DIGITÁLIS ARCHÍVUMOK MEGVALÓSÍTÁSÁNAK BIZTONSÁGI ALAPKÉRDÉSEI

Erdősi Péter CISA, e-mail: erdosi@itm.bme.hu
Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035

Kulcsszavak: elektronikus adattárolás, digitalizálás, informatikai biztonság

Napjainkban tanúi lehetünk a digitális világ egyre gyorsabb fejlődésének, az elektronikus iroda, az elektronikus iratok elterjedésének. Egyre erősebb az igény az eddig csak korlátozott helyen és időben hozzáférhető adatok, dokumentumok, információk digitalizálására, és a digitális változatok közzétételére, széleskörű elérhetőségének biztosítására mind a jelenben és a jövőben is – azaz nem kevésbé fontos, hogy ne csak a létrehozására, hanem a megőrzésre is koncentráljunk.

A digitális archívumok (a cikkben széles értelemben inkább **digitális adathalmaz**okat értünk „archívumok" alatt) megvalósításának azonban számos alapkérdése van, ami meghatározza a végeredmény minőségét, megbízhatóságát és biztonságát egyaránt. Az előadás ezekből az alapkérdésekből ragad ki önkényesen hármat, melyek az előadó szerint alapvető fontosságúak a digitális tartalmak közzétételében.

Az előadás három fontos kérdést boncolgat elméleti aspektusból a digitális adathalmazok vonatkozásában – a harmadik kérdésre kihegyezve a választ:

1. Mit tárolunk digitálisan, a világ mely részét?
2. Mit nyerünk és veszítünk a(veszteséges) tömörítési eljárásokkal?
3. Milyen mértékben kell a biztonsággal foglalkozni digitális adattárolás esetében?

Az előadásban az alábbi munkadefiníciókat alkalmazzuk:

- Információ$_A$: a rendelkezésünkre álló eszközökkel érzékelhető világnak egy jól körülhatárolt, adott tulajdonságokkal bíró eleme, ténye, analóg;
- Adat$_D$[1]: binárisan ábrázolt információ vagy az információnak egy része; digitális.

Az előadás a fenti kérdéseket járja körbe, a kérdésekhez kapcsolódó válaszokkal és azok következményeinek feltárásával együtt. Jelen keretek között nem foglalkozunk azzal a kérdéssel, hogy vajon honnan és mik kerülnek bele a tárolóba – a követelményeket oly módon próbáltuk megfogalmazni, hogy az érvényességüket ez ne befolyásolja.

Az adatok digitális tárolásának problematikájának tárgyalásában szükségesnek véljük a rögzítendő halmazok (digitalizálandó) és a rögzített halmazok (digitalizált) fogalmi szétválasztását, mivel arra akarunk bizonyítékokat keresni, hogy a kettő nem egyezik meg. Mielőtt elkezdenénk a kérdéseket tárgyalni, ezért fogadjuk el az absztraktban rögzített Információ$_A$ és Adat$_D$ definíciók érvényességét jelen kontextusra nézve, – elképzelhető, hogy érvényességük túlmutat ezen – itt azonban a kivetülésükkel nem foglalkozhatunk.

[1] Az alsó indexek használatával kívánjuk azt jelölni, hogy a továbbiakban ezeket a szavakat nem a máshol megszokott értelemben alkalmazzuk.

2. Mit is digitalizálunk és mit veszthetünk a digitális archiválás lépései során

2.1. Digitalizálás – az észlelés vesztesége

A világ digitális érzékeléséhez segítségül hívjuk a mesterséges intelligencia kutatások ágenseit (agent). Az ágensek szenzoraikon keresztül észlelik a környezetüket, dönthetnek valamely cselekvés elvégzése mellett, és manipulátoraikkal meg is változtathatják a környezetük állapotát (gondoljunk például a takarító-automatákra) – ez újabb észleléssel láthatja el az ágenst.

A digitalizálás szempontjából a digitalizáló eszközöket ebben a cikkben felfoghatjuk egy ágens szenzorainak is, amiből következik, hogy a környezet definiálása itt is értelmezhető tevékenység lehet. Abban az értelemben nem teljesen jó az analógia, hogy az ágens cselekvése itt nem értelmezhető a környezete függvényében, azaz eléggé korlátozott feladatú ágens – ha egyáltalán tekinthető annak – egy digitalizáló eszköz.

A lehetséges környezetek osztályozását [7] az alábbiak szerint végzi el:

- **hozzáférhető környezet**: amikor az ágens minden állapotot érzékelni képes, a helyes döntés végrehajtásához.
- **determinisztikus környezet**: amikor a környezet következő állapotát a jelenlegi állapota és az ágens cselekvése egyértelműen meghatározza – ekkor elvileg nem kell bizonytalanságokkal törődni.
- **epizódszerű környezet**: az ágens tapasztalatai epizódokra bonthatóak, így nem kell az ágensnek előre gondolkodnia.
- **statikus környezet**: ha a környezet megváltozhat, amíg az ágens gondolkodik, akkor beszélünk dinamikus környezetről ellenkező esetben a környezet statikus. Szemidinamikus egy környezet akkor, ha az nem változik az idő múlásával, de az ágens teljesítménye igen.
- **diszkrét környezet**: ha az észlelések és a cselekvések halmaza világosan definiált és jól elkülöníthető véges elemű, akkor a környezet diszkrét, ellenkező esetben folytonos.

A környezetek osztályozásából kitűnik, hogy – ha tekintünk egy digitalizálást végző eszközt és annak környezetét – nem mindegy, mi a digitalizálás tárgya, a rögzítendő információhalmazok változásával az érzékelőknek is más tulajdonságokkal kell bírniuk. Felmerülhet a kérdés, hogy milyen információkat vagyunk képesek rögzíteni (adattá átalakítani) és miket nem? (Egyes szóhasználatban fordítva is használatos a kérdés: milyen adatokat alakítunk információvá…) Általánosan érvényes válaszunk nyilvánvaló módon nincs erre a kérdésre, csupán gyakorlatias: azt tudjuk rögzíteni, amit a rögzítő eszközünk észlelni képes, vagy aminek az észlelésére utasítottuk. Így például egy papír fénykép digitalizálásánál nem biztos, hogy kíváncsiak vagyunk a kép hőmérsékletére, 0,5 cm távolságban mért relatív páratartalomra vagy a légnyomásra, azonban mindezek az adatok egy meteorológiai megfigyelésben nélkülözhetetlennek látszanak – szemben például a szemközti fa lombkoronájának zöld színárnyalata meghatározásával, amik egy másik szempontú megfigyelésben játszhatnak fontos szerepet. [7] megfogalmazza, hogy elegendő finomságú felbontásban a folytonos környezetek is átmennek diszkrétbe. A folytonosságot az ágens absztrakciós képessége jelenti és őrzi meg – ettől a mélységtől.
Az analóg információk diszkrét ábrázolása önmaga is veszteségesnek tűnik, hiszen nem minden bemeneti analóg feszültségi állapothoz tartozik a kimeneten egy digitális érték (az AD konverterek működéséből kiindulva) – ha a bemenet ténylegesen folytonos.

Tegyük fel például, hogy egy kamera 25 képet továbbít másodpercenként. Ebből az következik, hogy a 25 kép közötti információk elvesznek a rögzítés szempontjából – ezt nevezzük cikkünkben most az **észlelés veszteségének**. Ha a rögzítendő képmennyiséget – példánknál maradva – 1000x1000 pixel képmérettel, 8 bites színmélységgel és 8-bites intenzitás-információval számolva tároljuk, akkor óránként majdnem 5 és ¼ gigabájt mennyiségű adatunk keletkezik. A heti és havi adatmennyiség – folyamatos rögzítést feltételezve – 3,7 illetve 45,2 terrabájtra rúgna körülbelül.
Példának okáért ha akkor vagyunk teljesen elégedettek egy történés képi rögzítésével, ha másodpercenként nem 25, hanem 100 képet kapunk (100%), akkor a másodpercenkénti 25 képpel veszteségünk 75% - így (folyamatos mértékű) elégedettségünk 25%, és elégedetlenségünk mértéke is megegyezik a veszteség értékével.
Ekkora mennyiségű adat tárolása tömörítés nélkül a gyakorlatban nehezen képzelhető el.

2.2. Tömörítés – a tárolás vesztesége

Az információk tárolásához a fentiekből következően sok tárolási kapacitás, sok-sok digitális bit szükséges. A tárolás hatékonyságát növelhetjük, ha a tárolandó adatmennyiséget valamilyen tömörítési eljárással csökkentjük. Kétféle eljárást alkalmazhatunk: veszteséges és veszteségmentes tömörítési eljárást.
A tömörítési eljárásoknál a veszteséges számunkra az igazán érdekes. Arra a kérdésre keressük a választ, hogy mit veszítünk el a tömörítésnél? Ha rákeresünk a világhálón a veszteséges tömörítésre, kapunk eredményeket mind a mozgófilmek, mind a képek és a hangok területén is. A veszteség megfelelőségét ezekben az esetekben – úgy tűnik – az emberi észlelés határai jelentik, azaz amíg élvezhető a tömörített állomány, addig jónak mondható a tömörítés.
Az eredeti állományokhoz képest több a bizonytalanság a tömörített képekben, tehát információ vesztés minden esetben bekövetkezett. A különbséget ott lehet megfogni, hogy míg egyes esetekben az egyértelmű (azaz a hibahatáron belüli) információ-visszanyeréshez szükséges információk is elveszhetnek (romlik a használhatóság), addig más esetekben ezek megmaradnak, és az elveszített részek az ezen kívüli információkból hiányoznak – de ezek a működőképességet, hatékonyságot érdemben így nem befolyásolják.

3. Biztonság – a szükséges rossz?

3.1. Informatikai biztonsági követelmények

Miért kell a digitális adattárolásnál biztonsággal foglalkozni? Ha belegondolunk abba, hogy mit is tartalmazhat, vagy hogyan tartalmazza az információkat az adathalmaz, elképzelhető olyan válasz, ami a széles körben való megismerhetőséget korlátozná akár az adat jellege miatt (pl. személyes adat) akár az információ rendszerezettsége miatt. El tudunk képzelni egy olyan digitális információtárolót működés közben, mely nélkülözi a biztonság minden elemét? Egy gazdálkodó szervezetben keletkezhetnek olyan információk is, melyek védelmét jogszabály írja elő (titok). Ezek a felvetések a bizalmasság témakörébe tartoznak. Következő kérdésünk az lehetne, hogy mi garantálja azt, hogy az adatok információtartalma nem módosul, és ugyanazt adja vissza a tároló, amit benne feldolgoztak, elraktároztak – más szóval a sértetlenségre nézve is lehet garanciákat követelnünk egy ilyen rendszertől. Tovább fűzve a dolgot, kell maga a rendszer is, azaz működjön ott és akkor, amikor arra a lekérdezőnek szüksége van. Ezzel eljutottunk a rendelkezésre állás biztosításához is. Elvárható-e egy digitális adattárolótól – netán szükséges tulajdonsága-e -, hogy informatikai katasztrófa-helyzetben is működjön, és egy – a működésre nézve – katasztrofális esemény se vezessen a tárolt információk megsemmisüléséhez – különösen, ha az eredeti

információhordozó esetleg már nem is létezik. Mindezeket egy szóval úgy is mondhatjuk, hogy az elektronikus adatok tárolásának informatikai biztonságát is fel kell vetni kérdésként a tervezés és a működtetés során.

Az egyes informatikai biztonsági követelmények pontos meghatározásához először definiáljuk az „informatikai biztonság" fogalmát [1]:

INFORMATIKAI BIZTONSÁG (information security) – az informatikai biztonság az informatikai erőforrások biztonsága.

Biztonságon tehát az erőforrások bizalmasságának, sértetlenségének és rendelkezésre állásának minimális fenyegetettségét értjük, azaz egy olyan kedvező állapotot, melynek megváltozása nem valószínű(!)[2] de nem is lehet kizárni.

- **bizalmasság**: valaminek a megismerése korlátozott (jogosult, nem jogosult)
- **sértetlenség**: valami az eredeti állapotának megfelel, teljes (megjegyezzük, hogy a hitelesség és a letagadhatatlanság itt szerepel, mint tulajdonság)
- **rendelkezésre állás**: elérhető ott (hely) és akkor (idő), amikor arra szükség van.[3]

Informatikai biztonság alatt tehát az informatikai erőforrások bizalmassága, sértetlensége és rendelkezésre állása védelmét értjük. Informatikai erőforrásokon a COBIT3 (Control OBjectives for Information and related Technology [3]) által megfogalmazottak szerint az alábbiakat értjük:

- emberek
- alkalmazások
- technológia (hardverek, operációs rendszerek, adatbázis-kezelők)
- eszközök
- **adat**

Az elektronikus dokumentumokat az „adat" kategóriába soroljuk, hiszen minden elektronikus dokumentum fájl-szinten realizálódhat – tartalomtól és formátumtól függetlenül (a feltételes módot a statikus és dinamikus dokumentumok közötti különbség indokolhatja). Az adatok feldolgozásához szükségesek lehetnek alkalmazások, melyeket egy adott technológia (operációs rendszerek és hardverek) futtat. A technológiát szakképzett emberek (skill) működtetik, megfelelő környezeti viszonyok (hőmérséklet, áramellátás) között.

A továbbiakban a tárolásra kerülő elektronikus dokumentumokkal, azaz az őket feldolgozó információ-rendszerekkel foglalkozunk. Az elektronikus adathalmazok tárolásának biztonsági követelményeit az alábbiakban fogalmazzuk meg – a megvalósításra való utalások példaként értendőek:

- **bizalmasság:** a dokumentumok hozzáférés-védelme meghatározott, kikényszerített és ellenőrzött (ezt célszerű kiterjeszteni az esetlegesen létező, forrásként vagy bizonylatként szolgáló papíralapú dokumentumokra is az előírt titokvédelmi szempontból)
- **sértetlenség**: a dokumentum a keletkezésétől nem módosult (digitális aláírás), a dokumentum keletkezésének ideje tanúsított (időbélyegzés), a keletkezése megfelelő helyen, és eszközzel (eszköz-verifikáció) történt, a digitalizálást végző a másolat tartalmának egyezőségéért felelősséget vállal (elektronikus aláírás, archív aláírás)
- **rendelkezésre állás**: az elektronikus dokumentum a megfelelő helyen (alkalmas eszköz, elfogadott és felismert formátum), és időben (hibatűrő vagy katasztrófatűrő rendszer) használható. Mindez megmarad egy vagy több technológia-váltás (hardver, szoftver csere) után is, akár évtizedekre előre vetíthetően.

[2] Nincs 100%-os biztonság.

[3] A rendelkezésre állás biztonsági értelemben használatos, tehát általánosságban véve megkülönböztetendő a funkcionalitástól, a megbízható működéstől. A rendelkezésre állás biztosítása így nem terjed ki a megbízhatóságra, funkcionális megfelelőségre.

Az elektronikus dokumentumok aláírásának kérdése további elemek integrálását teheti szükségessé az Eat. (2001/XXXV. törvény az elektronikus aláírásról) előírásai szerint, mégpedig (egyszerűsítve):

- fokozott biztonságú aláírás – írásbeliség
- minősített aláírás – teljes bizonyító erő,
- archív aláírás – hosszú távú megőrzés.

Megemlítjük, hogy minden eljárás elektronikus aláírás, mely elektronikus hitelesítés módszeréül szolgál.
Felmerül további kérdésként az elektronikus dokumentumok példányszámának kezelése. Amennyiben szükség van erre, akkor olyan technológiai megoldást kell találni, mely lehetővé teszi az elektronikusan létrejövő példányok egymástól való elkülönítését, és megakadályozza illegális példányok, másolatok keletkezését.
Összefoglalva, az elektronikus dokumentumok kizárólagos használatát, és a tárolásuk védelmét akkor tarthatjuk elfogadhatónak, ha a biztonsági követelmények a szükséges mértékben és garanciával tervezésre és kielégítésre kerülnek, és olyan folyamatokat kell kialakítani, és a megfelelő informatikai eszközökkel megtámogatni, amelyekkel biztosítható, hogy a dokumentumok biztonsága (bizalmassága, sértetlensége és rendelkezésre állása) nem sérül sem a jelenben, sem pedig a jövőben, a tárolás fennállásának ideje alatt.

3.2. A védelem megvalósítása

3.2.1. Egyes védendő adatfajták

Napjaink gyakorlatában egyre többször előfordul, hogy az adatok gyakorlatilag kizárólag elektronikus úton – leggyakrabban számítógépen – keletkeznek. Az adat további életútja korábban papírba torkollott (nyomtatás, másolás), azonban egyre több a csak elektronikus úton keletkező, feldolgozott, tárolt és selejtezendő dokumentum, melyek kezelésére vonatkozóan nincs általános érvényű iránymutatás, alapelv. Ennek a trendnek a folytatódása nagyon valószínű.
Legtöbbször a papíralapú gyakorlat valamely eleme jelenik meg elektronikus formában, és beszerzésre kerülnek dokumentum-kezelő, iktató rendszerek, amelyeknek feladata a differenciált védelmet megvalósítani.
Védendő adatfajták közé alapvetően a titkokat, a személyes adatokat és az előkészítő anyagokat sorolhatjuk be. Az Alkotmányról szóló 1949. évi XX. törvény **59. §** (1)-ja szerint a Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.
A számtalan titokfajta közül - az Alkotmány 59. § (1) bekezdésével összhangban, a Ptk. a személyhez fűződő jogok között a ***levéltitok***, a ***magántitok*** és ***üzleti titok*** megőrzését részesíti védelemben. Az üzleti titok védelménél megjelenik további követelményként az is, hogy a titokbirtokos a védelem érdekében a szükséges lépéseket megtette.
A törvényileg védett magántitoknak azok az információk tekinthetők, amelyeknek megőrzéséhez az érintett személynek méltányolható érdeke fűződik. Ide sorolhatók az ún. hivatásbeli titkok (orvosi, ügyvédi stb.) is. A magántitok körébe tartozó adatok, tények, következtetések igen sokfélék lehetnek.
Erősen valószínű, hogy bármely – kiváltképp a nem közcélú – digitálisan tárolt adathalmazokban előfordulhatnak a fentiek szerint védendő adatok, ezért indokoltnak tűnik, hogy az adattárolási rendszerek létrehozása és működtetése során is tekintettel kell lenni a védendő adatok védelmi igényeire, hiszen attól, hogy egy adat tárolásra került, a védelmi igénye nem feltétlenül változik meg, de természetesen ez is előfordulhat.

3.2.2. A hitelesség megvalósítása

A hitelesség nem más, mint az állított azonosság megerősítése. A hitelesítés tárgyai – [2] alapján – a következők lehetnek:

- *Azonosság (identity)*
  Az azonosítás egy eljárás arra, hogy megállapítsuk ki vagy mi a partner a kommunikációban. Az azonosítás vonatkozhat természetes vagy jogi *személyre* (egyén vagy szervezet), illetve *eszközre*. A KI VAGY? illetve MI VAGY? megállapítására két esetben lehet szükség:
  1. a személy számonkérhetőségének biztosításához, vagy
  2. ha bízni akarunk abban, hogy az állított személy (szervezet, eszköz) ténylegesen az, amit állítottak róla.
- *Tulajdonság (attribute)*
  A tulajdonság **egy személy, szervezet vagy dokumentum** különleges jellemzője. A tulajdonság a következőkre vonatkozhat
  1. Jogosult valamit tenni? Például egy cég képviseletében aláírhat (képviseleti jog, utalványozási jog, tranzakció végrehajtási jog)
  2. Megfelel-e valamilyen szabványnak vagy jogi követelménynek? (pl. szkennelhet)
  3. *A dokumentum adat-tartalma sértetlen,* és le nem tagadható

  A tulajdonság **egy eszköz** esetében az eszköz jogosultságát adja meg, például, hogy beléphet egy bizalmas hálózatba.

Látható, hogy az elektronikus dokumentumok hitelessége a dokumentum egy tulajdonsága, mégpedig az, hogy a dokumentum tartalma megegyezik a keletkezéskori dokumentum tartalmával, és azóta a tartalma nem módosult.

Külön problémaként jelenik meg a *migrálás* elvégzése közben a hitelesség biztosítása. Az alapelv az, hogy az archivált dokumentumok információ-tartalma nem változhat, de a formátum és a technológiai alapok változása egyes esetekben elkerülhetetlennek tűnik. Például meg kell oldani a dokumentum formátum-változása következtében fellépő problémákat (pl. DOC -> PDF). A bináris adattartalom itt megváltozik, holott a dokumentum tartalma nem változik, illetve nem szabad, hogy megváltozzon. Ebben az esetben a hitelesség folytonos megvalósítása lehet itt a feladat.

A hitelesség problematikája felmerülhet az elektronikus dokumentum archívumba való bevitelekor, és minden egyes mozgatásakor is. Az archívum működtetőjének el kell valószínűleg döntenie, hogy a *tartalom* hitelesítésére, vagy a *folyamat* hitelesítésére – esetleg mindkettőre koncentrál. A két megközelítési mód – közös alapokon de – más-más intézkedéseket kíván meg a rendszerben.

3.3. Biztonságtechnikai szabványok

A biztonság megvalósítását mindenképpen valamely szabvány vagy keretrendszer mentén ajánlatos megvalósítani, az egyenszilárdság (homogenity) elvének betartása érdekében. A biztonság területén ez fokozottan érvényes, hiszen a potenciális támadó a rendszer leggyengébb pontján fogja – a legnagyobb valószínűséggel – a támadást elkövetni. Az egyenszilárdság biztosítása módszertani alapok nélkül pedig nehezen elképzelhető. Ezért a szabványok, keretrendszerek értelemszerű felhasználásával az egyenszilárdságú informatikai biztonsági alrendszer kivitelezhető, fenntartható és ellenőrizhető. Ilyenek például:

- Common Criteria (ISO/IEC 15408)
- BS7799 szabványcsalád
- A COBIT3[4] keretrendszer

[4] Copyright © 1996, 1998, 2000 by Information Systems Audit and Control Foundation. Az Information Systems Audit and Control Foundation és az IT Governance Institute engedélyével.

4. Következtetések

Láthattuk, hogy a digitalizálás mindenképpen információvesztéssel jár, azonban ez a veszteség nem feltétlenül befolyásolja az adataink „jóságát”, megfelelőségét, használhatóságát. Mindehhez az szükséges, hogy pontosan határozzuk meg, hogy a világ mely szeletét kívánjuk digitalizálni és megőrizni a fenntartás időszakában.

A célnak megfelelő tömörítési módszer alkalmazása másrészről segíti a szükségesnek ítélt információk megőrzését, de a nem relevánsak megmaradását nem garantálja. Megnézve tömörített tárolással készült képeket, megállapíthatjuk, hogy azt sem állíthatjuk 100%-os bizonyossággal, hogy ignorálja – hiszen valamit, valamilyen mértékben látunk (különösen szembetűnő ez a nagyításnál), de ez a megállapítás már átvezet a fuzzy-logikába[5], melynek tárgyalásától jelen keretek között eltekintünk. A fejezet számos olyan kérdést is felvet, melynek további vizsgálata ígéretesnek és szükségesnek tűnhet.

Az informatikai biztonságot digitális adathalmazok esetében – a fentiek alapján – alapvető fontosságúnak tartjuk, különösen a hosszú távú megőrzésnél, és remélhetőleg sikerült rávilágítani arra, hogy biztonság nélkül nem képzelhető el még rövid távon sem sikeres digitális adattárolás – hosszabb távon pedig szinte lehetetlennek látszik egy olyan rendszer fenntartása, mely nélkülözi a környezeti változásokra való reagálás, a válaszadás képességét.

Irodalomjegyzék

[1] BME GTK Információ- és Tudásmenedzsment Tanszék Biztonság Menedzsment Kutatócsoport: Az informatikai biztonság fogalmainak gyűjteménye, AJÁNLÁS 1.0 változat; 2004.

[2] Vasvári György: Bankbiztonság, BME GTK Információ- és Tudásmenedzsment Tanszék, 2003. február

[3] Control Objectives for Information and Related Technology; http://www.isaca.org

[4] MSZ ISO/IEC 17799:2002

[5] MSZE ISO/IEC 17799-2:2004

[6] ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation; 2002.

[7] Stuart J. Russell – Peter Norvig: Mesterséges intelligencia modern megközelítésben; Panem–Prentice-Hall 1995.

[5] Fuzzy-halmazok elmélete: egy eszköz annak specifikálására, hogy az objektum milyen mértékben illeszkedik egy bizonytalan leíráshoz. Ennek hiedelem mértéke nem kétértékű (igaz vagy hamis), hanem a [0,1] zárt intervallumon tetszőleges értéket felvehet – azaz hihetjük 0,6 értékben igaznak. Ez az eszköz kiválóan alkalmas tudáshiányból fakadó bizonytalanságok kifejezésére. Ha meg tudjuk szüntetni a bizonytalanságot, természetesen az állítás igazság-értéke 0 vagy 1 lesz. Erre azonban nem minden esetben van lehetőség.