Barát vagy ellenség az információs kommunikációs technológia?

Az Egyházi Könyvtárak Egyesülése (EKE) az adatvédelem kérdéseiről szervezett szakmai napot 2017. november 30-án a Sapientia Szerzetesi Hittudományi Főiskolán. A témaválasztást az új uniós adatvédelmi rendelet 2018 tavaszán esedékes hatályba lépése indokolta.

Ásványi Ilona, az EKE elnöke köszöntötte a szakmai nap előadóit és résztvevőit, majd kiemelte: az adatvédelem témakörében ez az első, könyvtáros szervezet által tartott szakmai nap. A rendezvény mottójául választott versben – „… és minden módon számon tartanak" – *Kosztolányi Dezső* a bürokrácia hatalmának erősödését vetette föl. Egy évtizeddel később *József Attila* már társadalmi méretűnek látta a kiszolgáltatottságot: „mikor lesz elég ok előkotorni azt a kartotékot, mely jogom sérti meg...". Hol vagyunk ma már ettől? Mostanára világméretűvé nőtt az emberek kiszolgáltatottsága. Ásványi Ilona hangsúlyozta: az adatvédelemről sok minden eszünkbe juthat: a könyvtár kezelésében lévő személyi adatok, az állománnyal vagy a működéssel összefüggő adatok, az adathordozók és számos egyéb tényező. A szakmai nap programját úgy állították össze, hogy minden fontos kérdés szóba kerüljön.

Kürti Sándor, a *Kürt Zrt.* elnöke „A vasaló nem attól meleg, mert a ruhához dörzsölik" című előadásában először röviden bemutatta az 1989-ben megalakított céget, melynek két fő tevékenységi területe az adatmentés és az informatikai biztonság. A *Kürt Adatmentést* 2014-ben fölvették a hungarikumok sorába; elsőként a technológiai hungarikumok közül.

A Kürt Zrt. a saját fejlesztésű adatmentő technológia révén vált világszerte ismertté – gyakorlatilag bármilyen adattárolóról bármit át tudnak menteni. 2001-ben a New York-i ikertornyok megtámadása nemcsak sok emberéletet követelt, de minden idők legnagyobb méretű adatvesztésével is járt. A Kürt Zrt. ingyen végezte a romok alól előkerült hordozókról az adatmentést; e tevékenységükért az USA elnöke személyesen mondott köszönetet.

A több évtizedes tapasztalat alapján Kürti Sándor pontosan látja, hogy hogyan kellene egy szervezetnek gondolkodnia és gondoskodnia az adatvédelemről, mivel az információáramlás az intézmény felelőssége, a vezetésnek kell biztosítania az adatvesztés és adatlopás elkerülését, illetve a sértetlenséget.

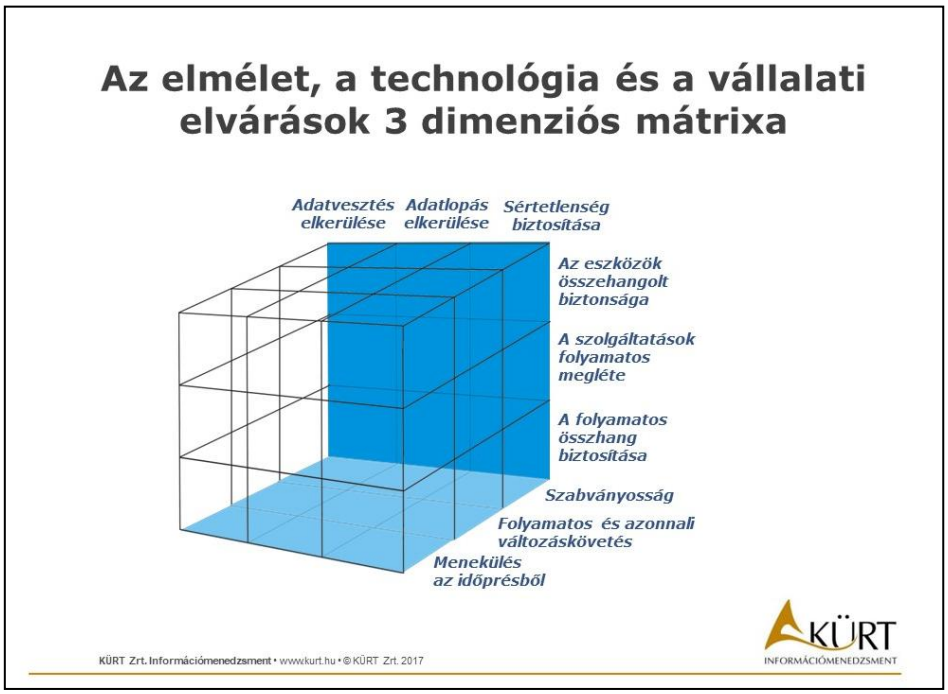
Az információbiztonsági alapkérdések technológiai vetületei:
1. az informatikai eszközök összehangolt biztonsága;
2. az informatikai eszközökhöz tartozó biztonsági szolgáltatások folyamatos felügyelete és gyakori ellenőrzése;
3. a fentiek folyamatos összhangjának biztosítása.

Fontos kritérium a szabályozottság, a szabványosság, a folyamatos és azonnali változáskövetés.

A közintézményekre különösen jellemző az időprésből való eszeveszett menekülés, amely arra vezethető vissza, hogy az informatikai problémák nap mint nap jelentkeznek, az erőforrások viszont csak szakaszosan állnak rendelkezésre (*1. ábra*).

Az információbiztonsági egyensúly tekintetében új nézőpontra kell helyezkedni:
- ki kell törni a technológia szorításából;
- a változáskövetést kiemelten kell kezelni;
- a humán oldalon komoly biztonsági tudatosságot kell tanúsítani;
- technológiai és humán oldalról is mérhetővé kell tenni a biztonságot.

Kertész Zoltán, a Kürt Zrt. adatmentési üzletágának igazgatója a „Mire bízzuk adatainkat?" című előadásában elmondta, hogy a cég a hozzájuk



1. ábra **Az információbiztonsági elméleti és technológiai problémái, továbbá az intézményi elvárások 3D mátrixa**

kerülő adathordozóknak mintegy 80%-át tudja megmenteni. Ez az arány magasabb is lehetne, ha az ügyfelek a hibás eszközt azonnal a szakértők gondjaira bíznák. Sajnos, ehelyett inkább újraindítással és más beavatkozással próbálkoznak, pedig minden egyes laikus művelet ront az adatmentés esélyein.

Érdemes tisztában lenni azzal is, hogy nincs olyan adattároló, amelyik örök időkig működőképes lenne. A merevlemezek (HDD-k) mintegy 10%-a előbb-utóbb meghibásodik; a hibák 32%-a emberi, 44%-a mechanikai okból következik be.

Az ún. flash adattárolók előnye, hogy kevés energiát fogyasztanak, nagy sebességre képesek, és nincs bennük mozgó alkatrész. Ezzel szemben a megbízhatóságuk korlátozott, mert a töltések jelentős része 5 év alatt megsemmisül – emiatt ezek az eszközök nem alkalmasak hosszú távú adattárolásra.

Hogyan kezeljük jól az adathordozóinkat? A fentiek alapján kijelenthetjük, hogy tökéletes adattároló nincs, jó módszer azonban van: az a jó megoldás, amelyik nem függ az adathordozótól. A legfontosabb, hogy legalább egy, de inkább kettő vagy több, különböző helyen őrzött, naprakész másolatunk legyen. A mentéseket időről időre ellenőrizni kell. Felhőben is lehet tárolni az adatokat, de csak azokat, amelyek mások számára nem értékesek.

Sándor Ákos, a *Szegedi Tudományegyetem Klebelsberg Könyvtárának* osztályvezetője az egyetemi könyvtár adatvédelmi gyakorlatáról és saját tapasztalatairól számolt be. Az egyetemi könyvtárakban általában hálózati meghajtókon és lokális gépeken is tárolnak különböző adatokat; a szolgáltató szervereken érhetők el az adatbázisok és a digitalizált állományok, emellett működtetik az elektronikus levelezőrendszert stb. Egy kívülálló nem is hinné, hányféle feltételnek kell az egyetemi könyvtári rendszernek megfelelnie. Többek között személyes adatokat is kezelnek, ezekhez azonban csak az arra jogosultak férhetnek hozzá. Egyúttal ez azt is jelenti, hogy a helyi hálózaton vannak a külső behatolás ellen fokozottan védendő gépek és adattárolók.

Sokféle lokális berendezés működik a hálózaton: kliens gépek, mobil eszközök, hálózati aktív eszközök stb. Az épületen belüli wifire nemcsak laptopokkal, de mobil eszközökkel is föl lehet csatlakozni. Szegeden a publikus gépek számához képest kb. háromszor annyi lett az összes csatlakoztatott eszköz, de a hallgatók még tovább is osztják

a wifi kapcsolatot – és ez számos szolgáltatási problémát okoz.

A publikus kliens gépeken minden műveletet naplóznak, és bizonyos szituációkat elemeznek. Előfordult már, hogy valaki adathalász szoftvert akart telepíteni. A rendszergazdák számára távoli bejelentkezésre is kell lehetőséget biztosítani, hogy szükség esetén be tudjanak avatkozni. Volt olyan eset, hogy péntek délután egy óra alatt ezer bejelentkezési kérés futott be. Közvetlen kárt ugyan nem okozott, de az erőforrásokat nagyon lekötötte.

A sok éves tapasztalat alapján néhány gyakorlati tanács: a jelszócsere nagyon fontos, ezt be kell tartatni a kollégákkal. Folyamatosan vizsgálni kell a szervereket és az adattárolókat. A külső támadások ellen egy lehetséges megoldás a „gép a gépben” – ez esetben kívülről, a megfelelő jogosultság nélkül csak egy konténerbe lehet bejutni.

Meg kell határozni a védendő adatok és eszközök körét, szabályozni kell a védelmet biztosító személyek hozzáférési jogosultságát, definiálni kell a hálózat adta lehetőségeket, illetve a használatból fakadó veszélyeket. Biztosítani kell a problémák megelőzésére szolgáló időt és energiát, a rendelkezésre álló tudást, a szabályozási és ellenőrzési mechanizmust. Elemezni kell a felmerült biztonsági problémákat, ezek okát és megoldását. Fel kell készülni a jövőbeli problémák időben történő felismerésére, lehetőleg megelőzésére. Folyamatosan monitorozni kell a rendszert, cselekedni a biztonságért – emellett nagyon fontos a mindenre kiterjedő dokumentálás.

1. Első helyen az adatvédelmi tudatosság erősítése áll: biztosítani kell a szervezeten belüli szakmai felkészültséget.
2. Az adatkezelés kritériumainak felülvizsgálata során át kell tekinteni az adatkezelés célját és szempontrendszerét, a személyes adatkezelés koncepcióját, továbbá a kezelt adatok tárolását, időtartamát stb.
3. Fontos az érintett(ek) megfelelő tájékoztatása, melynek keretében biztosítani kell az információs önrendelkezési jog érvényesülését, tekintettel az érintett(ek) jogaira.
4. Az érintett(ek) jogaira és a jogok érvényesítésére vonatkozó szabályok tisztázása.
5. Az adatkezelés jogalapja: tekintsük át a szervezetben zajló adatkezelési tevékenységet, majd az új szabályozás által meghatározott jogalapokhoz igazodva biztosítsuk az információs önrendelkezési jog érvényesülését.
6. A gyermekek jogainak kiemelt védelme: amennyiben szervezetünk gyermekek személyes adatait is kezeli, kiemelt figyelmet kell fordítani az adatvédelmi rendeletben az információs társadalommal összefüggő szolgáltatásokra megállapított, a gyermekek adatainak kezelésére vonatkozó szabályokra.
7. Az adatvédelmi incidens bejelentése: az új szabályok értelmében a személyes adat jogellenes kezelése vagy feldolgozása esetén az intézmények kötelesek az incidenst 72 órán belül bejelenteni a felügyelő hatóságnak, vagyis a NAIH-nak. A bejelentési kötelezettség elmulasztása jelentős bírsággal jár.
8. Beépített adatvédelem, előzetes adatvédelmi hatásvizsgálat: az új szabályok értelmében bizonyos esetekben az adatkezelőnek az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell lefolytatnia, és tovább erősödik a beépített adatvédelem követelménye is.
9. Új szabályok lépnek életbe, amelyek megszabják, hogy mely adatkezelőknek és adatfeldolgozóknak, mely esetekben kell adatvédelmi tisztviselőt kijelölniük.
10. Az új uniós rendelet meghatározza a személyes adatok harmadik országba történő továbbításának a feltételeit.
11. Az egy tagországon belül működő intézmények a nemzeti adatvédelmi felügyeleti hatóság illetékessége alá tartoznak. A több országban működő szervezetek esetében tisztázni kell, melyik hatóság felügyelete érvényes rájuk nézve.

Sziklay Júlia, a *Nemzeti Adatvédelmi és Információszabadság Hatóság* (NAIH) főosztályvezetője „Az új uniós adatvédelmi rendelet – kihívás és lehetőség” címmel tartott előadásában először arra a kérdésre adta meg a választ, hogy miért volt szükség az Unióban a legmagasabb szintű szabályozásra, az új uniós rendeletre?[1] A cél az adatvédelmi gátak lebontása volt; a korábbi szabályozás ugyanis korlátozta az uniós termékekhez és szolgáltatásokhoz való szabad hozzáférést. 2018.

[1] General Data Protection Regulation (GDPR), az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679

május 25. után kötelező lesz alkalmazni a tagországokban a szilárd, következetesebb jogi keretet biztosító uniós rendeletet, amelyet nem kell implementálni a nemzeti jogszabályok közé.

Valamennyi intézménynek, vállalkozásnak fel kell készülnie az uniós adatvédelmi rendeletben foglaltak teljesítésére. Az előadó pontokba szedve ismertette a szempontokat:

Kérdezhetnénk, mi közük van a könyvtáraknak az új adatvédelmi rendelethez? A válasz egyértelmű: ezek az intézmények is kezelnek személyes adatokat – saját munkavállalóik, illetve a könyvtárlátogatók adatait kezelik; ezen túlmenően esetleg még felhasználói profilokat is készítenek stb. Az iratok digitalizálása és a tartalomszolgáltatás során is gyakori a személyes adatok kezelése – bár ez inkább a levéltárakra jellemző.

Fontos tudni, hogy a bizonyítási és megfelelési teher az adatkezelőre hárul. Alapvető követelmény: biztonságos, jogszerű módon kell kezelni az adatokat, és az érintetteket megfelelő módon kell tájékoztatni arról, hogy milyen jogcímen, mely adataikat, mennyi ideig tárolják, esetenként kinek, milyen feltételekkel továbbítják.

A NAIH lehetőséget ad arra, hogy egy konzultáció keretében az adatkezelők előre tisztázzák a kérdéseket, pontosítsák a rájuk háruló kötelezettségeket.

Dancs Szabolcs, az *Országos Széchényi Könyvtár* (OSZK) *E-szolgáltatási Igazgatói Titkárság* főtanácsosa „A hiteles digitális másolat a könyvtáros szemével” című előadásában arra fókuszált, hogy milyen szerepet kap az adatmegőrzés a kulturális örökség átmentése során, mit jelent a digitalizálás kérdéskörében a hitelesség, a hiteles adatszolgáltatás és -megőrzés, illetve milyen technikai lehetőségek vannak a hiteles információszolgáltatás biztosítására.

Viktor Mayer-Schönberger, a „Big data” című könyv egyik társszerzője szerint a jelenlegi, posztfaktuális korban különösen fontos szerep jut a könyvtáraknak, amelyek a tényeken alapuló, valódi tudást szögezik szembe az alternatív (kreált) valósággal. Ennek következtében a könyvtárak legfontosabb versenyelőnye a hitelesség.

A könyvtárak számára célként fogalmazódik meg a hiteles forrásanyag nyújtása a tudományos igényű kutatás számára – ehhez járul a reprodukálhatóság követelménye.

2. ábra **Az IFLA az álhírek ismérveiről**

A hitelességet a következőképpen lehet megfogalmazni: az eredeti (analóg) objektumok tulajdonságait a lehető legnagyobb mértékben tükröző, a bennük lévő tartalom közvetítése szempontjából helyettesíteni képes digitális korpusz létrehozása, amely magában foglalja a teljes tipográfiai (vagy egyéb technológiával történő) kivitelezést (szöveg, illusztrációk, az egyes elemek külalakja és elrendezése stb.) is. A másodlagos cél a hiteles digitális korpuszra épülő, az általános társadalmi információigény kielégítését célzó egyéb szolgáltatások kialakítása: példányok és/vagy gyűjtemények virtuális rekonstrukciója stb.

Létezik egy kvázi szabvány, a digitális hasonmás elismerő pecsét (Digital-Surrogate Seal of Approval – DSSOA), amely azt jelzi, hogy a digitális változat pontos és teljes értékű helyettesítője az eredeti statikus, analóg objektum tartalmának és külalakjának. Alapkövetelmény a teljesség – vagyis az, hogy az eredeti dokumentum minden oldalát teljesen és tökéletes minőségben reprodukálták, továbbá a pontosság – vagyis, hogy a másolat megőrizte az eredeti elrendezést és külalakot. Azokra a digitális másolatokra, amelyek megfelel-

nek a követelményeknek, kiadható egy megfelelőségi igazolás.

Az USA-ban a legnagyobb könyvtárak, az *Igazságügyi Minisztérium*, a *NASA* és további szervezetek részvételével kidolgozták az ún. FADGI-irányelveket (Federal Agencies Digital Guidelines Initiative) a kulturális örökség körébe tartozó objektumok digitalizálására. Az irányelvek három eleme:[2]
- műszaki irányelvek és paraméterek;
- jó gyakorlatok;
- a digitális képek megfelelőségének értékelése (Digital Imaging Conformance Evaluation – DICE).

A metaadat-szolgáltatás feladata a hiteles, ellenőrizhető információk nyújtása. A digitális megőrzéshez szükséges metaadatok *Dappert* és *Enders* szerint:
- a *leíró metaadat* az intellektuális entitást írja le (pl. szerző és cím);
- a *strukturális metaadat* a fizikai relációk leírására szolgál;
- a *technikai metaadatok* tartalmazzák a műszaki információkat;
- az *adminisztratív metaadatok* közé tartoznak a történeti kontextusra vonatkozó ún. provenienciaadatok, a hozzáférési jogok és engedélyek stb.

A PREMIS (Data Dictionary for Preservation Metadata), a digitális objektumok megőrzésének és hosszú távú használhatóságának támogatására fejlesztett nemzetközi metaadatszabvány az adminisztratív és technikai adatokra fókuszál és szorosan kapcsolódik az *Open Archival Information System* szabványhoz.

Dancs Szabolcs végezetül ismertette azt az új szemléletű bibliográfiai leírási szabályzatot, amelyet a jövőben az OSZK használni fog. Az FRBR (Functional Requirements for Bibliographic Records) előnyei a jelenleg használatos HUNMARC szabványhoz képest: a strukturált, jelentést hordozó/jelentéstartalommal bíró, szemantikus adatok megfelelő algoritmusokkal összegyűjthetők és megjeleníthetők.

Drucker György, az OSZK E-szolgáltatási Igazgatói Titkárság projektmenedzsere az „Adatvédelmi kihívások az Országos Könyvtári Rendszer fejlesztésében” című előadását a globális tendenciák elemzésével kezdte, majd áttért az informatikai szektorban lejátszódó paradigmatikus változásokra – köztük a robotizációra. A könyvtárosi szakma valahol a középmezőnyben van a tekintetben, hogy egyszer majd robotok váltják föl a könyvtári munka bizonyos részét, például a raktári kiszolgálást vagy az adatfeldolgozás egy részét.

A növekedés és a hálózatosodás legnagyobb motorja – nemzetközi szinten is – a munkamegosztás és az együttműködés erősödése. A fejlesztések során kollaboratív platformban, nem pedig elkülönült rendszerekben kell gondolkodni. A digitális korszak kulturális javait ne az analóg korszakból származó adatstruktúrákkal akarjuk leírni. Használni kell az új koncepciókat, amelyekkel hatékonyabban megvalósítható a webes korszak és a digitális jószágok nyilvántartása és kereshetősége.

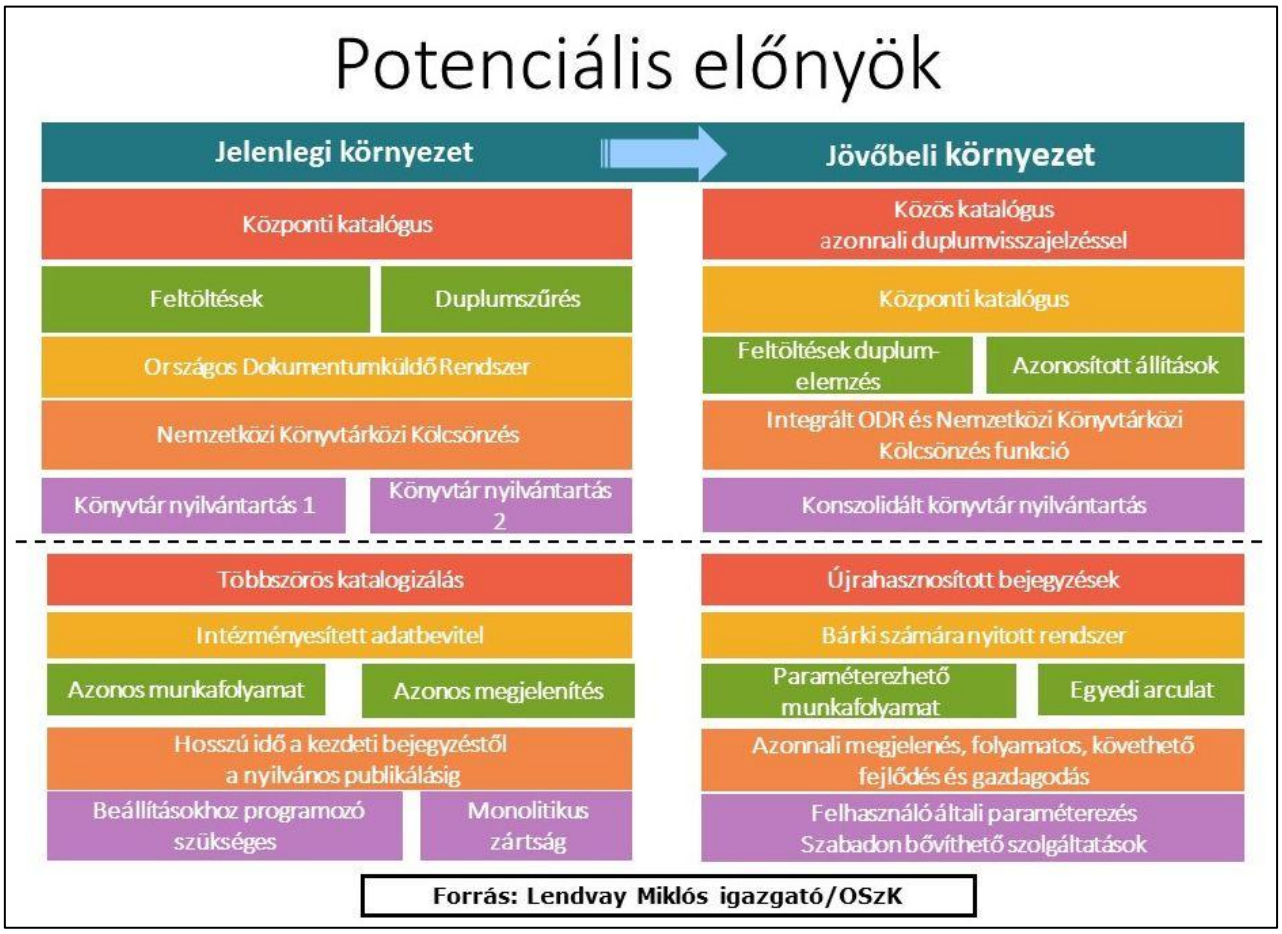
A nemzeti könyvtár régóta igen nehéz körülmények között működik. A legnagyobb gondot a szétaggolt és alig fenntartható adatbázisok tömege, a nem szabványos és nem támogatott alkalmazások sokasága, az erősen amortizált infrastruktúra, illetve az általános intézményi konszolidáció égető szüksége jelenti. Több mint 80 elkülönült adatbázist működtetnek, az átlagos eszközélettartam 8 év, de vannak 15 éves gépek is a hálózaton.

Az *Országos Könyvtári Platform* (OKR) projekt (*3. ábra*) eddig soha nem látott ígéretekkel kecsegtet. Az OKR célja egy több könyvtár által használható rendszer, illetve szolgáltatási platform kialakítása, amely alkalmas arra, hogy:
- egyes könyvtárak saját könyvtár-automatizálási rendszereként működjön,
- biztosítsa az adatbázisok, a katalógusok és a központi szolgáltatások kezelését,
- biztosítsa az analóg és digitális objektumok adatainak egységes kezelését,
- a dokumentumokat a használók az integrált szolgáltatások keretében vehessék igénybe,
- a különböző névtér-rendszerekkel, kiemelten a Magyar Nemzeti Névtérrel együttműködjön,
- nem partnerkönyvtárak is használhassák a rendszer bizonyos szolgáltatásait.

Az OSZK-ban egy digitalizáló üzemet alakítanak ki, ahol a 30 telepített eszközzel 40-60 munkatárs fog dolgozni. A digitalizálást támogató keretrendszer az egész országban folyó könyvtári digitalizálási projekteket is ki fogja szolgálni. A műhelyben állományvédelmi szempontú és szolgáltatási célú digitalizálás egyaránt folyik majd.

A nagy érdeklődés mellett tartott rendezvény prezentációi elérhetők az EKE honlapján.

[2] A FADGI-irányelvekről bővebben ld. Dancs Szabolcs cikkét a 3K 2017. októberi számában.



3. ábra **Az OKR-ben tervezett együttműködés potenciális előnyei**

Tószegi Zsuzsanna PhD
(c. egyetemi docens
ELTE BTK Könyvtár- és
Információtudományi Intézet)