DEVELOPMENT AND INTEGRATION OF MANAGEMENT SYSTEM STANDARDS

A SZABVÁNYOS IRÁNYÍTÁSI RENDSZEREK FEJLŐDÉSE, INTEGRÁCIÓJA

FOGARASI Attila[1] – SZŰCS Endre[2]

Abstract

The article presents the development of standard management systems, the essential elements of the most important management systems, emphasizing the importance of HLS standards. HLS (HLS = high level structure) standards have the same structure and contain many of the same concepts and definitions. The article analyzes new ways of standardization, its connection to the development of the legal system through the relationship between the certification system supported by the General Data Protection Regulation (GDPR) and the development of international standardization.

Keywords

management system standards, quality management, occupational health and safety, information security, General Data Protection Regulation

Absztrakt

A cikk bemutatja a szabványos irányítási rendszerek kialakulását, a legfontosabb irányítási rendszerek lényeges elemeit. Kiemeli az ún. HLS rendszerű szabványok jelentőségét. A magas szintű szerkezet szabványok (high level strukture, a továbbiakban: HLS) azonos felépítésűek, és sok azonos fogalmat és meghatározást tartalmaznak. A cikk elemzi a szabványosítás új útjait, kapcsolódását a jogrendszer fejlődéséhez az általános adatvédelmi rendelet (GDPR) által támogatott tanúsítási rendszer és a nemzetközi szabványosítás fejlődésének kapcsolatán keresztül.

Kulcsszavak

irányítási rendszer szabványok, minőségirányítás, munkahelyi egészség és biztonság, információbiztonság, általános adatvédelmi rendelet

[1] fogarasi.attila@phd.uni-obuda.hu | ORCID: 0000-0002-1585-7301 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | senior lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

A NEMZETKÖZI SZABVÁNYOSÍTÁS FEJLŐDÉSE

A termelési folyamatok összetettebbé válása, a termelésen belüli munkamegosztás, a munkafeladatok egymásutánisága már a társadalmi fejlődés korai szakaszában is megkövetelte a munkafolyamatokra vonatkozó szabályok rögzítését. A kontinuensen alkalmazott normák eleinte a termelői csoportokon belül validáltan jöttek létre. Amikor a termelési folyamatok a kis közösségeken túlnőttek, interkommunálissá váltak, különösen fontossá vált a normák globalizálódása. A megtermelt javak cserekereskedelmével megszületett az igény a szabályok általánossá tételére is.

Az egyik közösségen belüli termelési folyamat végterméke egy másik közösség termelési folyamatának nyersanyagává vált. Egy ilyen összetett folyamat csak az adott termékre vonatkozó normák összehangolása útján volt kezelhető eredményesen. A fejlődés eredményeként megjelentek az akkor még partikuláris hosszmértékek, súlymértékek, időmértékek. Később, az ipari forradalom, a tömegtermelés már elképzelhetetlen volt a részletes technológiai szabályok, szabványok alkalmazása nélkül.

A világ első nemzeti szabványügyi testülete Angliában, Mérnöki Szabványügyi Bizottság néven jött létre. A testületet Sir John Wolfe-Barry, a londoni Tower Bridge tervezője alapította, 1901-ben. Az intézet 1931-ben vette fel a mai nevét (British Standards Institution, a továbbiakban: BSI). [1]

A szabványosítás nemzetközi szervezetei közül először a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, a továbbiakban: IEC) alakult meg 1906-ban. A megalakulás előzménye az 1904-ben rendezett St. Louis-i világkiállításra datálható. A kiállításon ugyanis rendkívüli sikert aratott a „Villamos Palota", bár a kiállítók számtalan különböző feszültségű egyenáramú, 1-, 2-, 3 fázisú váltóáramú villamos rendszert alkalmaztak, a legkülönfélébb csatlakozókkal, dugaszokkal. A kiállítással párhuzamosan megrendezett tanácskozáson éppen ezért vetődött föl az ötlet egy állandó nemzetközi bizottság felállítására, amelynek feladata az elektromos készülékek és gépek minősítési feltételeinek és méréseinek meghatározása, egységesítése.

Az akkori tárgyalások eredményeként alapították meg Londonban az IEC-t, amely 1906. június 26–27-én tartotta első ülését a Hotel Cecilben, Alexander Siemens (A Siemens céget alapító Werner Siemens unokatestvére) elnökletével. Az alapító országok – Belgium, Kanada, Franciaország, Németország, Nagy-Britannia, Holland, Svájc, Spanyolország, Japán és az Egyesült Államok – között ott volt Ausztria-Magyarország is. Így hazánk már a szabványosítás hajnalán, az első országok között csatlakozott az új kezdeményezéshez.

A testület első titkára Charles Le Maistre lett, aki olyan megbeszéléssorozatot kezdeményezett, melynek köszönhetően 1926-ban megalapították a Nemzeti Szabványosító Egyesületek Nemzetközi Szövetségét (International Federation of the National Standardizing Associations a továbbiakban: ISA). A világháború után az ISA megszűnt és helyét az 1947-ben megalakult, Nemzetközi Szabványügyi Szervezet (Intarnational Standard Organisation a továbbiakban: ISO) vette át. [2] A nemzetközi szervezet megalapítása érdekében kifejtett munkásságáért, sokan Le Maistre-t tekintik a nemzetközi szabványosítás atyjának. [3]

A nemzetközi szabványügyi szervezetek megerősödésével párhuzamosan megszülettek a kisebb-nagyobb regionális szabványügyi szervezetek is, többek között az Európai Szabványügyi Bizottság (Comité Européen de Normalisation a továbbiakban: CEN) - 1975,

az Európai Elektrotechnikai Szabványügyi Bizottság (European Committee for Electrotechnical Standardization a továbbiakban: CENELEC) – 1973, illetve az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute a továbiakban: ETSI) 1988.

A kormányoktól független ISO-nak jelenleg 165 nemzeti szabványügyi testület a tagja. Az ISO központi titkárságának székhelye Genfben található. Az ISO működési elve azon alapszik, hogy tagjai segítségével szakértőket von be, akik megosztják egymással ismereteiket, és olyan önkéntes, konszenzuson alapuló, piaci szempontból releváns nemzetközi szabványokat dolgozzanak ki, amelyek támogatják az innovációt és megoldásokat kínálnak a globális kihívásokra [4].

A HAZAI SZABVÁNYOSÍTÁS RÖVID TÖRTÉNETE

A kiegyezést követő fellendülés, az építőipar rohamos fejlődése és az akkor korszerű építészeti módszerek, anyagok megjelenése következtében az építőanyagok szabványosítását 1875-ben kezdte el Magyar Mérnök- és Építészegylet, Ybl Miklós irányításával. Munkájuk eredményeként vált nyilvánvalóvá, hogy a szabványosítás intézményesített rendszerére is szükség lesz.

Az egész világon a legelsők között alakult meg 1921-ben hazánkban a szabványosítás első hivatalos szervezete, a Magyar Ipari Szabványosító Bizottság, amelynek alelnöki tisztségét Kandó Kálmán töltötte be. 1933-tól kezdett el működni a Magyar Szabványügyi Intézet. 1948-ban a Magyar Szabványügyi Intézetet államosították, és 1951-ben létrehozták a Magyar Szabványügyi Hivatalt, amely elvesztette függetlenségét és a közigazgatás részeként, hivatalként működött tovább. A független intézményi státusz kétségtelen előnyeit nem feledve, meg kell állapítanunk, hogy az állami intézményrendszerbe tagozódásnak is voltak előnyei. A hatósági jogkör lehetővé tette, hogy 1995-ig a szabványok betartása Magyarországon kötelező legyen.

Magyarország európai integrációjának részeként vállalt kötelezettsége volt a szabványosítás autonómiájának helyre állítása. A magyar szabványosítás rendszerét a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény formálta át ismét, amely tulajdonképpen visszaállította a szabványosítás klasszikus alapelveit. Fontos sarokpontja lett az új szabályozásnak, hogy a szabványosítás nem kormányzati feladat. A törvény értelmében a korábbi Magyar Szabványügyi Hivatal (a továbbiakban MSZH) megszűnt és megalakult a Magyar Szabványügyi Testület (a továbbiakban: MSZT), mint Magyarország nemzeti szabványügyi szervezete.

A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény 4. § (1) bekezdése – máig ható érvénnyel – rögzítette a szabvány fogalmát is:

„A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb.” [5]

A JELENTŐS IRÁNYÍTÁSI RENDSZEREK A JELENLEG HATÁLYOS SZABVÁNYOK TÜKRÉBEN

A szabványosítás mára túlnőtt az ipari termelés, a szűken vett technológiai folyamatok paramétereinek meghatározásán. Jelenleg 21.584 db. ISO szabvány van érvényben.

A szabványok nemcsak számosságukban váltak meghatározóvá, de megjelentek a komplex rendszerek, szervezetek irányítását meghatározó ún. „menedzsment irányítási rendszerek" (*Management System Standards, a továbbiakban: MSS*) szabványai is. Ez a szabványosítási terület az, ami a technológiai fejlődés társadalmi hatásainak leggyorsabban változó tükre, a fejlődés értékmérője. Az ISO jelenleg több mint 80 ilyen szabványt tart nyilván [6] (a*z MSS szabványok teljeskörű listáját az 1. számú melléklet tartalmazza*).

Az irányítási rendszerek egy része ún. HLS szabvány. A HLS szabványok azonos felépítésűek, és sok azonos fogalmat és meghatározást tartalmaznak. Ez különösen hasznos azon szervezeteknek, amelyek úgy döntenek, hogy egyetlen „integrált" irányítási rendszert működtetnek, amely egyidejűleg képes megfelelni két vagy több irányítási rendszer szabvány követelményeinek.

- A szervezetirányításban jelenleg az alábbi, egyébként ún. HLS típusú irányítási rendszer szabványok a legáltalánosabbak:
- Minőségirányítási rendszer (továbbiakban: MIR) – *MSZ EN ISO 9001:2015*
- Környezetközpontú irányítási rendszer (továbbiakban: KIR) – *MSZ EN ISO 14001:2015*
- A munkahelyi egészségvédelem és biztonság irányítási rendszere (továbbiakban: MEBIR) – *MSZ ISO 45001:2018*
- Információbiztonsági irányítási rendszer (továbbiakban: IBIR) – *MSZ ISO/IEC 27001:2014*

„Az ISO 9001 minőségirányítási, az ISO 14001 környezetirányítási és az ISO 27001 információbiztonsági szabványok közös jellemzője a folyamatközpontúság. Mindegyik az ISO 9001 felépítését követi. A szabványok végén található mellékletek a tartalomjegyzékek pontjait követve ezt a kapcsolatot részletesen bemutatják. A szabványalkotók egyik célja az volt, hogy a szabványok –a többszörös szabályozást elkerülve -integráltan is bevezethetők legyenek. A kialakított integrált irányítási rendszer „egyszeres" auditálása is megoldható." [7]

Célunk a szervezetirányítás ezen meghatározó szabványainak, illetve azok egymáshoz kapcsolódásának elemzése.

MINŐSÉGIRÁNYÍTÁSI RENDSZER: ISO 9001-ES SZABVÁNY

A minőségirányítási ISO 9001 szabvány talán legfontosabb újdonsága a működés folyamatalapú megismerése, feltérképezése, a működés folyamatokon keresztüli megértése volt. A szabvány 1987 márciusában jelent meg. Hazánkban az első kiadása MSZ EN 9001:1992 néven, 1992-ben történt.

„Ez a nemzetközi szabvány a minőségirányítási rendszer kialakítása, bevezetése, valamint eredményességének és hatékonyságának fejlesztése során a folyamatszemléletű megközelítés alkalmazását segíti elő. Egy szervezeten belül a folyamatok egy rendszerének alkalmazása, e folyamatok meghatározásával, kölcsönhatásaival és irányításukkal együtt „folyamatszemléletű megközelítés"-nek tekinthető…

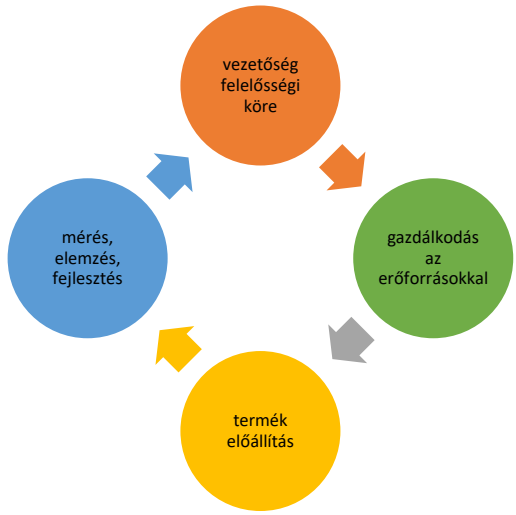
A folyamatszemléletű megközelítés egyik előnye az, hogy gondoskodik a rendszeren belül az egyes folyamatok közötti kapcsolatnak, továbbá a folyamatok kombinációjának és kölcsönhatásának folyamatos szabályozásáról." [8]

Ha ezt a megközelítést egy minőségirányítási rendszerben alkalmazzák, akkor ez kiemeli a következő szempontok fontosságát:

a) a követelmények megértése és teljesítése,
b) a folyamatok átgondolásának szükségessége a hozzáadott érték szempontjából,
c) a folyamat működésére és eredményességére vonatkozó adatok megismerése, valamint
d) a folyamatok folyamatos fejlesztése, objektív mérések alapján.

Az ISO 9001 szabvány bevezette azt a módszert, hogy minden folyamatot ún. Tervezés-Végrehajtás-Ellenőrzés-Intézkedés (Plan-Do-Check-Act, a továbbiakban PDCA) ciklusokban paraméterezünk. A szabvány röviden meghatározza a PDCA ciklus (1. ábra) elemeinek tartalmát is:

- **Plan**: (tervezés): azoknak a céloknak és folyamatoknak a megállapítása, amelyek a vevői követelményeknek és a szervezet politikájának megfelelő eredmények eléréséhez szükségesek;
- **Do**: (végrehajtás): a folyamatok bevezetése;
- **Check**: (ellenőrzés): a folyamatok és a termékek figyelemmel kísérése és összehasonlítása a politikával, a célokkal és a termékre vonatkozó követelményekkel, valamint az eredmények bemutatása;
- **Act**: (intézkedés): intézkedések megtétele a folyamat működésének folyamatos fejlesztésére. [8]



1. ábra PDCA ciklus az ISO 9001 szabvány szerint [8], saját szerkesztés

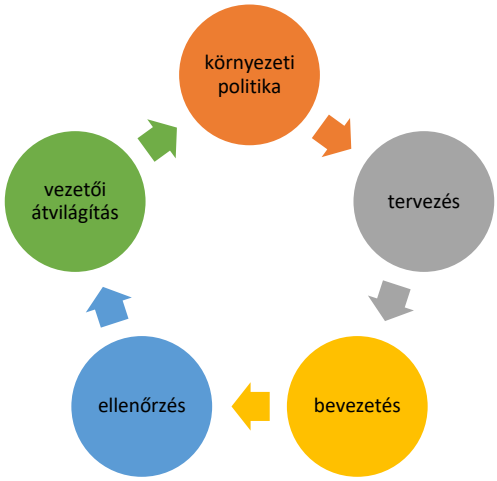
Az ISO 9001 ún. HLS szabvány, azaz meghatározásai, fogalmai a többi HLS szabvánnyal összeegyeztetettek.

KÖRNYEZETIRÁNYÍTÁSI RENDSZER (KIR): ISO 14001-ES SZABVÁNY

A KIR egy nagyon érdekes szabvány. Sokkal kevésbé egzakt követelményeket határoz meg, mint az ISO 9001, bár HLS szabványként a két szabvány alkalmas a szervezet irányítási rendszerének integrált kialakítására.

Magát az ISO 14001 szabványt a Nemzetközi Szabványügyi Szervezet 1996 szeptemberében adta ki először. A szabvány (*MSZ EN ISO 14001:1997*) már a következő évben, 1997-ben megjelent a Magyar Szabványügyi Testület gondozásában.

A szabvány deklarálja szoros kapcsolatát az ISO 9001 szabvánnyal. Átveszi, bár kissé módosítva a PDCA modellt is (*2. ábra*).



2. ábra PDCA modell az ISO 14001 szabvány szerint [9], saját szerkesztés

Az ISO 14001 szabvány nem tartalmaz abszolút követelményeket. Azt várja el a szervezettől, hogy legyen elkötelezett a jogszabályok maradéktalan betartásában. Vállalja a környezetvédelmi rendszerének folyamatos fejlesztését, illetve azt, hogy törekszik a környezetszennyezés minden formájának megelőzésére. Ez a megengedő szemlélet azt is lehetővé teszi, hogy két hasonló szervezet akkor is megfeleljen a szabványnak, ha környezetvédelmi teljesítményük színvonala egymástól lényegesen eltér.

Hangsúlyos eleme a szabványnak, hogy meghatároz néhány nagyon fontos környezet irányítási fogalmat. (*ISO 14001:2005*)

*„**Környezet**: A szervezet közvetlen környezete, amelyben az működik, beleértve a levegőt, a vizet, a földterületet, a természeti erőforrásokat, a növény és állatvilágot, az embereket és ezek kölcsönös kapcsolatait.*

***Környezeti tényező**: Valamely szervezet tevékenységének, termékeinek vagy szolgáltatásainak olyan eleme, amely kölcsönhatásba kerülhet a környezettel.*

***Környezeti teljesítmény**: Egy szervezet irányításának mérhető eredményei, a környezeti tényezők tekintetében.*

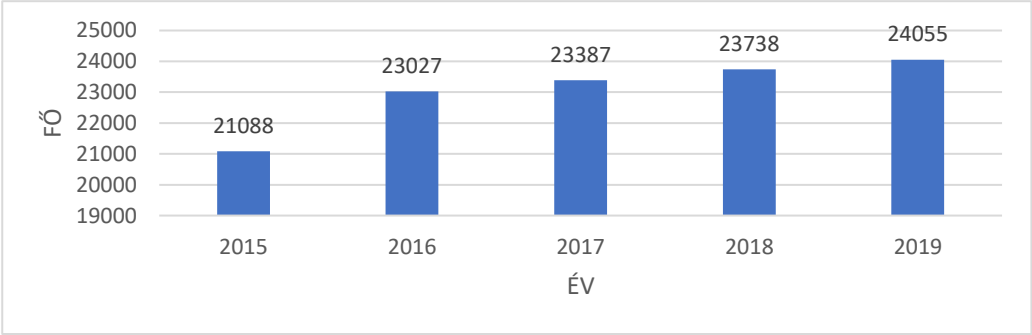
***Környezeti politika**: Egy szervezet környezeti teljesítményére vonatkozó általános szándékei és irányvonalai, ahogyan azt a vezetőség hivatalosan megfogalmazta.*

***Környezetközpontú irányítási rendszer (továbbiakban: KIR)**: Egy szervezet irányítási rendszerének aza része, amelynek az a szerepe, hogy kialakítsa és bevezesse környezeti politikáját és kezelje környezeti tényezőit."* [9]

A szabvány annak ellenére, hogy nem fogalmaz meg konkrét környezeti kritériumokat, maga a tanusítási folyamat, illetve a szabványból következő permanens fejlesztési igény arra sarkalja a szervezetet, hogy környezet terhelését folyamatosan optimalizálja.

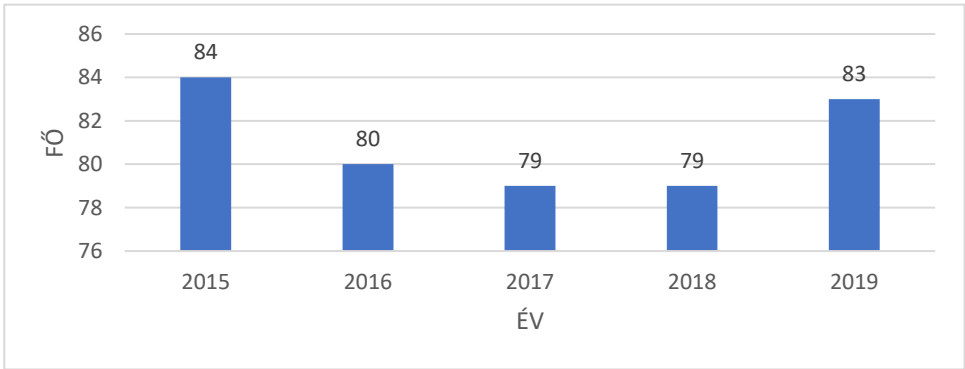
A MUNKAHELYI EGÉSZSÉGVÉDELEM ÉS BIZTONSÁG IRÁNYÍTÁSI RENDSZERE (MEBIR): ISO 45001

Évente sok ezer ember hal meg munkabalesetek, foglalkozási betegségek következtében. A sérülések, nem halálos megbetegedések száma pedig szinte felbecsülhetetlen. Az ENSZ szakosított szervezetének, a Nemzetközi Munkaügyi Szervezetetének (International Labour Organisation a továbbiakban: ILO) 2010. évi statisztikája szerint, az adatszolgáltató 56 országban több, mint 6 millió munkabaleset történt. Magyarország 2015-2019 közötti munkabaleseti statisztikája (*3. ábra*) szerint az éves munkabalesetek húszezer fő körüli létszámot érintenek.



3. ábra Az összes munkabaleset száma Magyarországon 2015-2019 [10], saját szerkesztés

Látható, hogy hazánkban évente egy közepes város lakosságát elérő számú munkavállalót ér munkabaleset, és közel száz ember hal meg munkabaleset következtében (*4. ábra*).



4. ábra Összes halálos munkabalesetek száma Magyarországon 2015-2019 [10], saját szerkesztés

A nemzetközi és a hazai szabványügyi szakemberek éppen ezért nagy fontosságot tulajdonítottak annak, hogy olyan szabványt fejlesszenek, amely évente csaknem hárommillió életet menthetnek meg és a HLS rendszerbe igazodván, a többi ISO-menedzsment rendszerhez hasonló módon felépítésüknek köszönhetően integrálhatóvá váljanak az olyan szabványokhoz, mint az ISO 14001 vagy az ISO 9001.

A BSI már az 1990-es években, a Nemzetközi Munkahelyi Egészségvédelmi és Biztonsági Értékelő Sorozat projektcsoport tagjaként kidolgozta és kiadta az első munkavédelmi és munkahelyi egészségvédelmi szabványát (*Occupational Health and Safety Assessment Series, a továbbiakban: OHSAS*) a BS OHSAS 18001 jelű szabványt. A szabványt 2007-ben megújították. Integrálták az ENSZ szakosított szervezetének, az ILO-nak az irányelveit és a munkabiztonság mellett egyre nagyobb hangsúlyt kapott a munkahelyi egészségvédelem. Ezt a brit szabványt emelte át a Magyar Szabványügyi Testület az MSZ 28001 jelű szabványba 2008-ban.

Az ISO csak 2018-ban hirdette ki az OHSAS szabványt, ISO 45001 címen. Az új számozást a BSI és a Magyar Szabványügyi Testület is átvette. A most hatályos számozás: MSZ ISO 45001:2018.

Érdekesség, hogy az ISO azért nem használhatta a BSI jól bevált 18001-es sorozatszámát, mert az már foglalt volt, ISO 18001:2004 néven a *rádiófrekvenciás azonosítás* témakörében érvényes szabvánnyal rendelkezett, így a brit szabványt az új, 45001 sorszámon hirdették ki. Magyarországon szintén foglalt volt a 18001-es sorszám (*MSZ 18001:1986 Gumi védősapka közúti járművek hidraulikus dobfékének nem ásványolajbázisú fékfolyadékkal működtetett kerékfékhengereihez 120 °C üzemi hőmérsékletig),*így nálunk eredetileg a szabvány a 28001-es sorszámot kaphatta csak meg. Szerencsére ma már mindenki az egységes, 45001-es sorszámot használja (*Egyébként megjegyezzük, hogy MSZ EN 45001:1990 Vizsgálólaboratóriumok működésének általános feltételei címen európai és magyar szabvány is volt már kihirdetve, amit időközben visszavontak…*)

A szabvány fontos eleme, hogy a szervezet képes legyen más érdekelt felek (munkavállalók, szerződéses partnerek, hatóságok) elvárásainak felismerésére. Fontos, hogy meghatározzák a tevékenységükben rejlő kockázati tényezőket és megoldásokat adjanak azok kezelésére. Mindez nem valósulhat meg a felső vezetés elköteleződése nélkül, ha nem vesz aktívan részt a szereplők elszámoltatásában, a folyamatok felmérésében.

INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR): ISO 27001

Az informatikai rendszerek egyszerre szolgálják és veszélyeztethetik cégek, szervezetek, közösségek működését. Az új szolgáltatások, felhőalapú megoldások, mesterséges intelligencia, okosvárosok, IT támogatású, automatizált döntéshozatali folyamatok megjelenése, rohamos terjedése újszerű kockázatokkal jár. A korábban megszokottnál jóval több figyelmet kell fordítani az informatikai biztonságra.

„ *2017 végén világszerte mintegy 3,8 milliárd internetfelhasználó volt, szemben a 2015-ös 2 milliárddal. A Cybersecurity Ventures úgy becsüli, hogy 2022-ra 6 milliárd internetező lesz (amely az addigra 8 milliárdra gyarapodó népesség 75%-a), 2030-ra pedig a számuk eléri a 7,5 milliárdot is (amely a jósolt 8,5 milliárdos lakosság 90%-a).*

2016-ban minden 39. másodpercre jutott egy hekkertámadás. A személyes adatok megszerzésére irányult sikeres támadások 95%-a három területre összpontosult: a

kormányzatra, továbbá a kereskedelmi és technológiai cégekre. 2016-ban a cégek 64%-a szenvedett el webalapú támadásokat, melyek 43%-a főként kisvállalkozásokra összpontosult. Tavaly összesen egymilliárd személyes profilt sikerült feltörni.
A Cybersecurity Ventures 2017-es jelentése szerint 2015-ben 3 milliárd dollár volt a kiberbűnözés okozta károk mértéke, és ez az összeg 2021-re meg fog duplázódni. A védekezésre költött összeg pedig öt éven belül el fogja érni az 1 milliárd dollárt." [11]

Nagyságrendben csak a kiberbűnözés okozta kár eléri Magyarország éves költségvetését. És akkor még nem is beszéltünk a látens, lappangó cselekményekről, illetve a bűnözés okozta erkölcsi, pénzben ki nem fejezhető károkról.

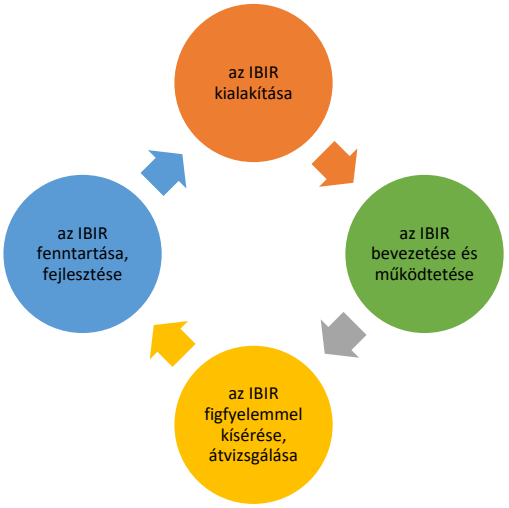
A szervezetek élete, működése ma már elképzelhetetlen informatikai rendszerek használata nélkül. Sőt az egyes jogi és szociológiai szempontból autonóm szereplők az IT rendszereiket, az internet közvetítésével, egymással összekapcsolva használják. Az így kialakuló nagyrendszrek működtetése megteremtette az illeszkedést segítő technológiai és irányítási szabványok kialakulásának szükségességét.

Az információbiztonság általánosan elfogadott irányítási rendszre az ISO 27001 szabvány lett. 2005 októberében jelent meg az első nemzetközi információbiztonsági irányítási rendszerre vonatkozó szabvány az ISO 27001:2005.

Az ISO / IEC 27001: 2005 minden típusú szervezetre kiterjedt. Alkalmas arra, hogy üzleti vállalkozások, kormányzati szervek, nonprofit szervezetek is bevezethessék. Az ISO / IEC 27001 szabvány szintén ún. HLS szabvány, így az ISO 9001 szabvánnyal összhangban meghatározza a dokumentált információbiztonsági irányítási rendszer létrehozásának, végrehajtásának, működtetésének, megfigyelésének, felülvizsgálatának, karbantartásának és fejlesztésének követelményeit. Fontos eleme a folyamatok feltérképezése, az azokban rejlő kockázatok felmérése és kezelése. Meghatározza az egyes szervezetek vagy azok részeinek biztonsági ellenőrzéseinek végrehajtási követelményeit is.

Az ISO 9001 szabványból örökölten az ISO 27001 szabvány is megalkotja a fejlesztésnek a PDCA cikluson keresztüli megvalósításoi modelljét (*5. ábra*) [12]

Tervezés (PLAN) (az IBIR kialakítása)	**Olyan IBIR-politika, -célok, -folyamatok és -eljárások kialakítása, amelyek lényegesek annak érdekében, hogy a kockázat kezelése és az információbiztonság fejlesztése a szervezet általános politikájával és céljaival összhangban lévő eredményeket tudjon felmutatni.**
Végrehajtás (DO) (az IBIR bevezetése és működtetése)	Az IBIR-politika, -intézkedések, -folyamatok és eljárások bevezetése és működtetése.
Ellenőrzés (CHECK) (az IBIR figyelemmel kísérése és átvizsgálása)	A folyamatok teljesítményének értékelése, és ahol lehetséges, mérése az IBIR-politikával, -célokkal és gyakorlati tapasztalatokkal összevetve, továbbá az eredmények jelentése a vezetésnek átvizsgálás céljából.
Beavatkozás (ACT) (az IBIR fenntartása és fejlesztése)	Helyesbítő és megelőző tevékenységek végrehajtása a belső IBIR-átvizsgálás (audit) és vezetőségi átvizsgálás eredményei, illetve egyéb lényeges információk alapján az IBIR folyamatos fejlesztése érdekében.



5. ábra A PDCA-modell az Információbiztonsági Irányítási Rendszer (IBIR)-folyamatokra alkalmazva [12], saját szerkesztés

ISO 27001:2005

„ ***Rendelkezésre állás (availability):*** *Olyan tulajdonság, amely lehetővé teszi, hogy az adott objektum, feljogosított entitás által támasztott igény alapján, hozzáférhető és igénybe vehető legyen.*

Bizalmasság, titkosság (confidentiality): *Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására.*

Sértetlenség (integrity): *A vagyontárgyak pontosságának és teljességének védelmét biztosító tulajdonság.„* [12]

Az információbiztonság éppen ezen pillérek védelme, megőrzése.

Az információbiztonság (information security) fogalma: Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése. Az információbiztonság fogalmi pillérei mellett, ezek a kiegészítő egyéb jellemzők is meghatározzák az információ biztonságát. Ilyen kategória többek között az információhoz hozzáférő azonosíthatóságát és az információ megváltoztathatatlanságát is biztosító hitelesség, számonkérhetőség, megbízhatóság is.

Az információbiztonsági irányítási rendszer (information security management system: továbbiakban: ISMS) az információbiztonságot szolgáló és „szavatoló” minőségirányítási szabvány. A rendszer, ahogy ezt az erről szóló MSZ ISO/IEC 27001 szabvány is rögzíti, az átfogó irányítási rendszernek az a része, amely egy, a működési kockázatokat figyelembe vevő megközelítésen alapulva kialakítja, bevezeti, működteti, figyeli, átvizsgálja, fenntartja és fejleszti az információvédelmet. [12]

A szabvány nagy előnye, hogy a mellékletében szinte sorvezetőt, check listát ad a szabványt bevezetni szándékozó kezébe, hogy elősegítse a megfelelésre felkészülést.
A szabályozás fő céljai és területei:

- A biztonsági szabályzat, politika kidolgozása.
- Az információbiztonság szervezetének meghatározása.
- A vagyontárgyak osztályozása, a felelősség meghatározása.
- Az emberi erőforrás biztonsága.
- A fizikai védelem kérdései.
- Kommunikációs, üzemeltetés irányítási feladatok meghatározása.
- Hozzáférés ellenőrzés.
- Az IT rendszerek biztonsági követelményei.
- Az információbiztonsági események kezelése.
- Az IT rendszerek üzletfolytonos működtetése.
- Compliance tevékenység szabályozása.

Mint a fenti listából látható, a szabvány nagyon alaposan és széles körben felméri, elemzi és értékeli a szervezet működési folyamatait.

2016. április 27-én megszületett a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet – GDPR). A rendelet az Európai Unió tagállamaiban a 2018. május 25-től kell alkalmazni.

A GDPR alaposan megmozgatta az unió lakosainak, információbiztonsággal foglalkozó szakértőinek életét, gondolkodását. A rendelet ugyan „csak" a polgárok személyes adatainak kezelésével kapcsolatban határoz meg kötelező szabályokat, ám a rendkívül magas bírságoktól való félelem a szervezet alkalmazkodási hajlandóságát jelentősen felerősítette. Sorra születtek az adatvédelmi tájékoztatások, információbiztonsági szabályzatok.

A GDPR 42. cikke foglalkozik a tanúsítás kérdésével. Az (1) bekezdés szerint:
*„A tagállamok, a felügyeleti hatóságok, a Testület, valamint a Bizottság – különösen uniós szinten – **ösztönzik olyan adatvédelmi tanúsítási mechanizmusok**, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak."*

Az ISO nem titkoltan annak érdekében, hogy a 42. cikk szerinti tanusítást elősegítse, azon szervezetek számára, akik már rendelkeznek ISO 27001 tanusítással, 2019 augusztusában kiadta az ISO/IEC-27701:2019-et (Privacy Information Management Systems a továbbiakban: PIMS) szabványt. A szabvány a szervezeten belül meghatározza a személyes adatvédelemi irányítási rendszer létrehozásának, fenntartásának szabványos követelményrendszerét. A GDPR alapelvi keretrendszerét konkrét kontrollokra és megoldásokra fordítja le.

A GDPR előírásokat tartalmaz arra nézve is, hogy olyan technikai intézkedéseket kell bevezetni és fenntartani, ami alkalmas arra, hogy az adatvédelmi incidenseket megelőzze. Azonban a rendelet nem nyújt támaszt a jogalkalmazónak ahhoz, hogy mik lehetnek ezek a technika mai állása szerint elfogadható védelmi intézkedések, melyek bevezetését a jogalkotó elvárja. Az ISO 27701 szabvány e területen is nyújt IT technológiai kapaszkodót a szervezetek számára.

„A Microsoft az EU-s GDPR-jogok globális kiterjesztése iránti elköteleződésének következő lépéseként a Microsoft Azure és az Office 365 szoftvereiben is megvalósítja a PIMS-et (személyes adatok védelmének irányítási rendszerét) és támogatja ügyfeleit és partnereit ezen interoperabilitási modell alkalmazásában." [11]

ÖSSZEGZÉS

Megállapíthatjuk, hogy a szabványosítás az eltelt több, mint száz éves történelme során nagy utat járt be. Az ipari fejlődés, a globalizáció, a nemzetközi termelési együttműködés már el sem képzelhető a jól működő nemzetközi szabványügyi együttműködés és a nemzetközi szabványok nélkül.

A szabványosítás magasabb szintjén jöttek létre az első irányítási rendszer szabványok. Ezen szabványok már nem csak az ipari termelés szervezetttségét, koordinációját segítették elő, de más szervezetek számára is kinyitották az együttműködés kapuit nemzeti és nemzetközi szinten is.

Létrejöttek a HLS szabványok, ahol már nem csak a szervezetek együttműködését segítették elő a szabványok, de a szabványok egymás közötti „együttműködése", egymásra épülése is magvalósult. Így egy megszerzett tanusítás a következő előszobája lehet, ezzel is promotálva a vezetői és szervezeti elköteleződést a szabványok mellett.

A GDPR rendelet megjelenése újabb mérföldkőhöz vezetett a szabványosítás történetében. A szabványosítás igénye már elszakad a termelési folyamatoktól. A GDPR egy kísérlet a személyes adatok védelmét szolgáló, országközi jogi szabályozás megteremtésére, oly módon, hogy a strikt jogi norma alkalmazkodni tudjon az egymástól redikálisan eltérő nemzeti jogrendszerekhez. Az egyszerű alkalmazkodás helyett a normakultúrába beépülés, a társadalmi értékrend formálása, a folyamatok önszabályozóvá válása is a célok között volt.

Ilyen rugalmas, önszabályozó rendszerek kialakításában nyugodtan hagyatkozhatunk a nemzetközi szabványosítás százéves hagyományaira, építhetünk sikereire. Ezért is várta a szakmai közönség az új nemzetközi szabvány megjelenését, ami az általános információbiztonsági szabványra ráépülve biztosítja a GDPR megfelelést. A szabvány elterjedése nagy segítség lesz a szervezetek gördülékeny együttműködése és egyidejűleg a rendeletnek megfelelés elérése területén.

IRODALOMJEGYZÉK

[1] British Standards Institution (BSI), „BSI; Our history," 2021.
[2] Nemzetközi Elektrotechnikai Bizottság (IEC), „IEC History," 2021.
[3] Kuert, Willy, FRIENDSHIP AMONG EQUALS (Recollections from ISO's first fifty years), Genf, Svájc, 1997, p. 16.
[4] Nemzetközi Szabványügyi Szervezet (ISO), „ISO About Us," 2021.
[5] A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény, 1995.
[6] Nemzetközi Szabványügyi Szervezet (ISO), „https://www.iso.org/management-system-standards-list.html," 2021.
[7] Michelberger Pál, Vállalkozásfejlesztés a XXI. században III. / Vállalatbiztonság pp. 35-52., D. N. I. Zoltán, Szerk., Budapest: Óbudai Egyetem, 2013, pp. 35-52.
[8] MSZ EN ISO 9001:2001, 2001.

[9] MSZ EN ISO 14001:2005, 2005.
[10] Innovációs és Technológiai Minisztérium Munkavédelmi Főosztály, „TÁJÉKOZTATÓ A MUNKABALESETEK ALAKULÁSÁRÓL A FELDOLGOZOTT MUNKABALESETI JEGYZŐKÖNYVEK ALAPJÁN 2020. első félév," 2020. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223 [Hozzáférés dátuma: 01 10 2021]. [Hozzáférés dátuma: 10 01 2021].
[11] Magyar Szabványügyi Testület, „Személyes adatok védelméről készült úttörő szabvány," 09 2020. [Online]. Available: https://prod.mszt.hu/hu-hu/szabvanyositas/hirek/2019/09/szemelyes-adatok-vedelmerol-keszult-uttoro-szabvany. [Hozzáférés dátuma: 09 01 2021].
[12] MSZ ISO/IEC 27001:2006, 2006.
[13] L. Berek, T. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.