így ezeknek a rendszereknek a fejlesztése és védelmének javítása meghatározó témája lesz a következő éveknek. A sikeres védekezés viszont sokszor nem technológiai kérdés, hanem az emberi tényező minősége. A támadók az esetek döntő többségében a gyenge láncszemeken keresztül jutnak be a legvédettebb rendszerekbe, így a legjobb megoldás ezt szervezeti szinten kezelni.

**Kulcsszavak**

IT biztonság, kibertevékenységek, járványhelyzet, kritikus infrastruktúrák

[1] kun.tamas@phd.uni-obuda.hu | ORCID: 0000-0002-6620-7157 | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Az elmúlt néhány évben egyre inkább közkedvelt célpontjaivá váltak a kritikus infrastruktúrák a kibertérben tevékenykedő szereplők számára, azonban maga a fogalom is vitatott, hogy mi számít kritikus infrastruktúrának. A magyar jogi szabályozás létfontosságú rendszerelemként is számon tartja ezeket az intézményeket, amelyeknek tartós kiesése a napi működésből beláthatatlan következményekkel járhat. Egy dolog azonban egészen bizonyos, a kórházak a társadalom kiemelt fontosságú rendszerelemei, azok részleges leállása is emberéletek kockán forgásával jár. Az egészségügyi adatok az Általános Adatvédelmi Rendelet (GDPR) alapján is érzékeny (sensitive) személyes adat [1] kategóriába tartoznak, azok védelme és kompromittálódásának elkerülése prioritást élvez az adatvédelem területén.

## ANYAG ÉS MÓDSZER

A vizsgálat tárgyát képezik azok a kibertevékenységek és intézkedések, amelyek a COVID-19 világjárvánnyal kapcsolatosan vagy annak tematizálásával kerültek fókuszba. Ezek az események azért fontosak, mert világszerte nemzetközi forgalmi korlátozások, közösségi távolságtartásra vonatkozó szabályozások vannak érvényben, amelyeknek hatásait csak azok feloldását követően leszünk képesek értékelni, valamint mérni a hatásait. A jelenlegi helyzet alapvető sérülékenységi faktorát tekintve elmondható, hogy az esetek/próbálkozások számát tekintve jelentős potenciállal bír a járványhelyzet kihasználása a pszichológiai manipulációs technikák alkalmazását illetően. Ez a környezet továbbá lehetőséget nyújt arra is, hogy a potenciális áldozatok száma növekedjen, tekintettel a kilátástalan helyzetre, valamint az általános bizonytalanságra, amely jellemzi a mindennapokat. Világszerte a jogi eszközökkel és egyéb jogosítványokkal felhatalmazott kormányok és szervezetek igyekeznek az általános pánikhelyzet elkerülésére, valamint a lépcsőzetes lazításra és a folyamatos visszatérésre törekednek a megszokott életvitel felé. Azonban a kibertér szereplőit a támadói oldalon motiválja a zavart állapot, hiszen az emberi tényező ebben a szituációban újabb és újabb sérülékenységeket generál. Ilyen sérülékenységi pont lehet akár a távmunka általánossá válása is, az otthonról végzett munka esetében a belső hálózatok szigorú szabályrendszerével ellentétben külső hozzáférési pontokról csatlakoznak a munkavállalók, előfordulhat az is, hogy saját eszközökről, amelyek biztonsági szintje megkérdőjelezhető. Fő irányvonalként a járvány megjelenésének idejétől (2019 december) a közelmúltig (2020 április) terjedő időszakot tekintem, helyenként viszont korábbi évek trendjeire is utalok. A tanulmányban szereplő események a források megjelenési idejét alapul véve vannak időrendi sorrendben.

## EREDMÉNYEK

### Zsarolóvírusos támadások egészségügyi rendszerek ellen

2018-ban az egészségügyi szervezetek a negyedik legáltalánosabb célpontjai (7%) voltak a zsarolóvírusos (ransomware) támadásoknak az iparági megoszlás alapján, egy 2019-ben megjelent a Cylance kiberbiztonsági vállalat elemzésében [2]. “Néha a zsarolóvírus olyan, mint az influenza. Amint a kórházak megoldást találnak a védelemre, egy új és

kifinomultabb verzió üti fel a fejét.” 2019 decemberében Hackensack Meridian Health csoport, amely 17 korházat számlál New Jerseyben lévő székhellyel, megerősítette, hogy fizetett a zsarolóknak annak érdekében, hogy újra hozzáférjen az informatikai rendszereihez. Ebből az következett, hogy a rendszerek két napig nem voltak elérhetők, és az osztályokat nem kritikus folyamatainak újra szervezésére, papíralapú dokumentálásra kényszerítette az elektronikus megoldások helyett. [3] „Ne vessük el azonnal a váltságdíj kifizetésének lehetőségét.” mutat rá Robert Garrett, a Hackensack Meridian Health igazgatója. A továbbiakban leszögezi, hogy sok esetben nem áll módunkban alkudozni a támadókkal, mert nem vagyunk abban a luxusban, hogy újraépítsük a rendszereinket, az idő szorít bennünket. [4] Amit ebben az esetben megfigyelhetünk, az a teljes kiszolgáltatottság. Egy kórházigazgató szemszögéből nézve az álláspont helytálló, viszont védelmi szempontból a kapitulációval egyenlő. Sokszor hivatkoznak ilyen típusú esetekben a szakértők véleményére a döntéshozók, hogy mennyire helyes vagy sem váltságdíjat fizetni. Újra felmerül a kérdés, hogy a kibertevékenységek terrorista, adott esetben háborús cselekményeknek azonosíthatók e, viszont az elkövető személy/csoport jellemzően rejtve marad. A kibertámadásokkal kapcsolatban általában elmondható, hogy a visszakövetési folyamatban (IP-címek visszakövetése) csak országokig jutunk el, tehát annyit tudunk meghatározni, hogy melyik országból érkezhetett a támadás, a konkrét elkövető nemzetisége sem határozható meg sok esetben, ezért „casus belli” (háborús indok) sem fogalmazható meg.

## Átfedések a koronavírus járvánnyal kapcsolatban

A Yoroi olasz hátterű kiberbiztonsággal foglalkozó vállalat szokásos vizsgálatai során egy „CoronaVirusSafetyMeasures_pdf” állományra figyelt fel, amelynek jobban utána jártak. Itt egy átlagos social engineering taktikáról, egy phishing típusú támadásról beszélhetünk, a fentebb említett állomány egy email csatolmányát képezhette, egy külön erre kialakított tesztkörnyezetben hajtották végre a feltárást. A fájl megnyitása után több művelet zajlik le, először egy TLS alapú védett kapcsolatot alakít ki, amely egy “share.]dmca.]gripe” elérési útvonalú fájlmegosztóra mutat, ezt a fájlból kinyert mintából is ki tudták olvasni. Ezután néhány script fut le, amelyek megalapozzák a fertőzést, kulcsok generálódnak a beállításjegyzékben (1. ábra), amelyek segítenek elkerülni a számítógép újraindításával kapcsolatos eljárásokat. Végeredményképpen a felállított kapcsolat alapján adathalászatra kiválóan alkalmas fertőzéses támadásról van szó. [5]


*1. ábra: A malware sematikus fertőzési útvonala [5]*

Amit ebben az esetben láthatunk az a szokásos eszköztár: tömeges vagy célzott célpont irányába elkészített levél és egy vagy több álcázott melléklet az aktuális téma alapján.

A COVID-19 keretei között éppen azért kiemelten veszélyesek ezek a próbálkozások, mert egy olyan világjárványról van szó, amellyel kapcsolatban minden egyes esemény egyenesen internetközpontú terjesztéssel is rendelkezik. A világ országaiban a meghatározó médiumok napi szinten számolnak be a „fejleményekről" idővel a társadalom teljesen elveszíti a napi rutinját a kitörést megelőző időkkel szemben. Felerősödik a „rugalmas" megoldások alkalmazása, széles körben terjednek el az internetalapú távoli hozzáférés útján történő munkavégzési megoldások, ezzel pedig újabb sebezhetőségek jelennek meg.

**CISA ajánlás a COVID-19 keretében jelentkező kockázatkezelésben**

A kibertevékenységek elemzése során célszerű nem csak a támadási eseményeket górcső alá venni, hanem annak fontos elemeit is, mint például a kritikus infrastruktúrák és az ellátási láncok, mert ezeknek a rendszereknek, intézményeknek, folyamatoknak a működtetése a rendkívüli helyzetben kiemelten fontos, valamint deklarálja azt a környezetet, ahol a támadók potenciális célpontjai találhatók.

Az Egyesült Államok Védelmi Minisztériuma (DHS) márciusban mind a járványhelyzettel, mind a kiberbiztonsági eljárásokkal kapcsolatban tesz javaslatokat, ahol több kulcsterületet határoz meg:

Infrastruktúra védelmi intézkedések (Kritikus Infrastruktúrák)

- Kijelölni a koordináló személyt és speciális felelősségi kört rendelni hozzá
- Kivitelezni egy hivatalos munkavállalói és munkahelyvédelmi stratégiát
- Képezni a munkavállalókat a személyes és munkahelyvédelmi stratégiákra
- Kiépíteni és tesztelni a rugalmas munkavégzés feltételeit és munkarendjének szabályozását
- Azonosítani a kritikus folyamatokat, javakat és szolgáltatásokat, amelyek elősegítik a szükséges működést
- Meghatározni, hogy mennyi ideig képes nélkülözni a szervezet a működéshez szükséges utánpótlásokat a csökkentett termelési kapacitások tekintetében
- Azonosítani és priorizálni a szükséges áruk és szolgáltatások beszállítóit
- Folyamatosan értékelni az aktív készültségi szintet a tervcélok elérése érdekében, vizsgálni azoknak hatásait, illetve az eseményeket, amelyek a megváltozott üzleti tevékenységből és társadalmi-gazdasági viszonyokból fakadnak
- Követni a szövetségi, állami, helyi, törzsi és területi COVID-19 tartalmú információs portálokat naprakész információért az enyhítéssel és társadalmi elszigeteléssel kapcsolatos stratégiákhoz [6]

Ellátási lánccal kapcsolatos intézkedések

- Mérlegelni a kieséseket az ellátási láncban a nemzetközi termelés és szállítás lassulásából fakadóan, ami a COVID-19 miatt jelentkezik
- Egyeztetni a szállítókkal bármely nehézség kapcsán, ami a helyzetből ered, illetve amire a jövőben számítani lehet
- Azonosítani az alternatív forrásokat a készletek, helyettesítő termékek és/vagy védelmi intézkedések területén, amelyek a zavarok enyhítését célozzák

Kapcsolatot létesíteni a törzsvásárlókkal, folyamatosan tájékoztatni az érdekükben tett enyhítésekkel kapcsolatos lépésekről [6]

Kiberbiztonsági intézkedések szervezetek számára

Biztosítani a rendszereket, amelyek távoli hozzáférést tesznek lehetővé

- Meggyőződni arról, hogy VPN kapcsolat van alkalmazásban, valamint a rendszerek naprakészek
- Fejleszteni a rendszerellenőrzést annak érdekében, hogy minél előbb információhoz jussunk szokatlan működés esetén
- Többlépcsős azonosítás alkalmazása
- Meggyőződni arról, hogy minden eszközön tűzfal és vírusírtó- és behatolás meggátló szoftver konfigurálva legyen
- Tesztelni a távoli hozzáférés kapacitásait
- Növelni a tudatos használat szintjét a távoli hozzáférést alkalmazók számára
- Frissíteni a reagálási terveket a megváltozott munkaerőszükséglet vonatkozásában [6]

Kiberbiztonsági intézkedések munkavállalók és ügyfelek számára

- Kerülni a kéretlen levelekben található linkek és azok csatolmányainak megnyitását
- Ne fedjünk fel személyes és pénzügyi adatot, valamint ne küldjünk választ kéretlen tartalomra
- Tekintsük meg a CISA útmutatását a pszichológiai manipuláció és adathalászati technikák felismeréhez a COVID-19 járvánnyal kapcsolatban
- Tekintsük meg a Szövetségi Kereskedelmi Bizottság által közzétett bejegyzést a koronavírus járvány során megismert csalási kísérletekkel kapcsolatban
- Használjunk megbízható forrásokat legitim kormányzati oldalakat, amelyek naprakész és hiteles információkkal szolgálnak a COVID-19 járvánnyal kapcsolatban [6]

### A „FormBook” malware a koronavírus köntösében

A MalwareHunterTeam szakértői felfedtek egy kampányt, ami a COVID-19 kötelékében terjed. A támadók a WHO képviselőiként adják ki magukat, a kéretlen levélben egy .zip állományban van a FormBook elnevezésű információlopásra tervezett trójait letöltő futtatható program MyHealth.exe néven. Korábban kiberkémkedési céllal ezt a kártékony kódot alkalmazták már amerikai és dél-koreai célpontok ellen is. [7]

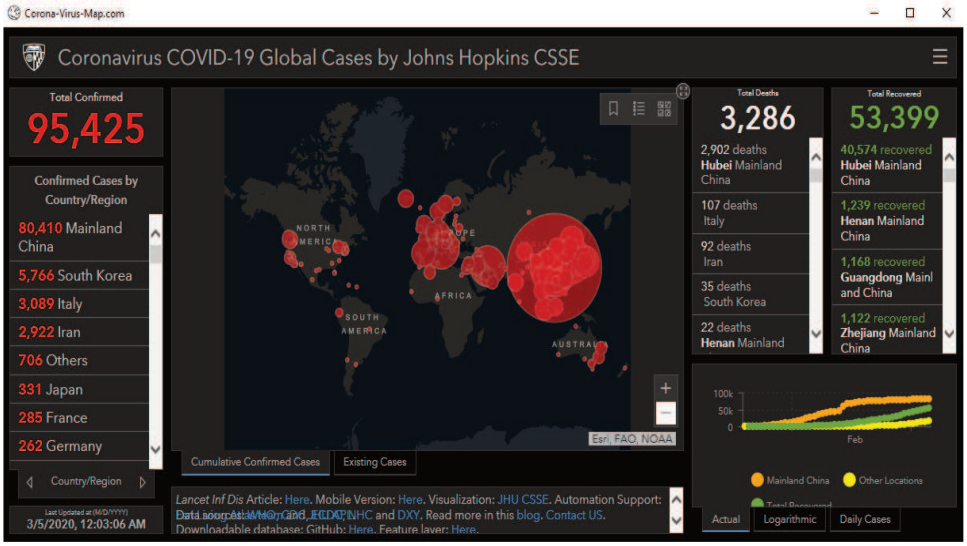
A FireEye elemzése alapján a kártékony kód helyi jelszavakat, sütibeállításokat, vágólapon szereplő tartalmakat, valamint adatokat lop el http időszakokból. A kód továbbá képes parancsokat is végrehajtani egy távoli vezérlőszerverről (C2) többek között: letölteni és futtatni fájlokat, folyamatokat elindítani, leállítani és újraindítani a számítógépet. [8]

### A COVID-19 terjedésével foglalkozó térkép weboldalának hamisítványa

Egy grafikus felhasználói felület (Graphical User Interface) használatával a háttérben fut a rosszindulatú kód (malware) AZORult névvel fémjelezve. Ezt az információlopási technikát 2016-ban fedezték fel először, illegális orosz oldalakon közkedvelten árulták.

Böngészési előzmények, bejelentkezési adatok, sütibeállítások és kriptovaluták lopására alkalmazták, valamint az ellopott adatokat további értékesítésre bocsátásának a lehetősége is adott. A kód többszintes összeállításban fut, multi-sub-process (azaz párhuzamosan és egymásra épülő, könyvtárrendszeri szinten) annak érdekében, hogy egy vizsgálat lefolytatását nehezebbé tegye. Annak érdekében, hogy a futása tartós legyen, a feladatütemezőt használja az operációs rendszerben. [9]

A kártékony kódot tartalmazó GUI felület (2. ábra) az eredeti webes forrásból kapja az adatokat, így a gyanútlan szemlélőnek akár fel sem tűnik, hogy nem hivatalos helyről szerzi az információkat. Az emberi természetet és a kíváncsiságra való hajlamosságot használja ki a támadó, altatva a célpont biztonságérzetét.




*2. ábra: A Corona-Virus-Map.com grafikus felülete [9]*

## Ransomware támadás egy cseh kórház ellen járvány közepén

Helyi idő szerint reggel 5 óra körül kibertámadás érte a Brno-i Egyetemi Kórházat 2020 március 14.-én a járvány közép-európai terjedésének sűrűjében. A kórház kénytelen volt leállítani informatikai struktúráját az incidens alatt, valamint érintette két alszervezetét is. A központi hangosbemondóban fél óránként elhangzott, hogy minden dolgozó állítsa le a számítógépét kibernetikai biztonsági okokból. Reggel 8 óra magasságában pedig újabb üzenet került bemondásra a hangosbemondóban, mely szerint az aznapi összes orvosi beavatkozás szünetel. [10] Egy nappal később túlterheléses támadás érte az Egyesült Államok egészségügyi és szociális minisztériumát is, melynek során nem történt behatolás, illetve negatív fejlemény. A támadás, ami a HHS szervereit érte nem bizonyult eredményesnek, mert számottevő lassulást nem sikerült elérnie. [11]

## Iráni hátterű kibertámadások a WHO dolgozói ellen

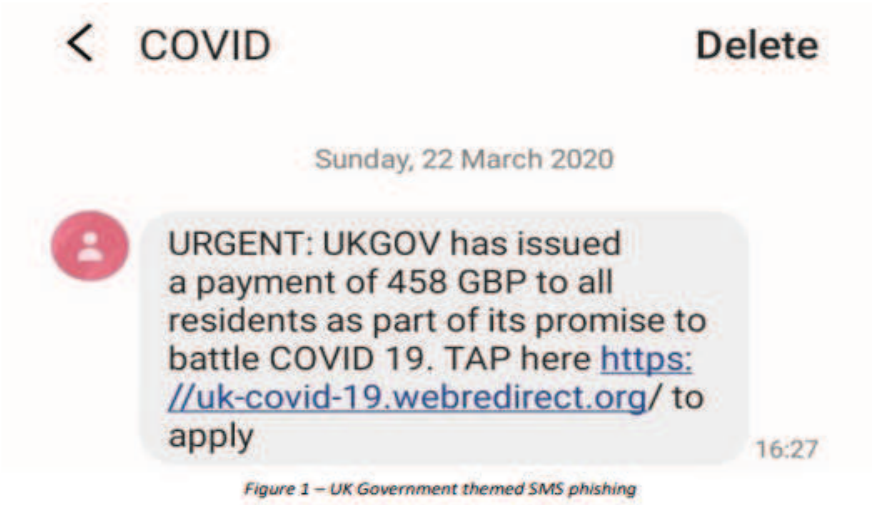
A Reuters márciusi közleménye alapján az ENSZ egészségügyi szervezetei és a hozzá kapcsolódó intézmények ellen elkövetett támadások megduplázódtak a COVID-19 járvány kezdete óta. A legutóbbi próbálkozás jelszavak ellopása volt a WHO dolgozóitól,

előre elkészített emaileket küldve személyes emailpostafiókjaikra, melyekben álcázott Google webes szolgáltatásokkal igyekezték megvezetni az áldozatokat. [12] A Foreign Policy beszámolója szerint, a mostani járványhelyzet miatt különösen fontos lenne, hogy globális szinten lévő magatartás legyen a kibertérben az egészségügyi szervezetek védelme érdekében. A lap továbbá beszámol arról, hogy a világ most végül kénytelen lépéseket tenni az egészségügyi infrastruktúra kiberbiztonsága végett.

A fenyegetettség azonban nem újkeletű, 2017-ben egy New York állam béli, Buffaloban lévő kórház, az Erie County Medical Center ellen elkövetett zsarolóvírusos támadás során a NotPetya vírus használatával 10 millió USA dollár értékben követeltek bitcoin kriptovalutát a támadók, a több, mint 6000 zárolás alatt álló számítógép feloldásáért cserébe. [13]

**A National Cyber Security Centre tapasztalatai a COVID-19 kapcsán jelentkező kártékony szereplőkkel szemben**

Az NCSC áprilisi kiadványában többek között szerepel egy SMS-alapú adathalászati kísérlet (3. ábra), ahol a támadó az Egyesült Királyság kormányának adja ki magát, és egy hivatalosnak tűnő szöveg mellett egy külső weboldalra mutató linket küld az áldozat számára. A kiadvány a továbbiakban kitér arra is, hogy a támadók nem csak email alapon jelentkezhetnek, WhatsApp és egyéb chatalkalmazásokat is előszeretettel használnak. Jellemzően bejelentkezési adatok ellopására törekednek, pénzügyi haszonszerzés céljával. De további példaként megemlítenek egy phishing kampányt is 2020 március 19.-i kezdettel, ahol Dr. Tedros Adhanom Ghebreyesus, feladótól a WHO főigazgatójának kiadva magukat az Agent Tesla nevű leütéskövető kémprogramot igyekeznek terjeszteni. Más kampányokban Excel fájlok is alkalmazásra kerülnek, amelyek megnyitása után egy makró fut le, ami aktiválja a rosszindulatú kód letöltését, erre példa a 'EMR Letter.xls.' nevű állomány, amelybe egy beágyazott dynamic-link library (DLL) telepíti a Get2 loader malware-t. Ez a kód pedig a GraceWire trójai programot telepíti a továbbiakban, ami a számítógép feletti irányítás átvételére hivatott. [14]




*3. ábra: COVID-19 témájú SMS-alapú adathalászat [14]*

**Adatszivárgás a Beaumontnál, 112 000 érintett adatainak kiszivárgása**

Az amerikai Michigan állam legnagyobb egészségügyi intézményében történt adatszivárgásról tett bejelentést 2020 április 17.-én a Beaumont Health Services, melynek során aktív és korábbi páciensek adatai kerültek illetéktelen kezekbe. A kikerült adatok természetét tekintve a páciensek neve, születési ideje, társadalombiztosítási azonosítója, egészségügyi állapotukra vonatkozó információ, valamint helyenként banki adatok, de még vezetői engedélyek adatai is kompromittálódtak. A kórház több, mint 1000 igazolt COVID-19 fertőzöttet kezelt ebben az időszakban. Ebben az évben ez a második eset, 2020 januárjában 1182 pácienst értesítettek, hogy egy munkavállaló jogosulatlan hozzáférése során kerültek ki adatok egy személyi sérülésekkel foglalkozó ügyvédi iroda számára. [15]

A pénzügyi érdek (financial gain) ahogyan általában megfigyelhető az információlopás szándékával elkövetett kibertevékenységek során itt is jól tetten érhető, hogy a járványhelyzetet kihasználva a támadó könnyűszerrel ragadta meg a lehetőséget. Egy negyedéven belül két támadás egészségügyi adatok megszerzése céljával pedig intő jel a társadalom számára.

## KONKLÚZIÓ

Néhány hónap leforgása alatt eljutottunk oda, hogy valós veszélye van annak, hogy többtízezres nagyságrendben kerülhetnek adatok illetéktelen kezekbe, akár hivatalos ajánlások megjelenése után pár héttel. A támadások volumene a korábbi évekhez képest, főként az egészségügyi szektorban a járványhelyzettel kapcsolatban multiplikálódott, ez a jövőre tekintettel még inkább aggasztó, mert a támadások száma és a károkozások mértéke jelentős. A járványhelyzet nem csak a távoli hozzáférés és munkavégzés elméleti és gyakorlati megoldásaiban változtatott, de új irányokat is felvázol, abba az állapotba, ami előtte volt, visszatérni már nem fogunk tudni. Továbbra is azt állítom, hogy teljes mértékben biztonságos rendszer nem létezik, hiszen az ember/munkavállaló, mint tényező mindig jelen lesz a folyamatokban, hasonlóan egyéb csalási eseményekhez, a kiberbiztonság területén is törekedni kell a belső tájékoztatásra, ezzel hatékonyan tudjuk csökkenteni a fennálló kockázatokat és növelni tudjuk a szervezeti reagálóképességet egy lehetséges incidens esetére.

## HIVATKOZÁSOK

[1] European Commission, „What personal data is considered sensitive?,” 18 12 2019. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en. [Hozzáférés dátuma: 23 05 2020].

[2] Cylance, 25 02 2019. [Online]. Available: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf?_ga=2.194100014.207560192.1557408928-1034628078.1557241850. [Hozzáférés dátuma: 23 05 2020].

[3] J. K. Cohen, „Ransomware targeting health systems in more 'sophisticated' ways,” 24 01 2020. [Online]. Available: https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways. [Hozzáférés dátuma: 20 05 2020].

[4] R. Garrett, „Lessons learned from a targeted ransomware attack," 20 12 2019. [Online]. Available: https://www.modernhealthcare.com/opinion-editorial/lessons-learned-targeted-ransomware-attack. [Hozzáférés dátuma: 23 05 2020].
[5] Yoroi, „New Cyber Attack Campaign Leverages the COVID-19 Infodemic," 25 02 2020. [Online]. Available: https://yoroi.company/research/new-cyber-attack-campaign-leverages-the-covid-19-infodemic/. [Hozzáférés dátuma: 08 04 2020].
[6] CISA, „CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19)," 06 03 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf. [Hozzáférés dátuma: 21 05 2020].
[7] Nemzeti Kibervédelmi Intézet, „VIGYÁZAT: ÚJABB KORONAVÍRUS MALSPAM KAMPÁNYOKAT FEDEZTEK FEL," 03 2020. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/vigyazat-ujabb-koronavirus-malspam-kampanyokat-fedeztek-fel/. [Hozzáférés dátuma: 23 05 2020].
[8] P. Paganini, „New Coronavirus-themed malspam campaign delivers FormBook Malware," 08 03 2020. [Online]. Available: https://securityaffairs.co/wordpress/99156/cyber-crime/coronavirus-spam-campaign.html. [Hozzáférés dátuma: 14 05 2020].
[9] Reason Labs, „COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report," 09 03 2020. [Online]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. [Hozzáférés dátuma: 13 03 2020].
[10] C. Cimpanu, „Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," 13 03 2020. [Online]. Available: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/?fbclid=IwAR3jE3mDkxTfKSL8UOeGlsqaXsgQ1wN_SekAn7t9EEMpYr5BW-fA9XX3p4M. [Hozzáférés dátuma: 20 03 2020].
[11] S. Stein és J. Jacobs, „Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 16 03 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. [Hozzáférés dátuma: 29 05 2020].
[12] J. Menn, C. Bing, R. Satter és J. Stubbs, „Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources," 02 04 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC. [Hozzáférés dátuma: 29 05 2020].
[13] C. Ruhl, „Note to Nations: Stop Hacking Hospitals," 06 04 2020. [Online]. Available: https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/. [Hozzáférés dátuma: 23 05 2020].
[14] National Cyber Security Centre, 08 04 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf. [Hozzáférés dátuma: 23 05 2020].

[15] D. Walsh, „Data breach at Beaumont exposes information of 112,000 patients,” 17 04 2020. [Online]. Available: https://www.crainsdetroit.com/health-care/data-breach-beaumont-exposes-information-112000-patients. [Hozzáférés dátuma: 26 04 2020].

# APPEARANCE OF THE END USER NEEDS ABOUT THE ENERGY CONSUMPTION EFFICIENCY AND RELIABILITY OF THE PRODUCT

# VÉGFELHASZNÁLÓI IGÉNYEK MEGJELENÉSE AZ ENERGIAFELHASZNÁLÁS HATÉKONYSÁGÁNAK ÉS A TERMÉK MEGBÍZHATÓSÁGÁNAK NÖVELÉSE ÉRDEKÉBEN

BESZÉDES Bertalan[1]

**Abstract**

My study, which deals with domestic and foreign sources, aims to present the development possibilities of technical equipment used in industrial and civil fields, from the point of view of energy efficiency. Following the introduction of the topic, I will write about the emerging needs of end users and then I will present the results of a questionnaire-based needs survey. In a separate sub-chapter I deal with the user-tracable and user-controllable modes of operation of the technical equipment and the possibilities of cost-effective feasibility. At the end of my study, after summarizing the results, I discuss the centralized energy use controlling.

**Keywords**

energy efficiency, reliability, lifetime, maintainability, serviceability, tracebility, modularity

**Absztrakt**

Hazai és külföldi forrásokat feldolgozó tanulmányom célja, hogy az ipari és polgári területen használt műszaki berendezések fejlesztési lehetőségeit mutassam be, az energiahatékonyság szempontjából. A téma bevezetését követően a végfelhasználók újonnan megjelenő igényeiről írok, majd ismertetem egy kérdőív alapú igényfelmérés eredményeit. Külön alfejezetben foglalkozom a műszaki berendezések felhasználó által monitorozható és befolyásolható működési módjaival és a költséghatékony megvalósíthatóság lehetőségeivel. Tanulmányom zárásaként az eredmények összefoglalása után a központosított energiafelhasználás felügyeletéről értekezem.

**Kulcsszavak**

energiahatékonyság, megbízhatóság, élettartam, karbantarthatóság, szervizelhetőség, monitorozhatóság, modularitás

[1] beszedes.bertalan@amk.uni-obuda.hu | ORCID: 0000-0002-9350-1802 |assistant lecturer/egyetemi tanársegéd | Óbudai Egyetem Alba Regia Műszaki Kar

## BEVEZETÉS

A 21. század globalizált gazdasága számtalan olcsó termékkel árasztja el a világot. Számos az említett termékek közül folyamatosan csökkenő minőségű és élettartamú. Sokak számára értelmetlen ez a nagy mértékű fogyasztás, mivel a bolygónk erőforrásai végesek. Valahol mind érezzük, hogy ez messze nem helyes. A jelen társadalom fényűző homlokzata mögött idő előtt leselejtezett eszközök által alkotott szeméthalmok tömege rejlik.

Miért van az, hogy az egykor drága státusszimbólumok meghibásodás okán a roncstelepen végzik? Miért van az, hogy az új még fel nem használt alapanyagok a szeméttelepen végzik? Vajon mennyi alapanyag és energiaráfordításba került az előállításuk. A kérdésekre a válasz érkezhet egy kérdés formájában is: Vajon meddig folytatható ez a pazarló gyakorlat? Ideje újragondolni a korszerű energiafelhasználással kapcsolatos általános megközelítést.

Megváltoztatni a jelenlegi gazdasági működést igen nehéz, de lehetőséget javasolni az erőforrások egy opcionális felhasználási módjára igen hasznos. Számos felhasználó szívesen áldozna fel az általuk használt eszköz teljesítményéből, ha ezért cserébe megnőne a használt berendezés élettartama. Ezzel a lehetőséggel kevés berendezés rendelkezik – háztartási berendezések közül egy sem –, pedig piaci igény van rá, és biztosítása alacsony költségen megoldható.

## ENERGIAHATÉKONYSÁG

Honnan tudhatjuk, hogy egy eszköz, háztartás vagy éppen ország mennyire energiahatékony?

Az ország gazdaságának energiaintenzitását gyakran használják az energiahatékonyság mutatójaként - főleg azért, mert összesített szinten, ez a mutató viszonylag könnyen elérhető az országok értékeléséhez és összehasonlításához. Azonban, egy alacsonyabb energiaintenzitású országban nem feltétlenül szükséges magas energiahatékonyság. Például egy enyhe éghajlattal rendelkező, kis, szolgáltatás-alapú ország alacsonyabb intenzitással bírna, mint egy hideg éghajlattal rendelkező nagy ipari alapú ország, még akkor is, ha az utóbbi országban az energiát hatékonyabban használják fel. Ugyanígy, az alacsonyabb intenzitás irányába mutató tendenciákat nem feltétlenül vezérli a hatékonyságjavulás. Ezért fontos részletesebb elemzést végezni, amely betekintést nyújt a végső energiafelhasználási trendeket befolyásoló tényezőkbe.

2009-ben az IEA (International Energy Agency – Nemzetközi Energiaügynökség) felismerte az energiahatékonysági politikák jobb ellenőrzésének szükségességét, ez magában foglalja a végfelhasználások országspecifikus elemzését a legnagyobb ágazatokban - lakásépítés, szolgáltatások, ipar és közlekedés. Az energiahatékonysági politikák elengedhetetlenek a kulcsfontosságú energiapolitikai célok eléréséhez, mint például az energiaszámlák csökkentése, az éghajlatváltozás és a légszennyezés kezelése, az energiabiztonság javítása és az energiahatékonyság növelése. Ennek ellenére a globális politikai lefedettség (~35%) számos lehetőséget hagy kihasználatlanul.

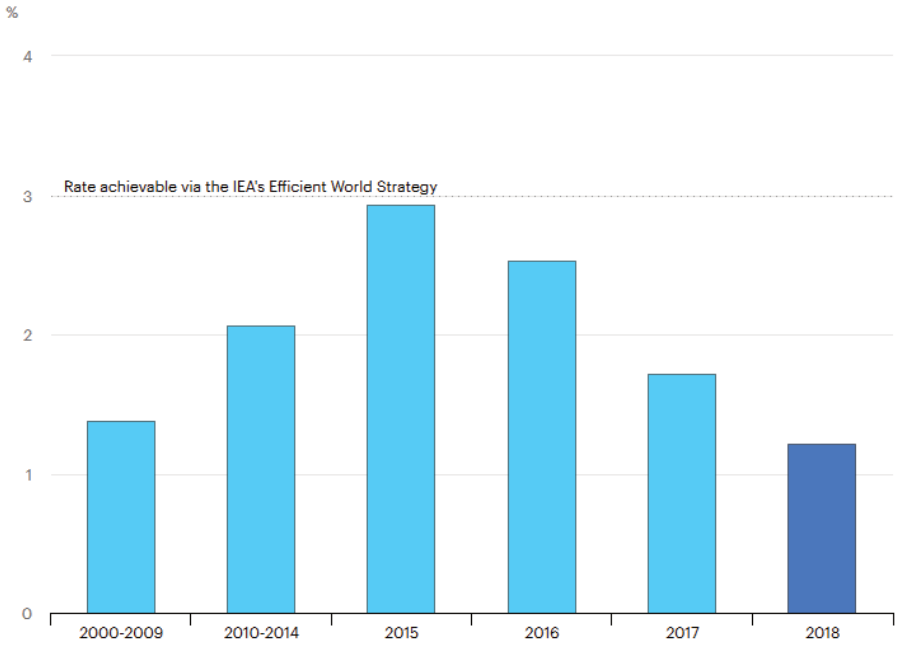
Az energiahatékonysággal kapcsolatos megbízható adatok és mutatók kulcsfontosságúak az energiahatékonysági politikák hatékonyságának megismeréséhez és nyomon követéséhez, mivel ezek mutatják az energiaigényt.

Az IEA statisztikai elemzéseiből látható, hogyan alakul az IEA tagországok végső energiafelhasználása és nyomon követhető a nemzeti energiahatékonysági politikák fejlesztési irányai és megvalósulási hatékonyságai is. [1] A kitűzött és elfogadott évenkénti 3%-os hatékonyság növekedést egyelőre nem sikerült megközelíteni.

## ENERGIAHATÉKONYSÁG VÁLTOZÁSA

A globális energiahatékonysági fejlesztések csökkenő lendülete komoly aggodalomra ad okot. Az IEA Energy Efficiency 2019 jelentése a fogyasztók, a vállalkozások, a kormányok és a környezet szempontjából súlyos következményekkel bíró lassulásnak az okait vizsgálja. [2]

2015 óta a globális energiaintenzitás javulása évente gyengül. A fűtés, hűtés, világítás, mobilitás és egyéb energiaszolgáltatások iránti igények folyamatosan nőnek. A globális gazdaság energiaintenzitásának (a gazdasági tevékenység egységenként felhasznált energiamennyiség) javulása lassul. [3] A 2018. évi 1,2% -os javulás a 2010. óta megfigyelt átlag fele körül volt (1. ábra). Jóval a kívánatos 3%-os átlagérték alatt jár a mutató. Ez tükrözi az új energiahatékonysági politikák relatív hiányát és a meglévő intézkedések szigorításának szükségességét. [4]




*1. ábra: A primer energiaintenzitás globális javulása, 2000-2018 [5]*

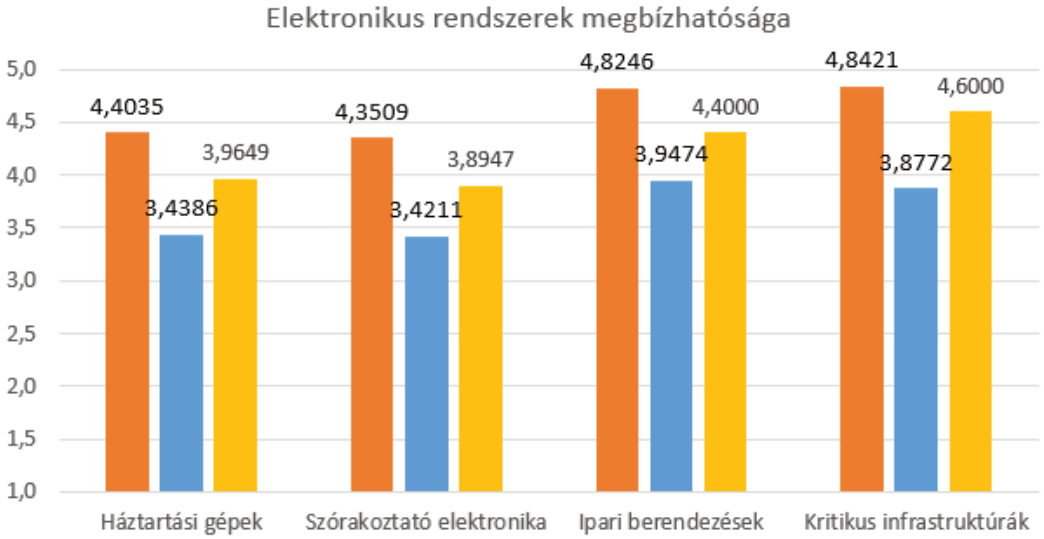
## EREDMÉNYEK

Jelen tanulmány a háztartási és ipari, villamos energiával működtetett berendezések szempontjából vizsgálódik. Az ismertetett eredmények ugyan nem hoznak közvetlen globális változást, de valós adatokkal mutatják meg a kutatás létjogosultságát. Ily módon pedig alapul szolgálna tényleges fejlesztések kezdeményezéséhez.

A kutatás alapját szolgáló kérdőívek kitöltői jellemzően műszaki oktatásban részt vevő, műszaki oktatásban részt vett, műszaki munkakörben dolgozó vagy műszaki érdeklődésű nők és férfiak, a 18-27 éves korosztályból. Ez az a csoport, akinek legnagyobb mértékben és értékben lesz ráhatása a beszerzendő műszaki berendezés kiválasztására és/vagy fejlesztésére.

A kérdőívben a megkérdezettek 1-től 5-ig terjedő skálán, egész számokkal adhattak választ a kérdésekre. Az 1-eshez tartozott a „nem fontos”, az 5-öshöz a „nagyon fontos” jelentés. A két érték között fokozatos átmenet volt.

A válaszadók a háztartási gépek, szórakoztató elektronikai eszközök, ipari villamos berendezések és kritikus infrastruktúrákban megtalálható elektronikus rendszerek szempontjából értékeltek. A 2. ábra kategóriánkénti első oszlopa (narancssárga) mutatja, hogy a megkérdezettek szerint mennyire fontos az adott területen az elektronikai rendszerek megbízhatósága; a második oszlopa (kék) mutatja, hogy a megkérdezettek szerint az adott területen mennyire megbízhatóak az elektronikai rendszerek; a harmadik oszlopa (citromsárga) mutatja, hogy a megkérdezettek szerint az adott területen mennyire tartják fontosnak az elektronikus rendszerek megbízhatóságának növelését.

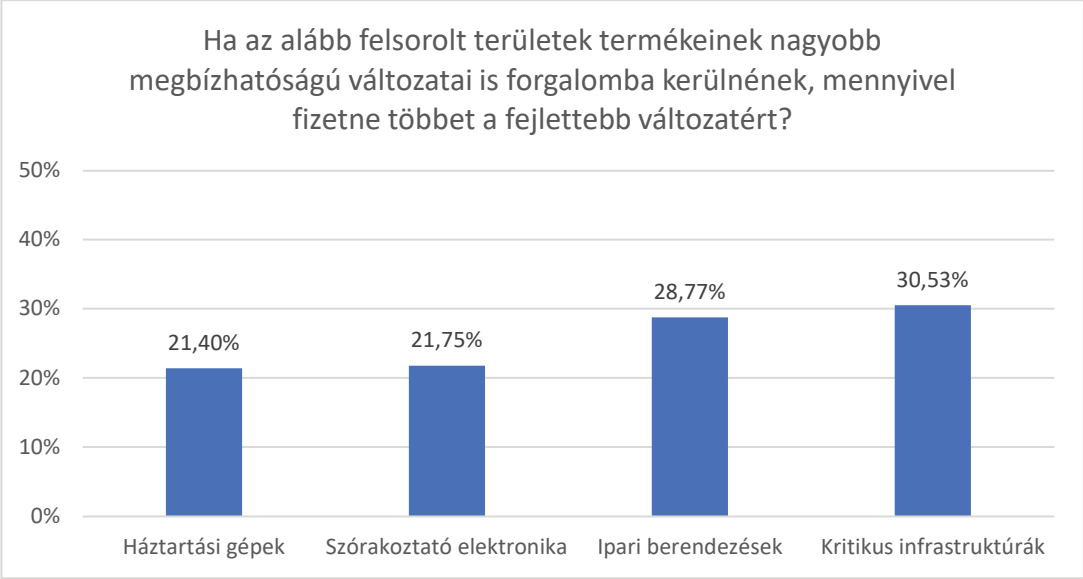



*1. ábra: Elektronikus rendszerek megbízhatósága*

Az adatokból jól látszik, hogy a felhasználóknak, mind polgári-, mind ipari berendezések terén igénye van a nagyobb megbízhatóságú elektronikus berendezésekre és rendszerekre. Ez az igény az alábbi ábra szerinti fizetőképes keresletben is megmutatkozna. A vizsgált területeken ~20-30%-os árnövekedést is vállalnának a végfelhasználók, ha ezért nagyobb megbízhatóságú eszközöket használhatnának. (A kérdőívben 10%-os pontossággal volt lehetőség a válaszadásra.)

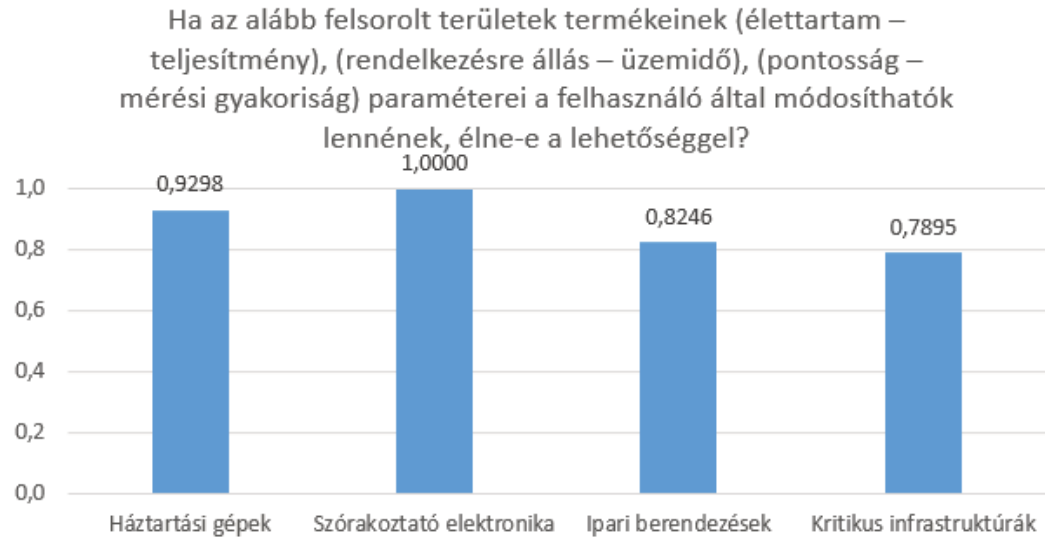
A polgári és ipari elektronikus berendezések megbízhatóság növelése minimális költségen lehetséges például: magasabb minőségű alkatrészek beépítése, konstrukciós változások eszközölése, tervezési és tesztelési alapelvek változtatása, minimális költségű hardver és szoftver modulok beépítése, stb. A hosszútávú eladási darabszámok és értékesítési

stratégiák tárgyalása ennek a cikknek nem célja, de jól látható egy új optimum kialakításának lehetősége, amivel a környezeti terhelés nagy mértékben csökkenthető.




*2. ábra: Nagyobb megbízhatóságú elektronikai berendezések többletköltségének vállalási hajlandósága*

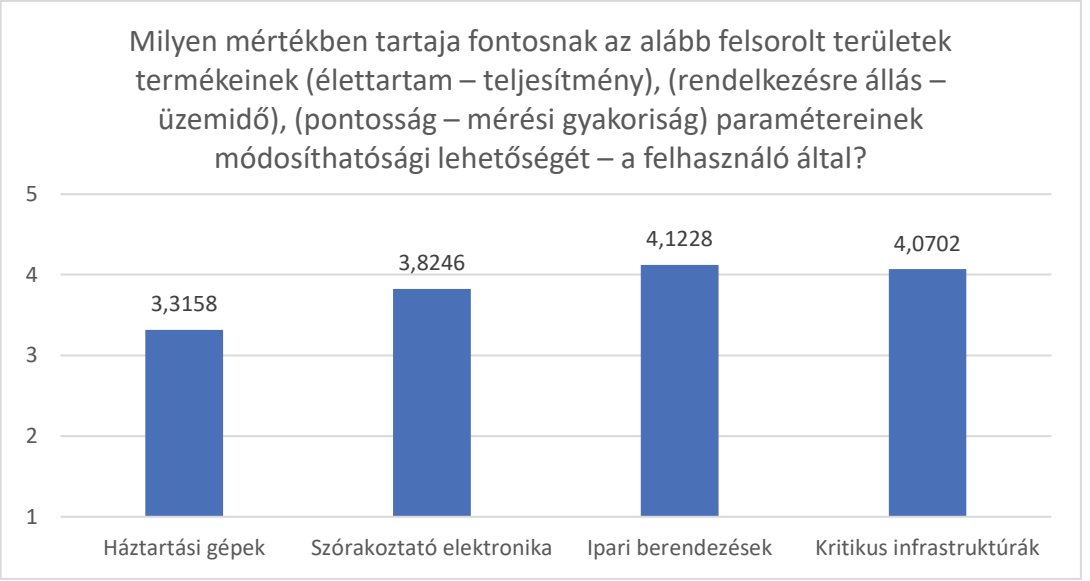
Belátható, hogy a különböző gyártók, különböző termékcsaládjainak, különböző termékeinek, különböző változatainak és évjáratainak tovább skálázása a megbízhatóság szempontjából nem feltétlenül járható út (beleértve a gyártói szoftveres, esetleg licenszelt lehetőségeket is). Lehetőségként kínálkozik a végfelhasználó kezébe adni a termék finombeállításának képességét.



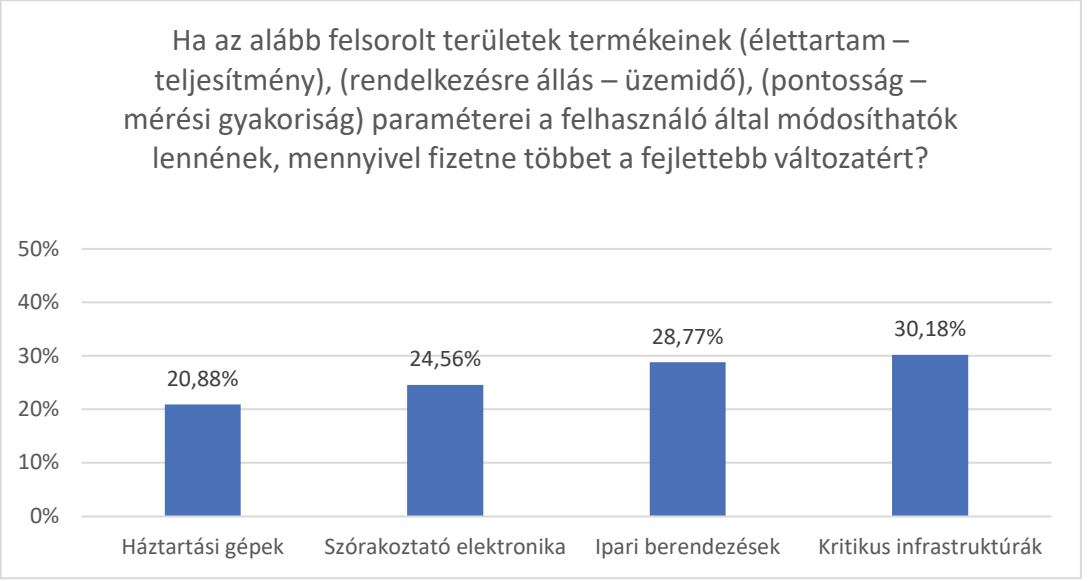

*3. ábra: Felhasználók igénye az általuk skálázható elektronikai berendezésekre*

A 4. és 5. ábrán látható, hogy erre nagy igénye lenne a felhasználóknak (a kérdőívet kitöltők válaszlehetősége igen vagy nem volt), kiemelten a polgári területeken. A polgári elektronikus berendezések alapanyagfelhasználása és környezeti terhelése – mennyiségükből adódóan – jóval nagyobb, mint az ipari berendezéseké.

Polgári elektronikai berendezések esetében szintén fontos az élettartam kérdése (alapanyag és erőforrás felhasználásának és veszélyes hulladék keletkezésének mértéke szempontjából).




*4. ábra: Felhasználó által skálázható elektronikai berendezések*




*5. ábra: Felhasználó által skálázható elektronikai berendezések többletköltségének vállalási hajlandósága*

Az ipari elektronikai berendezések esetében elsősorban az élettartam (üzembiztosság szempontjából), állásidő, szervízidő és egyéb megbízhatósági paraméterek állnak szemben a teljesítménnyel.

A szigetüzemű tápellátással rendelkező berendezések esetében a rendelkezésre állás-üzemidő-teljesítmény közötti egyensúlyról dönthet a felhasználó. Az energiafelhasználás (ébrenléti idő, számítási idő és teljesítmény) valamint a mérések pontossága és gyakorisága is kínál beállítási lehetőséget. Szoftveres/firmwares megoldással automatizálható – a felhasználói beállításokhoz igazodva – az energiafelhasználás, csökkenthető a mérések gyakorisága (csökkentve az ébrenléti időt) valamint a mérések pontossága (csökkentve a mérési és számítási időt) amennyiben a mért érték nem, vagy csak nagyon lassan változik. Amennyiben a mért paraméter változási sebessége megnövekszik, akkor a mérési gyakoriság és a mérési pontosság is követi azt. A 6. ábrán látható, hogy a fizetőképes kereslet szintén ~20-30%-os többletköltséget vállalna az opció megléte érdekében.

## MODULÁRIS FELÉPÍTÉS

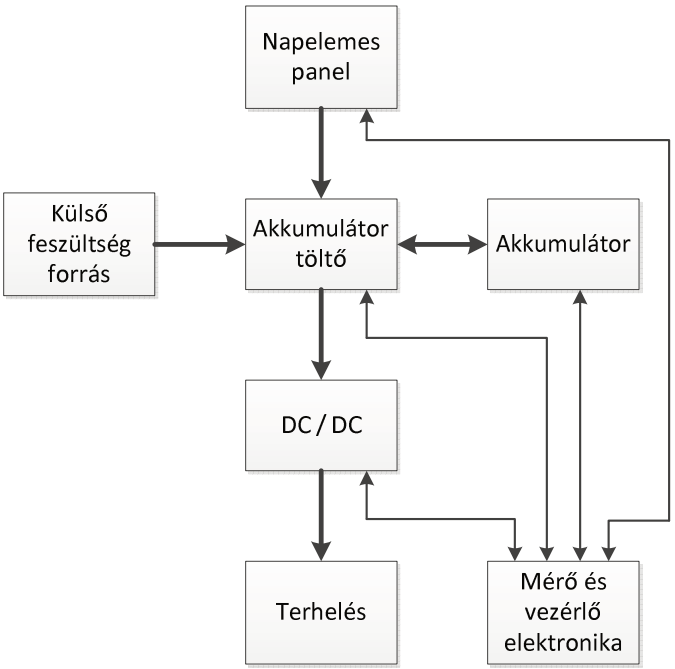
A hétköznapok során használt műszaki eszközeink egyre bővülő tára és csökkenő használati ideje egyre több hulladáktermelést és erőforrásfelhasználást jelent. A felhasználók bővülő műszaki ismeretei és a műszaki berendezésekbe történő beavatkozási hajlandósága egyre növekszik. Az internet segítségével a javításhoz szükséges információk is széles körben, könnyen hozzáférhetőek.

Fontos, hogy csak a megfelelő műszaki előképzettséggel rendelkező felhasználók módosítsanak villamos berendezéseket, valamint fontos a megfelelő műszaki előképzettséggel rendelkező felhasználók számának növelése. Javasolt a középiskolai álltalános képzés hangsúlyos részévé tenni az alapvető műszaki ismeretek elsajátítását azzal a céllal, hogy a hétköznapi műszaki problémákat a végfelhasználók önállóan képesek legyenek megelőzni vagy elhárítani.

Moduláris felépítésű elektronikus berendezések némi többlet térfogat, hardver, szoftver és mérnökóra árán még kevesebb erőforrás felhasználása és hulladék termelése mellett javíthatóak meghibásodás esetén.

Az alábbi példa egy szigetüzemű moduláris tápellátó rendszer modellje található. A 7. ábrán a modell blokkvázlata látható. A modulok rögzítése csavarkötéssel vagy rugalmas fülek segítségével könnyen megoldható, a közöttük lévő oldható galvanikus kapcsolat szalagkábelekkel kialakítható. Board-to-board típusú csatlakozókkal a modulok egymáshoz történő rögzítése és a villamos csatlakozás egy eszköz segítségével megvalósítható.

A fotovoltaikus modul biztosítja a villamos energia ellátását szigetüzemű működés esetében. Az optimális hatásfok elérése érdekében az akkumulátor töltő modul látja el a napelemes panel impedanciaillesztését. Az akkumulátor töltő modul feladata az akkumulátor szakszerű töltése és kisütése, a túltöltés, mélykisülés, töltőáram, terhelőáram, stb. felügyelete. A tápellátás és az akkumulátor töltése külső feszültségforrásból is ellátható. A DC/DC konverter modul a terhelés számára szükséges stabil egyenfeszültség(ek) előállítását biztosítja.




*6. ábra: Moduláris szigetüzemű tápegység blokkvázlata*

A mérő és vezérlő elektronika felügyeli az egyes modulok működési módjait, valamint monitorozza az állapotukat, eltárolja a mért értékeket. A modulok mérése egyszerűen egy eléjük és mögéjük elhelyezett feszültség és árammérő áramkörrel valósítható meg, ezek alkatrészköltsége minimális. A mért adatokból a modulra vonatkoztatott bemenő és kimenő teljesítmény számolható, ezekből pedig egy a modulra vonatkoztatott hatásfok állapítható meg. A modulok az idő elteltével öregednek, elhasználódnak. A hatásfokromlás, illetve a hatásfok romlás sebessége a tárolt adatokból megállapítható, és egyszerű algoritmussal – jó közelítéssel – előre jelezhető a meghibásodás a felhasználó számára. A felhasználó számára elegendő a megfelelő-cseréle szorul-üzemképtelen típusú visszajelzés.

A mérő és vezérlő elektronika a gyakorlatban egy mikrokontroller és a köré épülő hibrid elemek, a gyakorlatban néhány euro centből megvalósítható. Legtöbb termékben van mikrokontroller, az új funkciók eléréséhez elegendő az eszközt vezérlő firmware bővítése, valamint a passzív elektronika kiegészítés.

A vezérlő modul vezérlési vagy szabályozási feladatait a felhasználó könnyen változtathatná a megengedett határok között. Az eszközhözhöz a felhasználó csatlakozhat vezeték nélkül vagy az eszközön eleve kialakított kezelőfelületet almenüjét is használhatja.

Az eszköz lehetőséget nyújthat a felhasználó számára a teljesítmény-élettartam mérleg beállítására például egy 5 állású mérleg skálán. Az akkumulátor esetében (például egy powerbank esetében), a gyakorlatban ez azt jelenti, hogy ha a felhasználó a teljesítményt választja, akkor az nagyobb töltőáramot (gyorsabb töltést), megváltozott töltési diagramot, magasabb töltőfeszültséget, alacsonyabb mélykisülési feszültséget, nagyobb maximális terhelőáramot jelenthet. Eredményképpen az akkumulátorban nagyobb mennyiségű töltés kerül eltárolásra, valamint az elektrokémiai elemek is nagyobb terhelésnek lesznek

kitéve. A nagyobb teljesítmény ára, az akkumulátor élettartamának csökkenése. Amennyiben az élettartam felé billen a mérleg, az előbb említettekel ellentétes irányú beállítások íródnak be a vezérlőrendszerbe.

**Egy villanymotor vezérlése esetében**

Elektronikus energiaátalakítók (például akkumulátortöltő elektronika, DC/DC konverter, stb.) esetében gyakori meghibásodási pontok a teljesítményfélvezető kapcsolóelemek, nagyfrekvenciával terhelt diódáka, induktivitások, szűrő kondenzátorok. A nagyobb terhelőáram nagyobb terhelést jelent az említett alkatrészekre. A MOSFET-ek csatorna ellenállása (szaturációban) megnövekszik, ez nagyobb hődisszipációt eredményez, ami gyorsítja az alkatrészek öregedését. Az elektrolit kondenzátorok is kiszáradnak a hő hatására, belső ekvivalens ellenállásuk megnövekszik. Az említett hatások a modul hatásfokának a romlásához, illetve megnövekedett energiafelhasználáshoz vezetnek.

Villanymotor vezérlése esetében is van lehetőség a teljesítmény-hatásfok-élettartam értékek súlyozására. Az adott fordulatszámhoz tartozó üzemi áram maximálható, az indítási áram vagy a fordulatszám változásakor fellépő áram csúcsok csökkenthetőek, ha a fordulatszám változásának sebességét vagy a motor által felvehető impulzusszerű áramok értékének maximumát csökkentjük. Eredményképpen a villanymotor hő- és mechanikai terhelése, energiafelvétele csökken. Kommutátoros motor esetében a kommutátor és a szénkefék élettartama növelhető (például mosó- vagy szárítógépben is megtalálható univerzális motorok esetében). A motorvezérlő elektronika szintén tartalmaz félvezető kapcsolóelemeket, melyek élettartama a kisebb terhelések hatására kitolható.

Fűtőelemek vezérlésekor is hasonló gondolatmenet alapján járhatunk el. A fűtőelemek bekapcsolásakor szoftveresen vezérelt vagy hardveresen megvalósított lágyindítással a fűtőelem élettartama nagy mértékben kitolható.

## VILLAMOSENERGIA FELHASZNÁLÁS KÖZPONTOSÍTOTT VEZÉRLÉSE

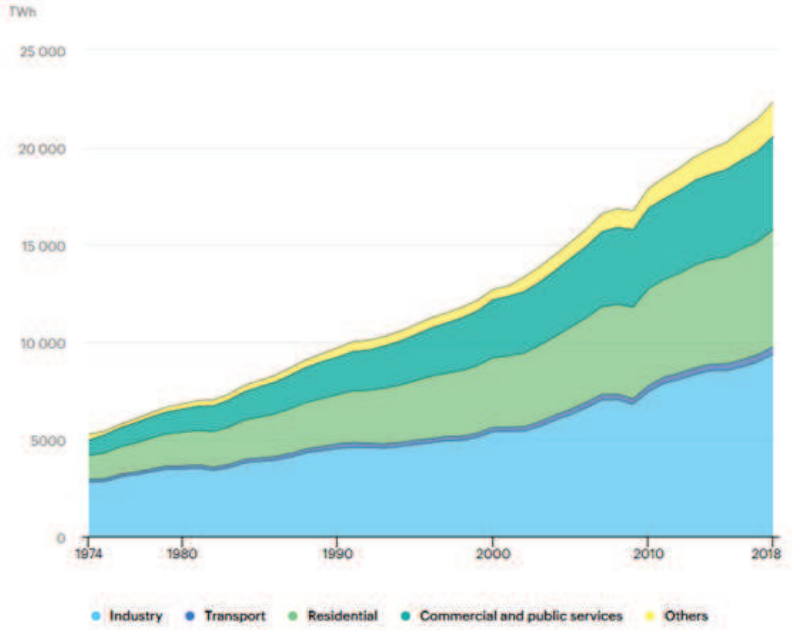
A világ teljes villamosenergia felhasználásának ~30%-a a háztartásokra, ~25%-a a kereskedelmi és közszolgáltatásokra, ~40%-a az ipari szereplőkre vonatkozik. A megújuló energiaforrások költségeinek csökkentése és a digitális technológiák fejlődése hatalmas lehetőségeket nyit meg, miközben új energiabiztonsági dilemmákat hoz létre. A szél- és a napenergiából származó villamos energia biztosítja a 2040-ig terjedő további villamosenergia-termelés több mint felét a megalkotott energiapolitika forgatókönyvében, és a fenntartható fejlődés forgatókönyvének szinte teljes növekedését.

A döntéshozóknak és a szabályozóknak gyorsan kell lépniük, hogy lépést tudjanak tartani a technológiai változások ütemével és az energiarendszerek rugalmas működésének növekvő igényével. Az olyan kérdések, mint például a tárolás piactervezése, az elektromos járművek és a hálózat közötti interfész, valamint az adatvédelem mind új kockázatoknak tehetik ki a fogyasztókat.

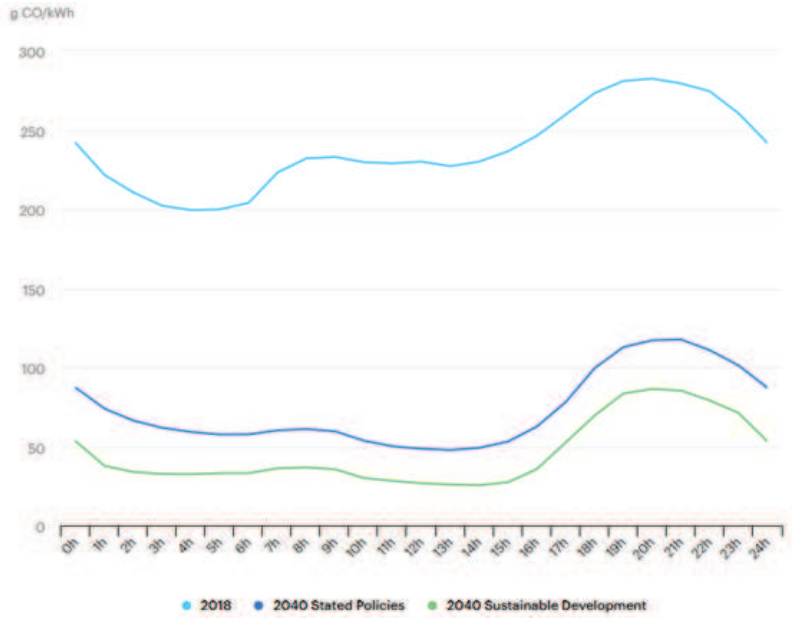
A feladatot tovább nehezíti a 24 órás intervallumon belüli nem egyenletes villamosenergia felhasználás is.

A végfelhasználó készülékek teljesítményfelvételét és dinamikáját – indokolt esetben – az áramszolgáltató is módosíthatná. [8], [9] A kommunikációs csatorna számára jó választás lehet egy vezeték nélküli IoT technológia alkalmazása. [10], [11] A tervezett nagy

arányú megújuló energiaforrások által termelt villamos energia tárolására szolgáló berendezések költségei csökkenthetőek lennének ezzel a megoldással. A szükséges terméket terhelő extra költséget jelentő hardver és mérnökóra sokszorosa térülhetne meg, ami globális szinten jelentős erőforrások megjelenését eredményezné




*7. ábra: A világ villamosenergia-fogyasztás ágazatonként, 1974–2018 [6]*




*8. ábra: A 24 órás villamosenergia-ellátás átlagos CO2-kibocsátásának intenzitása az Európai Unióban, 2018 és 2040 közötti időszakban [7]*

## ÖSSZEFOGLALÁS

Tanulmányom legfontosabb eredményének azt tartom, hogy a bemutatott kutatás alapján a műszaki oktatásból hamarosan kikerülő, műszaki munkakörben munkát vállaló, várhatóan ~45 aktív munkaévre készülő generáció határozottan fontosnak tartja és ésszerű felár mellett igényli is a háztartási és ipari berendezéses teljesítmény-hatásfok-élettartam arányok végfelhasználó általi beállíthatóságának lehetőségét.

A szerző meggyőződése, hogy a műszaki berendezések kiegészítése a vázolt rendszerelemmel, releváns piaci, gazdasági és környezeti hatással rendelkezik.

## KÖSZÖNETNYILVÁNÍTÁS

A „Végfelhasználói Igények Megjelenése az Energiafelhasználás Hatékonyságának és a Termék Megbízhatóságának Növelése Érdekében" című dokumentum az Innovációs és Technológiai Minisztérium UNKP-19-3 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült. A szerző kijelenti, hogy a Mű a saját egyéni, eredeti alkotása, annak egyedüli szerzője és alkotója.

## FELHASZNÁLT FORRÁSOK

[1] IEA (2019), „*World Energy Outlook 2019"*, IEA, Paris https://www.iea.org/reports/world-energy-outlook-2019 (letöltve: 2020.08.05.)

[2] IEA (2019), „*Energy Efficiency 2019"*, IEA, Paris https://www.iea.org/reports/energy-efficiency-2019 (letöltve: 2020.08.05.)

[3] IEA (2020), „*Global Energy Review 2019"*, IEA, Paris https://www.iea.org/reports/global-energy-review-2019 (letöltve: 2020.08.05.)

[4] IEA (2020), „*Energy Efficiency Indicators 2020"*, IEA, Paris https://www.iea.org/reports/energy-efficiency-indicators-2020 (letöltve: 2020.08.05.)

[5] IEA, „*Global improvements in primary energy intensity, 2000-2018"*, IEA, Paris https://www.iea.org/data-and-statistics/charts/global-improvements-in-primary-energy-intensity-2000-2018 (letöltve: 2020.08.05.)

[6] IEA, „*World electricity final consumption by sector, 1974-2018*", IEA, Paris https://www.iea.org/data-and-statistics/charts/world-electricity-final-consumption-by-sector-1974-2018 (letöltve: 2020.08.05.)

[7] IEA, „*Average CO2 emissions intensity of hourly electricity supply in the European Union, 2018, and by scenario, 2040"*, IEA, Paris https://www.iea.org/data-and-statistics/charts/average-co2-emissions-intensity-of-hourly-electricity-supply-in-the-european-union-2018-and-by-scenario-2040 (letöltve: 2020.08.05.)

[8] A. Szűts, „*Developing a Complex Decision-Making Framework for Evaluating the Energy-Efficiency of Residential Property Investments"*. ACTA POLYTECHNICA HUNGARICA 12 : 6 pp. 231-248. , 18 p. (2015)

[9] I. Czibere, I. Kovách, G. B. Megyesi. „*Environmental Citizenship and Energy Efficiency in Four European Countries (Italy, The Netherlands, Switzerland and Hungary)"*. SUSTAINABILITY 12 : 3 Paper: 1154 , 18 p. (2020)

[10] A. Szűts, I. Krómer: „*Estimating Hungarian Household Energy Consumption Using Artificial Neural Networks*", Acta Polytechnica Hungarica, Vol. 11, No. 4,pp. 155-168,2014

[11] A. Szűts, I. Krómer: „*Developing a Fuzzy Analytic Hierarchy Process for Choosing the Energetically Optimal Solution at the Early Design Phase of a Building"*, Acta Polytechnica Hungarica, Vol. 12, No. 3, pp. 25-39, 2015

# SECURITY OF SUPPLY FOR SECURITY | ELLÁTÁSBIZTONSÁG A BIZTONSÁGÉRT

MOLNÁR, Ferenc[1]

**Abstract**

We use the term energy in almost every area of our lives. Energy serves our lives in innumerable forms. Today, almost half of the energy used globally makes the lives of people living in cities more comfortable. This comfort also means a complete dependence on energy for civilization. Today, we live in an energy-based society, the development of which is ensured by an energy-based economy. Without usable energy, both would collapse. Heating, cooling, ventilation, all production would stop. Devices that require electricity would become unusable. Traffic would stop and all technical achievements would become inoperable. In the absence of electricity, law enforcement and national defense would also collapse. The groups of security science can be interpreted only in the case of the availability of electricity, such as security informatics, communication, cybernetics, operations research as well as the entire vertical of defense technologies.

**Keywords**

energy, sustainable development, energy supply, security of supply

**Absztrakt**

Az energia kifejezést életünk szinte minden területén használjuk. Az energia megszámlálhatatlan formájában szolgálja az életünket. Napjainkban a globálisan felhasznált energiamennyiség csaknem fele a városokban lakó emberek életét teszi kényelmesebbé. Ez a kényelem egyben az energiától való teljes függőséget is jelenti a civilizáció részére. Manapság energia alapú társadalomban élünk, amelynek fejlődését a szintén energia alapú gazdaság biztosítja. Felhasználható energia hiányában mindkettő összeomlana. Leállna a fűtés, hűtés, szellőztetés, minden termelés. Használhatatlanná válnának a villamos energiát igénylő eszközök. Megállna a közlekedés és minden technikai vívmány működésképtelenné válna. A villamos energia hiányában a rendvédelem és nemzetvédelem is összeomlana. A biztonságtechnikai tudomány csoportjai csak a villamosenergia rendelkezésre állása esetén értelmezhetőek, mint a biztonsági informatika, kommunikáció, kibernetika, operációkutatás csakúgy, mint a védelmi technológiák teljes vertikuma.

**Kulcsszavak**

energia, fenntartható fejlődés, energiaellátás, ellátásbiztonság

[1] molnar.ferenc@phd.uni-obuda.hu | ORCID: 0000-0002-0008-0544 | head of sustainable energy generation team/fenntartható termelési csoportvezető | MVM Magyar Villamos Művek Zrt.

## BEVEZETÉS

Az energia kifejezést életünk szinte minden területén használjuk, az energia megszámlálhatatlan formájában szolgálja a mindennapjainkat. Az energiát a tudomány különféle ágazatai is másképpen írják le a saját szempontrendszerük szerint. Az emberiség fejlődésének meghatározó mozgatórugója az energia felhasználásának minősége, mennyisége és folyamatosan gyarapodó számú hozzáférési formája. Napjainkban a globálisan felhasznált energiamennyiség csaknem fele a városokban lakó emberek életét teszi kényelmessebbé. Ez a kényelem egyben az energiától való teljes függőséget is jelenti a civilizáció részére. Manapság energia alapú társadalomban élünk, amelynek fejlődését a szintén energia alapú gazdaság biztosítja. Felhasználható energia hiányában mindkettő összeomlana. Megszűnne a fűtés, hűtés, szellőztetés, víz-, gázellátás, leállna minden termelés, használhatatlanná válnának a villamos energiát igénylő eszközök, megállna a közlekedés és minden technikai vívmány működésképtelenné válna. A villamos energia hiányában a rendvédelem és nemzetvédelem eszközrendszere is összeomlana. A biztonságtechnikai tudomány csoportjai csak a villamosenergia rendelkezésre állása esetén értelmezhetőek, mint a biztonsági informatika, kommunikáció, kibernetika, operációkutatás csakúgy, mint a védelmi és elhárítási technológiák teljes vertikuma. Itt említhetjük akár a social engineering technikákat [1] vagy a biometrikus azonosítási technológiákat [2] példaként. Az energia felhasználható formáiban történő rendelkezésre állása az emberi közösségek és az egyes emberek biztonságát is meghatározza. A biztonságot, mint állapotot a biztonságtudomány létező egészségnek nevezi. Ez az egészség fogalom az emberi test és a társadalom tökéletes állapotát fejezi ki. A biztonságtudomány az objektív valóságot kettős módon közelíti meg. Egyik vizsgálati irány a technológia hasznossága az egyéni és társadalmi fejlődés szempontjából. A másik megközelítési iránya ugyanennek a technológiának a negatív hatása az egyének egészségére és a környezet terhelésére. Ezzel összefüggésben kell megemlíteni a munkavégzés biztonságát is, amely a technológiai fejlődést követve kell, hogy kielégítse a folyamatosan változó követelményeket. A jelenkori energiafelhasználás mértékének egyik negatív hatása a Föld készleteinek mérhetetlen kizsákmányolása és a globális felmelegedés felgyorsulása. A globális felmelegedés ciklusok végig kísérik a Földtörténetet, azonban a több évmilliós ciklust az emberi tevékenységek következménye ezt néhány száz évre rövidítette le. Ilyen például az üvegház hatást növelő gázok légkörbe történő fokozott kibocsátása. A Föld légkörének jelenlegi klímáját az üvegházhatás biztosítja. A Földet az üvegházhatást okozó gázok üvegbúraként veszik körbe. A jelenség az üvegház jelenségről kapta a nevét. A nap sugárzása áthatol az üvegen, felmelegíti a földfelszínt és a keletkező hő egy részét az üvegfalak, vagyis az üvegbúra magába zárja. Ez a jelenség biztosította a jelenlegi földi élet kialakulásához szükséges klimatikus viszonyokat és annak fennmaradásához is szükséges. Az ipari forradalom óta az emberi tevékenység hatására folyamatosan emelkedő mértékben egyre nagyobb mennyiségű a légtérbe juttatott üvegház hatású gáz. Ennek következtében egyre vastagabb a felhalmozódott üvegházhatású gázréteg, tehát folyamatosan erősödik az üvegházhatás, amelynek eredménye, hogy csökken a légkörből kijutó hőmennyiség. A légkör felmelegedésének erősödéséhez nagyban hozzájárul az odajutatott hőmennyiség mértékének fokozódása is. A környezetbe jutó többlet hőmennyiség az általunk felhasznált energiák veszteségi hányadából származik. A legnagyobb veszteségi hőmennyiség és egyben üvegházhatású gáz kibocsátó szektorok az energia előállítás, a közlekedés-szállítás, az ipar és az épületek. Ezek egy része a mindennapi életünk biztonságát is szolgálja. A szektorok egyre

emelkedő energia felhasználását az egyes ember növekvő fogyasztása, a mára csaknem 8 milliárdnyi populáció folyamatos gyarapodása, valamint az elavult technológiák alkalmazása okozza. A tét nem kisebb, mint az emberiség túlélése, amely csak az élhető bolygónk megőrzésével lehetséges.

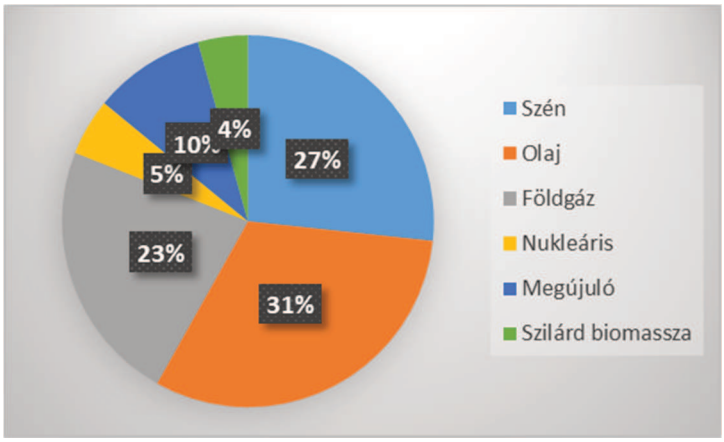
Az IPCC 2014-es adatai szerint üvegházhatást okozó gázok 76%-át a széndioxid teszi ki, amely az égési folyamatok következményeként termelődik [3]. Az IEA (International Energy Agency) által 2018-ban kiadott Word Energy Outlok (WEO) alapján, 2017-ben a karbon emisszió közel 42%-át az energiatermelés, csaknem 25%-át a közlekedés-szállítás és 19%-át az ipari termelés okozta [4]. A globális fejlődés akkor válhat fenntarthatóvá, ha a folyamatosan növekvő energiaigényt drasztikusan csökkenő emisszió mellett tudjuk biztosítani, azaz meg tudjuk valósítani a tiszta energiák térnyerését az energiatermelési és felhasználási szerkezet összetételében. Az egyik kézenfekvő megoldási irány lehet az elektrifikáció valamint a digitalizáció kiterjesztése a közlekedési, az épületek és az ipari szektoron belül úgy, hogy ezzel egyidőben a növekvő villamosenergia-szükségletet karbonsemleges források alkalmazásával kell kielégíteni. A villamosenergia-termelésben meghatározó szerep jut a nukleáris bázisú technológiáknak az ellátásbiztonság, a széndioxid kibocsátás csökkentése és a klímavédelem érdekében.

## GLOBÁLIS VILLAMOSENERGIA-FELHASZNÁLÁS ÉS TERMELÉS

### Globális kitekintés

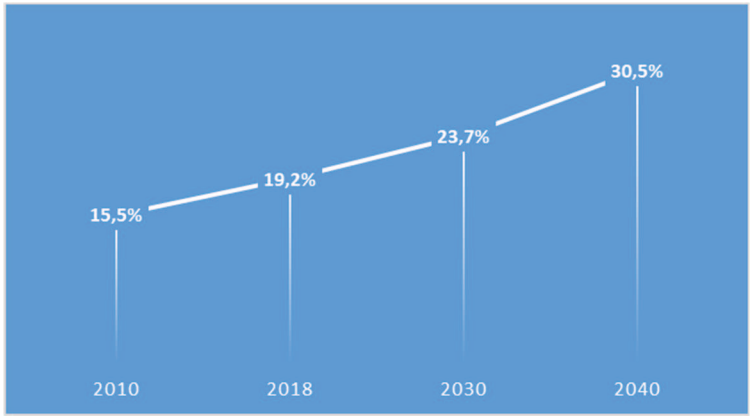
Az energiaátmenet kiemelt szerkezeti eleme a villamosenergia használata lesz. A fenntartható fejlődésben az ellátásbiztonságban és az emisszió csökkentés lehetőségeiben már jelenleg is központi szerepet foglal el és a jelentősége folyamatosan erősödő tendenciát mutat az előrejelzések szerint. A villamosenergia felhasználása teszi lehetővé a digitalizáció széleskörű használatát így a gazdaság minden szegmensében az automatizálás biztosította lehetőségek előnyé alakítását. Elsődleges szempont, hogy az előállított villamosenergia milyen primer forrásból származik. A növekvő villamosenergia-igény kielégítését a termelői oldalon a fenntartható fejlődést szem előtt tartva, tehát a karbon lábnyom folyamatos csökkentése mellett kell biztosítani. A karbonkibocsátás-mentesen üzemelő erőművek a megújuló és a nukleáris bázisú energiatermelő technológiák közül kerülhetnek ki. A nukleáris energia békés célú felhasználásának legnagyobb területe az energetika. Az atomreaktorok több mint fél évszázada megbízhatóan és nagy mennyiségben előállított tiszta energiával szolgálják a társadalmi és a gazdasági fejlődést. Érdemes áttekinteni, hogy milyen helyzetből indulunk az előttünk álló energiaátmenet kihívásainak megoldásához vezető úton.

A globális energia igény-növekedés folyamatában a 2010. óta eltelt időszakot vizsgálva a 2018. év produkálta a legnagyobb mértékű fogyasztásnövekedést ezzel elérve a 14314 Mtoe (Megatonna olaj-egyenérték) értéket. A 2018-as bővülés mértéke 2,3% volt, amelynek 70%-áért az USA, Kína és India együttesen voltak felelősek. Annak ellenére, hogy 2010. óta a primer energiaforrások közül a legnagyobb növekedést a megújuló források érték el a felhasználás több mint 80%-át 2018-ban még mindig a fosszilis forrásokból nyertük [5].



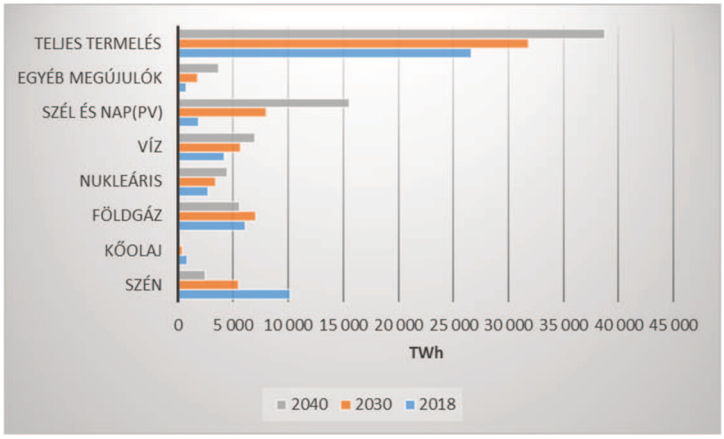

*1. ábra: A globális primer energia felhasználás arányai 2018-ban (saját szerkesztés WEO 2019 alapján).*

A szakpolitikai előrejelzések azt mutatják, hogy az előttünk álló 2040-ig tartó időszak éves energia-igény növekedése valamivel 1% felett fog alakulni ellentétben a 2000. óta tartó évi 2% emelkedési tendenciával. A gazdasági fejlődés várhatóan továbbra is erős marad azonban az energiahatékonyság előtérbe kerülésével a klímavédelem mellett az energiaigény kiszolgálása is biztonságosabbá válik. Az energiaellátó rendszerek fenntartható fejlesztése szempontjából nagy kihívást jelent a fejlődő országok városainak évi 70 milliónyi lakossal való bővülése. A fejlődő országok minden számukra könnyen elérhető primer forrást felhasználható energiává alakítanak. A fenntartható fejlődés érdekében az energetikán kívüli másik legnagyobb fosszilis forrásokat felhasználó szektor energiaátmenetét is érdemes áttekinteni. A szakpolitika előrejelzése szerint az olajfogyasztás üteme 2025. után jelentősen vissza fog esni, annak ellenére, hogy a személygépkocsik száma várhatóan 2018. és 2040. között további 70 %-kal fog emelkedni. Még inkább figyelemre méltóak az előző számok, ha azt is hozzávesszük, hogy az olajfogyasztás globális csúcspontja 2020. év végére várható. A fenntartható fejlődés energiaátmenete csak akkor lehet sikeres, ha a növekvő energiakereslet mellett is háttérbe tudjuk szorítani a fosszilis bázisú primer forrásokat a villamosenergia-felhasználás kiterjesztésével. A kőolaj felhasználása a közlekedésben a növekvő járműszám ellenére is 40%-kal kell, hogy csökkenjen 2040-re a 2018-as értékekhez mérten. A fenntartható fejlődésben a villamosenergia növekvő részarányát szemlélteti a következő diagram a teljes energiaigényhez viszonyítva. [5]




*2. ábra: A fenntartható fejlődésben a villamosenergia részaránya a végső fogyasztáshoz képest %-ban megadva. (saját szerkesztés WEO 2019 alapján).*

A villamosenergia szerepét a dekarbonizációs célok teljesítésében jól érzékelteti, hogy a végső felhasználáshoz viszonyítva a jelenlegi 19 %-os részesedése több mint 30 %-os értékre fog növekedni. A gazdaságilag fejlett országok jórészt ennek betudhatóan lesznek képesek folyamatosan csökkenteni a végső energiaigényük mértékét az energiaintenzitásuk folyamatos javításával. A fenntarthatóság érdekében átlagosan évi 3,6 %-kal kell csökkennie a teljes energiafelhasználásnak 2040-ig. Önmagában a növekvő villamosenergia részarány még nem oldja meg a klímavédelemmel kapcsolatos feladatokat. Azt is el kell érni, hogy a villamosenergia előállítása tiszta azaz karbonmentes forrásból valósuljon meg. Vizsgáljuk meg, hogy a villamosenergia előállítás szerkezeti összetétele milyen képet festett 2018-ban és a fenntarthatóság érdekében milyen arányban kellene a primer energiaforrásoknak részt vennie az energiamixben 2040-ben




*3. ábra: A fenntartható fejlődésben a villamosenergia-termelés primer forrásainak részesedése a teljes előállításon belül TWh-ban megadva. (saját szerkesztés WEO 2019 alapján).*

A grafikon egyik érdekessége, hogy az új megújuló források, azaz a szél és a nap erőteljes térnyerése mellett a kőolaj és a szén energetikai felhasználása folyamatosan és

drasztikusan csökken addig a földgáz szerepe 2030-ig még hangsúlyozottabbá válik. Felvetődhet a kérdés vajon mi indokolhatja ezt a látszólagos ellentmondást? A kérdés megválaszolásához érdemes az új megújulók, vagyis az időjárásfüggő termelők térhódításának a járulékos hatásait elemezni. A villamos hálózat stabilitását az együtt járó rendszerek egyensúlya biztosítja. A fogyasztói igényeknek és a megtermelt villamos energiának mindig egyensúlyban kell lennie. A fogyasztói igények folyamatos változását kismértékben a forgógépes erőművek nyomatéka nagyobb mértékben a rugalmassági kapacitások kompenzálják. A rugalmassági, vagyis szabályzó kapacitások az alap és a menetrendtartó erőművek által megtermelt villamos energia és a fogyasztói igények közötti rést hivatottak kitölteni. Szerencsés földrajzi adottságú országokban a duzzasztós vízerőművek kiváló karbonsemleges szabályozó források lehetnek. A duzzasztós erőművek folyókra épülnek és a gátrendszerük alkalmas arra, hogy a folyó vizének irányított visszatartásával szabályozottan engedjék át a vizet a turbinákon. A szabályozott villamosenergia termelésen túl a folyó hajózhatóságára is hasznos építmény. Ennek hiányában azonban a terhelési és termelési görbe közötti különbséget nagyon gyakran gázturbinákkal és gázmotorokkal tudják kiszabályozni. Az időjárás függvényében termelő megújuló bázisú erőművek hektikus termelésének és az elektrifikáció következtében egyre változatosabb formában felhasznált villamosenergia-igény változásának eredményeként minden eddiginél jóval nagyobb szükség lesz a különbség kiegyenlítésére. Amíg a korszerű energiatárolók fejlesztése és elterjedése nem hoz átütő eredményt addig a gázturbinák szerepe a hálózati paraméterek megőrzésében megkerülhetetlen. Kedvező természeti adottságú országok a villamosenergia rendszerük terheléskiegyenlítési és hálózatszabályozási feladataikat szivattyús-tározós erőművekkel is megoldhatják. Ebben az esetben egy tóból vagy folyóból a vizet a termelési időszakok többlet, olcsó energiájával felszivattyúzzák egy magasan mesterségesen kialakított tározóba. A tározóban felhalmozott vízmennyiséget a villamosenergia rendszer szabályozási igényei alapján engedik le a vízturbinákon keresztül, amelyek a villamos hálózatra termelnek. Ezek a leszabályozási feladatokban is hatékonyan részt vehetnek.

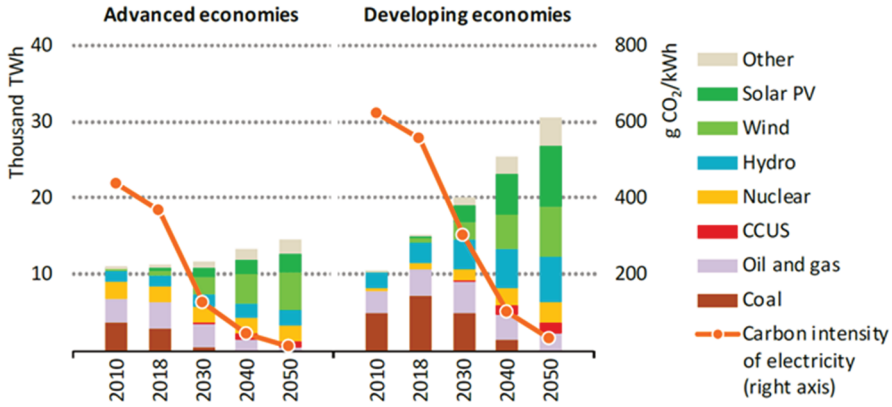
**A nukleáris bázisú tiszta energia**

A tiszta energia előállítás stabil és meghatározó eleme a nukleáris bázisú termelés. Az atomenergia energetikai hasznosítása a világ első atomreaktorában megvalósított szabályozott láncreakció beindításával kezdődött 1942. december 2-án. Az atomkort elindító első reaktort, amelyet atommáglyának neveztek el a Chicagói Egyetem stadionjának lelátója alatti teremben Fermi vezetésével épült meg, amelynek terveit többek között Szilárd Leó valamint Wigner Jenő készítette. Az ezt követő években a fegyverkezési verseny mellett az atomenergia békés célú felhasználása is forradalmi változáson ment keresztül. Az USA-ban, Idahoban 1951-ben már 200 kW villamos teljesítmény leadására képes reaktort keltettek életre. A világ első hálózatra termelő reaktora az Obnyinszki Atomerőműben létesült 1954-ben, 5 MW kapocsteljesítménnyel. Kereskedelmi céllal épült atomerőművet először 1957-ben Pittsburgh város villamosenergia-ellátása céljából létesítettek 3 év leforgása alatt. A 60 MW villamos teljesítmény kiadására készült nyomottvizes reaktor a haditengerészet anyahajó erőforrás szerepkörből polgáriasult közcélú villamos termelővé. [6]

A kezdetektől a mába ívelő fejlődést a Nemzetközi Atomenergia-ügynökség által közzétett legfrissebb mennyiségi adatok jellemzik a legjobban. A világon jelenleg 441 ener-

getikai célú nukleáris reaktor üzemel összesen 390 113 MW beépített nettó villamos teljesítménnyel. A nukleáris kapacitás fenntartás és bővítés érdekében 54 reaktor épül világszerte összesen 57 441 MW tervezett nettó villamos teljesítőképességgel. Az atomerőművek jelentőségét igazolja a 18 505 összes reaktor év, amely az eddigi szolgálatuk eredménye. [7]

A klímavédelmi intézkedések közül a legfontosabbak közé tartozó széndioxid kibocsátás csökkentéséhez az atomenergia felhasználása nagymértékben hozzájárul. A szakpolitika prognózisa szerint a jelenlegi trendet alapul véve 2040-re a nap és a szél források termelése már dominálni fog a villamosenergia-termelésen belül és 2050-re már a teljes globális áramtermelés felét fogják adni. A vízenergia 17%-os részesedése mellett a nukleáris termelés 10%-os súllyal tartja meg nélkülözhetetlen szerepét az ellátásbiztonságban. A fenntartható fejlődéshez áttörésre van szükség bioenergiák hasznosításában is. Ezek hasznosítása a remélt 7%-os részesedést fogja elérni. A CCUS (Carbon Capture, Utilization, and Storage) új alkalmazott technológiaként teheti lehetővé 5%-nyi saját réssel a szén és földgáz tiszta energiaként történő felhasználását. A CCUS technológia egyelőre fejlesztési fázisban van, még nem piacképes. A CO2 kivonás nélküli széntüzelést alkalmazó energiaátalakítási technológiák a fejlett gazdaságokban 2030-ig, a fejlődő gazdaságokból 2045-ig valószínűleg kivonásra fognak kerülni a termelési szerkezetből. A villamosenergia-ellátó rendszerek rugalmasságát a 2020-as évek végéig még a földgáz elégetésének fokozódása mellett lehet biztosítani. Ezt követően azonban az energiatároló technológiák előtérbe kerülése lesz jellemző így a gázturbinák átadhatják a helyüket a Storage szegmensnek. A következő ábrán azt követhetjük végig, hogy 2050-ig milyen energiaátmenetet kell megvalósítania a fejlett és fejlődő gazdaságoknak a fenntartható jövő érdekében. [5]

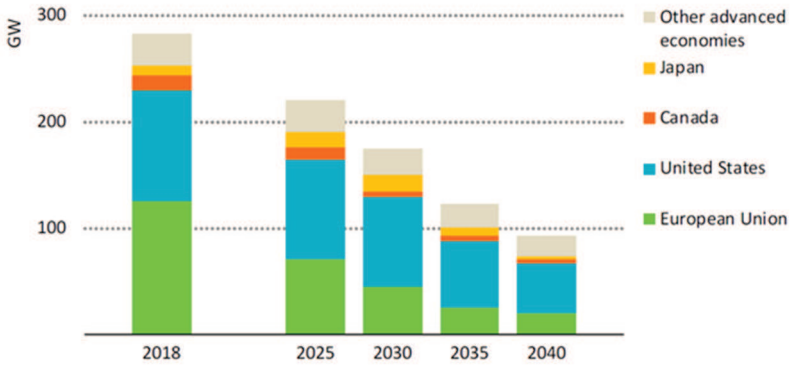



*4. ábra: A fejlett és fejlődő gazdaságok trendje a zéró karbon kibocsátás felé a villamosenergia-termelésben [5].*

Ahhoz, hogy 2050-re a villamosenergia-termelés karbon intenzitása 23g CO2/kWh értékre csökkenjen a 2018-as 475 g CO2/kWh értékről a következő energiaátmenet megvalósulását kellene elérni. A Föld teljes lakossága rendelkezni fog a villamosenergia-felhasználás lehetőségével. Ennek kiegészítéseként a közlekedés-szállítás, más ágazatokkal együtt villamos energiafelhasználásra fog áttérni a jelenlegi egyéb más energiaforrásokról. A globális energiafelhasználáson belül a 2018-ban rögzített 19%-os villamosenergia-részarány

2050-re közel meg kell, hogy kétszereződjön. Ezzel a növekedéssel a villamosenergia-fogyasztás a 2018-ban felhasznált mennyiségéhez képest, 2050-re 70%-kal lesz magasabb, amely több mint 45 000 TWh értéket fog jelenteni. A villamosenergia-termelés forrásszerkezete teljesen át fog rendeződni az alacsony emissziót biztosító energia mix irányába. A karbonmentes források 2018. évi 36%-os aránya a 2030-ra prognosztizált 60% körüli értéken keresztül el kell, hogy érje a 94%-os részesedést. [5]

A villamosenergia-igény ellátásához biztosítani kell a termelő kapacitásokat. Ehhez a meglevő kapacitások fenntartása és a növekedési trend követése szükséges az előállító oldalon. Az atomenergia felhasználása kiemelt jelentőségű az energiaátmenetben, ezért fontos áttekintenünk a helyzetét. A fejlett országok karbonmentes termelői közül jelenleg a legnagyobb volument képviseli, amely 18%-os részesedést jelent a teljes előállított villamosenergia-mennyiséghez képest ezen országokat együtt véve. A klímavédelem szempontjából a nagy fejlődési ívet felmutató megújuló források és az innováció erőteljes szakaszában levő CCUS technológiák mellett a nukleáris energia szerepe megkérdőjelezhetetlen a tiszta energiaátmenetben. A szabályozott láncreakció hasadási energiájának átalakítása alaperőművekben történik, ezért az ellátásbiztonság szempontjából is meghatározó a szerepük. Alaperőműként az állandó fogyasztói tartomány folyamatos megtermelése mellett a turbógenerátorok nyomatéka is hozzájárul a hálózat stabilitásához. A fejlett gazdaságok döntéshozatali bizonytalansága következtében nehéz helyzetbe került az ágazat. Az üzemelő atomerőművek átlagéletkora 35 év. Az üzemidő hosszabbításoknak köszönhetően még hosszú időre versenyképes tiszta energiaforrásként lehet rájuk számítani. A gazdaságosságukra jellemző adat, hogy a retrofiton átesett létesítmények előre becsülhetően 40÷60 USD/MWh közötti fajlagos áron tudnak majd nagy mennyiségben karbonmentes áramot termelni. Az üzemidő hosszabbításra más országokhoz hasonlóan hazánkban is jó példa az MVM Paksi Atomerőmű folyamatos korszerűsítése. A meghosszabbított üzemidővel termelő erőművek még a csökkenő költség trendet felmutató megújuló technológiákkal szemben is piacképes alternatívát kínálnak.



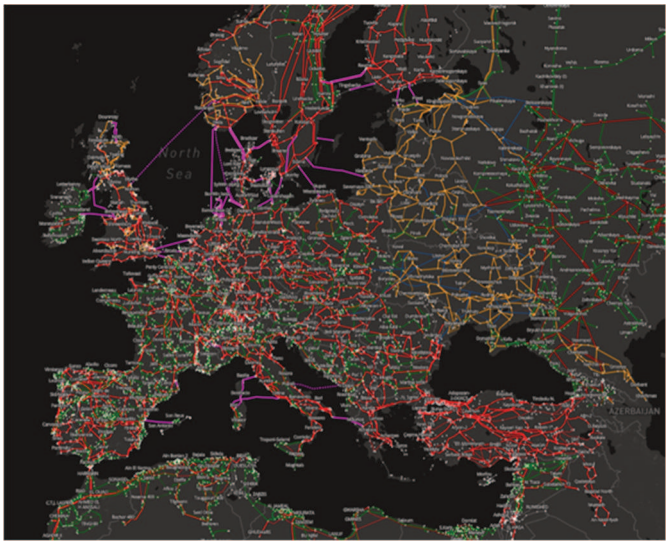

*5. ábra: A jelenleg üzemelő atomenergia kapacitások jövője a fejlett gazdaságokban további beruházások nélkül. [5].*

Amennyiben nem történnek üzemidő hosszabbítások és nem indulnak új beruházások a fejlett gazdaságokban, abban az esetben 2040-re a beépített atomerőmű összteljesítmény az egyharmadára fog csökkeni a 2018-as állapothoz képest. Ez a klímavédelemre és

a villamosenergia árakra is erősen negatív hatást gyakorolna. A helyzetet nehezítik a nap, mint nap tapasztalt negatív kampányok, a költség és a határidő túllépésekre hivatkozó propaganda. A fejlesztés alatt álló kisméretű moduláris reaktorok piaci megjelenése hozhat széleskörű pozitív fogadtatást és új lendületet a nukleáris kapacitásokat bővítő beruházásoknak. A kieső, illetve elmaradó nukleáris kapacitások esetén az egyébként sem könnyű fenntartható fejlődéshez szükséges emisszió csökkentési célok eléréshez jóval nagyobb erőfeszítések kellenének. A rendszerből ílymódon hiányzó atomerőművek helyettesítése megújuló forrásokkal becsülhetően legalább1,6 trillió USD többlet beruházási költséget jelentene a 2040-ig elemzett időszakban. [5]

**Hazai energiafelhasználás és -termelés**

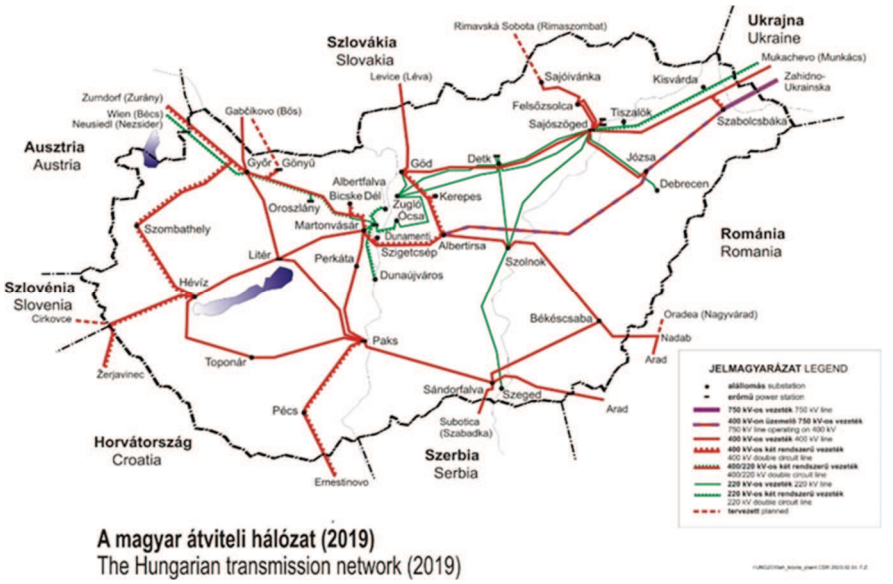
Magyarország az ENTSO-E tagja. ENTSO-E a European Network of Transmission System Operators for Electricity rövidítése, vagyis a villamosenergia-átviteli rendszerüzemeltetők európai hálózata. Az ENTSO-E koordinálja a 35 ország 42 villamosenergia-átviteli rendszerüzemeltetőjének (TSO: Transmission System Operators) határokon átnyúló rendszerüzemeltetését, rendszerfejlesztését és villamosenergia-piaci tevékenységeit. Az ENTSO-E felhatalmazást kapott az EU belső energiapiacra vonatkozó gáz- és villamosenergia-piac további liberalizálására. A tevékenysége magába foglalja az egész Európára kiterjedő tíz éves időszakra vonatkozó villamosenergia-hálózat fejlesztési tervek, az átláthatósági platformok, a hálózati kódexek, az iránymutatások és az egész Európára kiterjedő módszerek kidolgozását. Az ENTSO-E Brüsszelben található központja kielemelt figyelmet fordít az együtt járó rendszer műszaki, kereskedelmi és politikai kérdések összehangolt kezelésére, az Európai Bizottsággal, a szabályozó hatóságokkal, szakmai egyesületekkel és az érdekképviseletek megteremtésére. Az ENTSO-E tagság együttműködésének eredménye az ellátásbiztonság fenntartása a világ legnagyobb és legversenyképesebb villamosenergia rendszerében, valamint az új kihívások eredményes megoldása, mint amilyen a megújuló bázisú erőművek rendszerintegrációja.




*6. ábra: ENTSO-E átviteli rendszer térképe. [8]*

ENTSO-E átviteli rendszer térképen a 220 kV-os és annál magasabb feszültségszintű távvezeték nyomvonalak, valamint a 100 MW-nál nagyobb teljesítményű erőművek láthatóak.

Magyarország villamosenergia rendszerének (VER) termelői szektorát a MAVIR (Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt.) minden évben felülvizsgálja. Ennek egyik viszonyítási pontját az ENTSO-E által 2018. évben kiadott 10 éves hálózatfejlesztési terve képezi. Az évenkénti elemzések célja a hazai erőművek életkorának és műszaki jellemzőinek figyelembe vételével áttekintést adni a termelői oldal helyzetéről és az ezzel kapcsolatos eseményekről, amelyek az erőművek leállítását vagy éppen a beruházások alakulását is tartalmazzák.

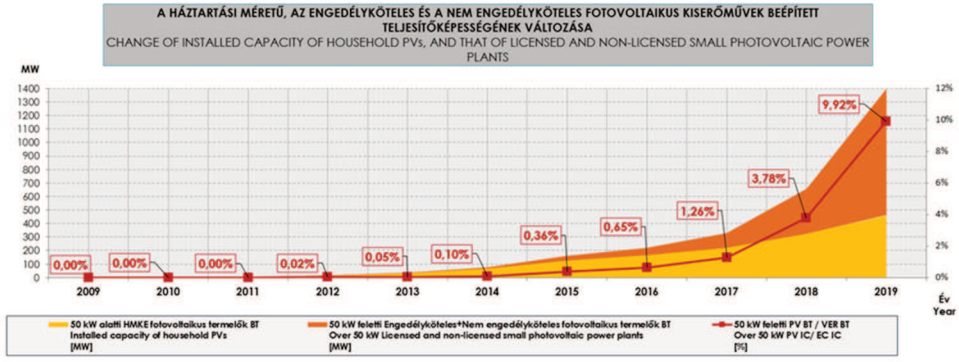



*7. ábra: A magyar átviteli hálózat térképe. [9]*

A Magyar Villamos Energia Rendszer (VER) felépítése funkcionális és feszültségszint szerinti hierarchikus szintekre tagolódik. A villamos hálózat rendeltetése, hogy az erőművekben előállított villamos energiát összegyűjtse és eljuttassa a felhasználókig. Az erőművek rendeltetésük szerint lehetnek alaperőművek, menetrendtartó és csúcserőművek. Az MVM Paksi Atomerőmű 2000MW beépített és a nukleáris kapacitás fenntartására előkészített Paks II. Atomerőmű Zrt, 3+ generációs, AES 1200 típusú létesülő 5. és 6. helyszámú blokkjai 2400 MW tervezett teljesítménnyel tipikus alaperőművi termelők. Alaperőmű a lignit tüzelésű Mátrai Erőmű is. A primer energaforrások átalakítását szolgáló technológia szerint is különbséget tehetünk, nukleáris, fosszilis bázisú, megújuló alapú energiatermelő technológiák között. A villamos hálózat legmagasabb hierarchikus szintje az alaphálózat, amely 220 kV, 400 kV és 750 kV-ra szigetelt rendszerek együttese. Rendszerszintű feladata a nagy mennyiségű energiák gazdaságos szállítása. Ezeken a feszültségszinteken történik a határkeresztező kapacitások által biztosított nemzetközi kooperáció, valamint az alaperőművek és a jellemzően 100 MW feletti termelő létesítmények betáplálási pontjait biztosítja.

A VER 34 alaphálózati transzformátor állomásán keresztül jut el a villamosenergia legnagyobb hányada az elosztóhálózatba, amely 132 kV, 35 kV, 22 kV, 10 kV feszültségszinten látja el a nagy ipari üzemeket és a fogyasztói körzeteket. Erre a feszültségszintre csatlakozhatnak a 100 MW alatti beépített teljesítménnyel rendelkező ipari méretű erőművek. Az ipari üzemek belső hálózatai a 10 kV, 6 kV és 3 kV középfeszültségen üzemelnek. A lakossági fogyasztók részére kisfeszültségen, vagyis 0,4 kV-on juttatják el a villamos energiát a Hálózati Engedélyesek vagyis az áramszolgáltatók.

A napelemes erőművek terjedésének egyik jelentős iránya a kiserőmű és a háztartási méretekben történő létesítés. 2020. év első felében már a közel 1500 MWp teljes mennyiségből, összességében csaknem 500 MWp fotovoltaikus napelem kapacitás üzemelt lakossági tulajdonban. [10]

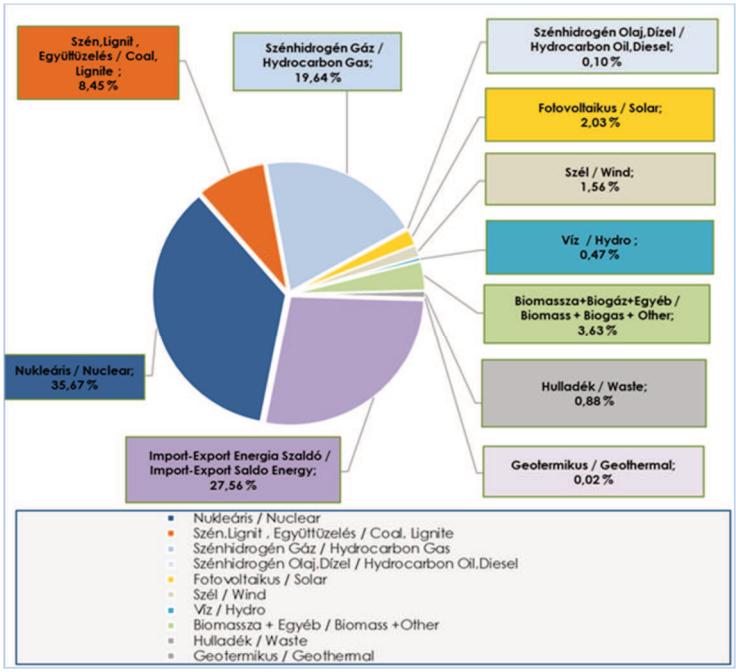



*8. ábra: A hazai napelemes beépített teljesítmények változása 2009 és 2019 között. [10]*

A korábban centralizáltan termelő forrásokhoz igazított hálózati struktúra, folyamatos és teljes átalakuláson megy keresztül. Korábban az energiaáramlás jól tervezhető módon a nagyerőművektől áramlott az ipari és a lakossági fogyasztók felé. Napjainkban a decentralizáltan termelő kis és háztartási erőművek előre nehezen prognosztizálható menetrend szerint már kis és középfeszültségről táplálnak a hálózatba, gyakran megfordítva ezzel az energia áramlások irányát. A decentralizált termelés jelentős hálózatfejlesztési igényeket vonz maga után, valamint teljesen újra kell tervezni és átalakítani a hálózati automatikák és villamos védelmek rendszerét.

A villamosenergia rendszer felépítése és működése minden körülmények között az ellátás biztonságot kell, hogy szolgálja. Az ellátás biztonság meghatározó eleme a hazai termelő kapacitások rendelkezésre állása. A termelési volumen és szerkezeti összetétel változásának nyomon követése teszi lehetővé a közép és hosszútávú forrásoldali tervezést. A jelenleg üzemelő erőművek egy részének kiöregedése a fejlett országok trendjébe illeszkedően hazánkat is érinti. A tervezés során meghatározó alapdokumentumnak kell tekinteni a hazai energiapolitikát megalapozó Energiastratégia 2030 kiadványt, a Magyar Energetikai és Közműszabályozási Hivatal által kiadott ajánlásokat a 12542/2019 sz. határozat szerint valamint az Európai Bizottság 2016-ban kiadott Tiszta energia minden európainak (Clean Energyfor all Europeans Package), ajánlást és a villamos energiáról szóló rendeletet.

A magyar energiapolitika alapvetései az ellátás biztonság érdekében születtek. Ezek közé tartozik, hogy a teljesen nyílt és szabad versenyfeltételek között a vonatkozó rendeletek és előírások betartása mellett, bárki építhet erőművet. Az európai együtt járó villamosenergia rendszer részeként a villamosenergia piac vonatkozásában is cél az egységesülő európai rendszerbe történő integrálódás. Egy megbízhatóan üzemelő nagy rendszer részeként akkor járunk el kellő körültekintéssel az ellátásbiztonság szempontjából, ha képesek vagyunk megtermelni a saját szükségletünket és ezzel az együtt járó rendszer stabilitásához is hozzájárulunk. Természetesen az árampiacon is előnyösebb helyzetben üzletelünk, ha elegendő termelő kapacitás áll mögöttünk. A következő ábrán vizsgáljuk meg, hogyan alakult a hazai bruttó végső felhasználás forrás szerkezete a 2019. évi feldolgozott adatok alapján.




*9. ábra: A teljes bruttó villamosenergia felhasználás megoszlása 2019-ben. [10]*

2019. évben a teljes hazai villamosenergia fogyasztás 45,66 TWh volt, amely szerény növekedést jelent a 2018-ban felhasznált 45,42 TWh mennyiséghez képest. Ami lényeges változás, hogy a nukleáris termelés hányada valamivel növekedett a szén és lignittüzelés részesedése viszont csökkent az előző évi adatokhoz képest. Ez az MVM Paksi Atomerőmű esetén 16,29 TWh, a szén-lignit elégetése pedig 3,86 TWh termelt villamosenergia mennyiséget jelentett 2019-ben. A megújuló tartományban a napenergia területén csaknem 1,5%-os termelésbővülés tapasztalható, de ezzel együtt is csupán 2%-kal járult hozzá az éves igények kielégítéséhez. Az ellátás szerkezetében 30% alá csökkent az importból származó villamosenergia fogyasztás ezzel szemben növekedett a földgáz elégetéséből származó energia mennyiség. Az ellátás szempontjából megállapítható, hogy az MVM Paksi Atomerőmű termelési volumene a legnagyobb szerkezeti elem. Nélküle sem a klímavédelmi sem a rezsicsökkentési célok nem tudnának teljesülni. Alaperőműként a Mátrai

erőmű termelési mennyisége is jelentős mértékben hozzájárul a hazai részarány növeléséhez. A hazai termelés a teljes villamosenergiaigény 72,4%-át fedezte, amelyből 49,2%-kal az atomerőmű és 11,7%-kal a lignit-szén technológia vette ki a részét. A nukleáris kapacitás fenntartása és a Mátrai Erőmű kapacitás megújítása tehát elemi érdekünk a társadalmi jólét és a gazdasági teljesítőképesség biztosításához. A hazai földgáz felhasználás 20%-a származik saját forrásból, ezért a földgáz döntő részének beszerzése is a meglehetősen magas energia igényünk importfüggőségét erősíti. Energiatárolók hiányában az időjárásfüggő megújulóként termelő naperőművek változékony termelésének korrigálásában is részt vesznek a gázturbinák. A naperőművek térnyerését a rugalmassági kapacitások létesítésével is le kell követni. Az elmúlt évek nem hoztak jelentős termelési szerkezet átalakulást. [10]

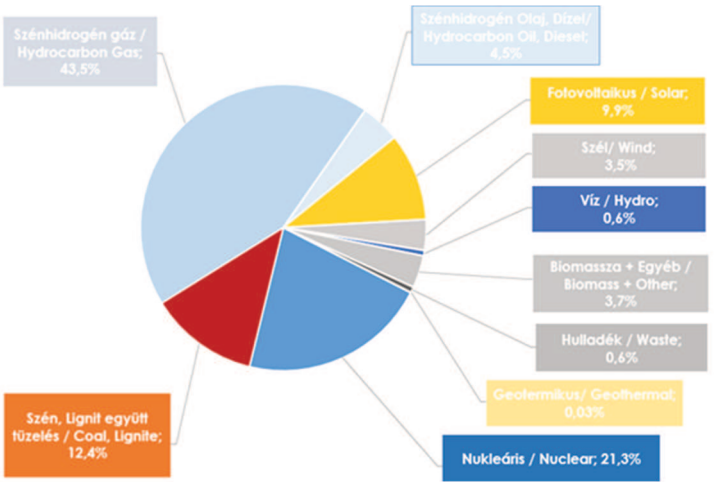
A hazai rendszer vizsgálatának folytatásához a 2019. december 31-én rendelkezésre álló beépített kapacitások jellemzőit tekintsük át.

| **Primer források** | **Beépített teljesítmény (MW)** |
|---|---|
| Hagyományos erőművek összesen | |
| Nukleáris | 2012,8 |
| Szén, Lignit, Együtt tüzelés | 1166,3 |
| Szénhidrogén Gáz | 4111,8 |
| Szénhidrogén Olaj, Dízel | 421,1 |
| **Összesen** | **7712,0** |
| Megújuló erőművek összesen | |
| Fotovoltaikus | 936,3 |
| Szél | 327,5 |
| Víz | 57,8 |
| Biomassza + Egyéb | 346,1 |
| Hulladék | 59,4 |
| Geotermikus | 2,7 |
| **Összesen** | **1729,8** |
| **VER összes beépített** | **9441,8** |

*10. ábra: A Magyar Villamosenergia Rendszer beépített kapacitás értékei 2019-ben. [10]*

A táblázatban szereplő fotovoltaikus részesedés a háztartási méretű egységeket nem tartalmazza. A hagyományos erőművek, amelyek jellemzően a nagyerőműveket jelentik és csaknem 82%-os arányt képviselnek a teljes erőművi flottában. A primer források szerinti technológiák beépített teljesítményei alapján a megoszlás arányait a következő ábra szemlélteti. Ha összevetjük a korábban részletezett megtermelt energiamennyiségek arányát a beépített teljesítmények részesedésével szembetűnő az arányok eltolódása. Ennek magyarázata a különböző technológiák egymástól eltérő teljesítmény kihasználási tényezőjében

rejlik. Ez a tényező százalékos értékben azt mutatja meg, hogy egy erőmű éves termelését az év hány százalékában termelné meg akkor, ha a névleges teljesítményén az év 8760 órájában üzemelne.

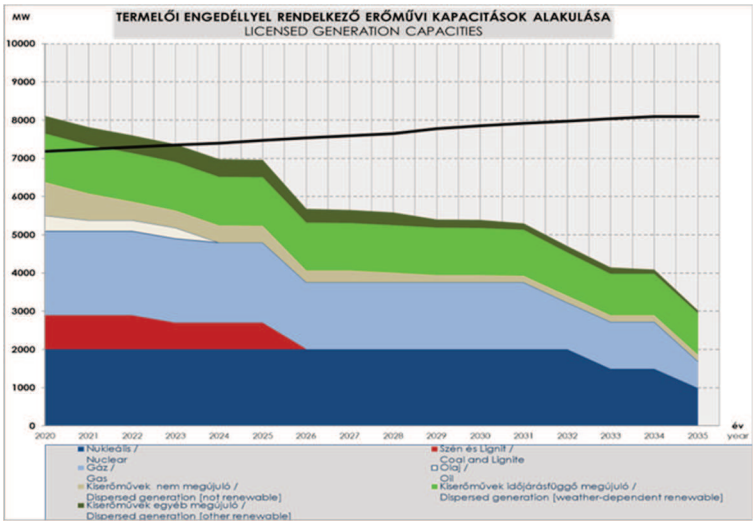



*11. ábra: A Magyar Villamosenergia Rendszer beépített kapacitásainak arányai 2019-ben. [10]*

Összehasonlításként 2019-ben a következő teljesítménykihasználási tényezők mellett termeltek az erőműveink: MVM Paksi atomerőmű 92,36%, Mátrai Erőmű 53,85%; szélerőművek 24,75% és a fotovoltaikus naperőművek 16,01%. A felsorolásból illetve az összevetésből élesen kitűnik, hogy az alaperőművek irányítható és szabályozható jellegéből adódóan az állandóan jelentkező fogyasztói igényt kielégítve jóval magasabb kihasználtsággal termelnek, mint az időjárástól függően energiát szolgáltató új megújuló bázisú termelő egységek. [10]

Érdekességképpen érdemes átgondolni azt, hogy a fosszilis primer energiaforrások elégetése nemcsak a szén-dioxid kibocsátása révén terheli a környezetét, hanem az égési folyamathoz felhasznált oxigén elvonásánál is. Az MVM Paksi Atomerőmű éves villamosenergia előállítása közel akkora mennyiségű oxigén elvonásától mentesíti a környezetet, mint amennyit a Magyarországon található összes erdő termel ugyanebben az időszakban. Ez nagyjából a teljes lakosság belélegzett oxigén mennyiségével azonos. [11]

Az ellátásbiztonság érdekében tisztában kell lenni azzal, hogy a meglévő, üzemelő erőművek közül a kiöregedés milyen mértékben fogja befolyásolni a termelési potenciált. A MAVIR prognózisa szerint a meglévő erőművek leállítása következtében 2029-ben 5326 MW, 2033-ra pedig 3908 MW összteljesítményű nagyerőműre számíthatunk összesen a jelenleg is üzemelők közül. A napjainkban üzemelő kiserőművekből mindössze 849 MW-ra számíthatunk 2033-ban. [9]




*12. ábra: A VER-ben maradó források és a várható csúcsterhelés. [10]*

A fenti ábrán a jelenleg meglévő erőművek beépített bruttó névleges teljesítménye látható a technológiák szerinti bontásban 2020. és 2035. közötti időszakban. Az ábra szemléletesen mutatja be, hogy termelőképesség csökkenése és a várható igények között meglehetősen gyorsan és nagymértékben növekszik a különbség. Tehát a hiányzó kapacitások pótlása elkerülhetetlen. A fogyasztói igények ellátásához szükséges hiányzó beépített teljesítmény biztosítására több alternatíva is kínálkozik. Valószínűleg az import szükségletünkkel a belátható időtávlaton belül még együtt kell élni. A külföldről érkező energiától való kitettségünket csökkenthetjük a meglévő eszközeink élettartam hosszabbító felújításával vagy új erőművek rendszerbe állításával. Az országos energetikai jövőkép megtervezéséhez nagyon sok és komplex tényező egyidejű elemzésének értékelését kell elvégezni mind hazai mind nemzetközi vonatkozásban. Az ellátásbiztonság folytonosságának koncepciója a társadalmi, gazdasági és globális fenntarthatósági szempontok figyelembevételével a szakpolitika feladata és felelőssége. A döntések meghozatalánál fontos szempontként kell figyelembe venni, hogy az energetikai beruházások viszonylag hosszú átfutási idővel valósíthatóak meg, ezért mindenképpen hosszútávú döntések szükségesek. A jövőbe mutató irányokat sokkal inkább kellő körültekintéssel, megalapozottan előkészített stratégiai döntésekkel, mint a pillanatnyi piaci hangulat alapján kell meghatározni. A jelenlegi piaci viszonyokat egyrészt a Németországban beépített több mint száz gigawatt időjárásfüggő valamint a főként Lengyelországban, Csehországban és Ukrajnában az élettartamuk végén járó szén bázison termelő erőművek alakítják. Ez hosszú távon nem fenntartható állapot, ezért a piaci árak emelkedése várható. [9] A másik fontos szempont, hogy a hazai felhalmozott erőműves szakmai tapasztalatot és tudást csak egy létező erőműpark esetén lehet fenntartani. A világon egyedüli lehetőségekkel rendelkező MVM Paksi Atomerőmű Karbantartó Gyakorló Központ új blokkok szempontjai szerinti bővítését érdemes lehet mérlegelnie a szakpolitikai döntéshozóknak. Piaci alapú nemzetközi képzések lebonyolítására is alkalmas lehetne. A hazai energiapolitika egyik meghatározó intézkedése volt a Nemzeti Energiastratégia 2030 megalkotása és további feladata ennek folyamatos felülvizsgálata és naprakészen tartása.

## ÖSSZEFOGLALÁS

Az emberiség fejlődésének meghatározó mozgatórugója az energia felhasználásának minősége, mennyisége és folyamatosan gyarapodó számú hozzáférési formája. Az energia felhasználás nyújtotta kényelem egyben az energiától való teljes függőséget is jelenti a civilizáció részére. Ez a kényelem egyben az energiától való teljes függőséget is jelenti a civilizáció részére. Manapság energia alapú társadalomban élünk, amelynek fejlődését a szintén energia alapú gazdaság biztosítja. Felhasználható energia hiányában mindkettő összeomlana. Megszűnne a fűtés, hűtés, szellőztetés, leállna minden termelés, használhatatlanná válnának a villamos energiát igénylő eszközök, megállna a közlekedés és minden technikai vívmány működésképtelenné válna. A villamos energia hiányában a rendvédelem és nemzetvédelem eszközrendszere is összeomlana. A biztonságtechnikai tudomány csoportjai csak a villamosenergia rendelkezésre állása esetén értelmezhető, mint a biztonsági informatika, kibernetika, operációkutatás csakúgy, mint a védelmi technológiák teljes vertikuma. Az energia felhasználható formáiban történő rendelkezésre állása az emberi közösségek és az egyes emberek biztonságát is meghatározza. A biztonságot, mint állapotot a biztonságtudomány létező egészségnek nevezi. Ez az egészség fogalom az emberi test és a társadalom tökéletes állapotát fejezi ki. A biztonságtudomány az objektív valóságot kettős módon közelíti meg. Egyik vizsgálati irány a technológia hasznossága az egyéni és társadalmi fejlődés szempontjából. A másik megközelítési iránya ugyanennek a technológiának a negatív hatása az egyének egészségére és a környezet terhelésére. A jelenkori energiafelhasználás mértékének egyik negatív hatása a Föld készleteinek mérhetetlen kizsákmányolása és a globális felmelegedés felgyorsulása. Az ipari forradalom óta az emberi tevékenység hatására folyamatosan emelkedő mértékben egyre nagyobb mennyiségű a légtérbe juttatott üvegház-hatású gáz. Ennek következtében egyre vastagabb a felhalmozódott üvegházhatású gázréteg vastagsága, így csökken a légtérből kijutó hőmennyiség is. A legnagyobb veszteségi hőmennyiség és egyben üvegház-hatású gáz kibocsátó szektorok az energia előállítás, a közlekedés-szállítás, az ipar és az épületek.

Az IPPC 2014-es adatai szerint üvegházhatást okozó gázok 76%-át a széndioxid teszi ki. [3] Az IEA (International Energy Agency) által 2018-ban kiadott Word Energy Outlok alapján, 2017-ben a karbon emisszió közel 42%-át a villamosenergia előállítása, csaknem 25%-át a közlekedés-szállítás és 19%-át az ipari termelés okozta. [4] A 2013-as évben az üvegházhatást okozó gázok 72%-ának kibocsátásáért, a különböző gazdasági szektorokhoz köthető energia felhasználás tehető felelőssé. [12] A globális fejlődés akkor válhat fenntarthatóvá, ha a folyamatosan növekvő energia igényt drasztikusan csökkenő emisszió mellett tudjuk biztosítani, azaz meg tudjuk valósítani a tiszta energiák térnyerését az energiatermelési és felhasználási szerkezet összetételében. A dekarbonizáció egyik kézenfekvő megoldási iránya az elektrifikáció lehet, amely lehetőséget nyújt a digitalizáció kiterjesztésére a közlekedési és ipari szektoron belül. Ez a nagyon magas szintű automatizálást, vagyis az okos rendszerek alkalmazását jelenti. A dekarbonizációs célok csak abban az esetben teljesíthetőek, ha a kiöregedő erőművi technológiák pótlását és az ezzel egyidőben jelentkező villamos energiaigény növekedés szükségletét karbon semleges források alkalmazásával lehet kielégíteni. A klímavédelem és az ellátásbiztonság teljesítése érdekében a villamosenergia termelésben meghatározó szerep jut a nukleáris bázisú technológiáknak.

A világon jelenleg 441 energetikai célú nukleáris reaktor üzemel összesen 390 113 MW nettó beépített villamos teljesítménnyel. A nukleáris kapacitás-fenntartás és bővítés érdekében 54 reaktor épül világszerte összesen 57 441 MW nettó tervezett villamos teljesítőképességgel. Az atomerőművek jelentőségét igazolja a 18 505 összes reaktor év, amely az eddigi szolgálatuk eredménye. [7] A legújabb 3+ generációs atomerőművi blokkok megnövelt biztonságú rendszerelemeit már a 2011-es fukushimai atomerőmű baleset tapasztalatait alapul véve alakították ki. A villamos energia rendszerek stabilitásához az alaperőművi funkciót kiegészítő manőverező képességükkel is nagyban hozzájárulnak.

A szakpolitikai előrejelzések szerint nap és a szél források termelése dominálni fog a villamos energiatermelésen belül 2050-re. Erre az időpontra már a teljes globális áramtermelés felét fogják adni. A vízenergia 17%-os részesedése mellett a nukleáris termelés 10%-os súllyal tartja meg nélkülözhetetlen szerepét az ellátásbiztonságban. Ahhoz, hogy 2050-re a villamosenergia termelés karbon intenzitása 23g CO2/kWh értékre csökkenjen a 2018-as 475 g CO2/kWh értékről a nukleáris energia felhasználása kiemelt jelentőségű. Amennyiben a fejlett gazdaságok nukleáris ágazatában nem történnek üzemidő hosszabbítások és nem indulnak új beruházások, abban az esetben a rendszerből hiányzó atomerőművek helyettesítését megújuló forrásokkal kellene megoldani. Ennek becsülhetően legalább1,6 trillió USD többlet beruházási költség vonzata lenne a 2040-ig elemzett időszakban. [5]

## FELHASZNÁLT FORRÁSOK

[1] Cs. Kollár, Á. Zakar, „A social engineering és a manipulációs technikák és módszerek” *Biztonságtudományi Szemle*, 2. évf. 3. szám.
[2] T. Kovács, I. Milák, Cs. Otti, „A biztonságtudomány biometriai aspektusai” *http://www.pecshor.hu/periodika/XIII/kovacsti.pdf, letöltés: 2020. augusztus 28.*
[3] EPA United States Environmental Protection Agency (2020.): https://www.epa.gov/ghgemissions/global-greenhouse-gas-emissions-data
[4] International Energy Agency, World Energy Outlook, 2018. (WEO, 2018)
[5] International Energy Agency, World Energy Outlook, 2019. (WEO, 2019)
[6] MVM Paksi Atomerőmű Zrt.(2020): http://www.atomeromu.hu/hu/Documents/Korai_eredmenyek.pdf
[7] International Atomic Energy Agency, Power Reactor Information System, (2020): https://pris.iaea.org/pris/
[8] ENTSO-E (2020.): https://www.entsoe.eu/
[9] MAVIR (2019) Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt. adatpublikáció 2019.
[10] MAVIR (2020) Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt. adatpublikáció 2020.
[11] MVM Paksi Atomerőmű Zrt. (2020.): http://www.atomeromu.hu/hu/Latogatoknak/Lapok/default.aspx
[12] Európai Bizottság (2018): A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, az Európai Gazdasági Szociális Bizottságnak, a Régiók Bizottságának, az Európai Beruházási Banknak, Tiszta bolygót mindenkinek, Európa hosszútávú stratégiai jövőkép egy virágzó, modern, versenyképes és klímasemleges gazdaságról, Brüsszel,

2018.11.28. (COM 2018) 773 Final Center For Climate And Energy Solutions https://www.c2es.org/content/international-emissions/

**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