BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

A digitális állam információbiztonsága: kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban

Information security and the digital state: the role of the risk management principles in the strategic documents

Beláz Annamária
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
belaz.annamaria@phd.uni-obuda.hu

***Összefoglalás* — Napjaink szolgáltató állam modelljének elsőszámú célja az ügyfél-elégedettség növelése, ennek megfelelően a hatékony közigazgatási rendszer kiépítése. Hazánkban az elmúlt évek digitális-állam kiépítésével összefüggő fejlesztési programjai is ezt a célt szolgálták. Nem szabad ugyanakkor elfelejteni, hogy a digitális állam kiépítésekor prioritást kell élveznie az információbiztonsági szempontoknak.**

A tanulmány célja, annak elemzése, hogy milyen szerepe van az információbiztonsági kockázatfelmérési és kezelési elvek megjelenésének a nemzeti stratégiai dokumentumokban, valamint annak bemutatása, hogy jelenleg milyen formában tartalmazzák a stratégiai dokumentumok meg ezen elveket.

***Kulcsszavak*:** információbiztonság, kockázatmenedzsment, stratégiai irányítás, közigazgatás, digitális állam

***Abstract* — The aim of our modern days` on demand government is to build effective efficient and economic public administration system and to increase client satisfaction. This is why electronic governmental services, identification and authentication processes developed continuously during the past few years in Hungary. The improvement programs on digital state building supported this goal as well. We cannot lose sight of the fact that during digitalisation programs in order to build an open, safe and secure digital state, cybersecurity aspect must be a priority.**

The purpose of the study is to present and analyse the role of the risk management principles in the current Hungarian national strategies. Moreover the research will examine their coherence with international standards.

***Keywords*:** information security, risk management, strategic governance, digital state, public administration

1 BEVEZETÉS

A hálózat alapú információs rendszerek létfontosságú szerepet játszanak a társadalmak mindennapi életében. A közigazgatás modernizációja és a digitalizálódás folyamata hozzájárul ahhoz, hogy a hatósági ügyintézési feladatok bekerüljenek a hivatali épületekből az állampolgárok lakásaiba, személyes okos eszközeibe, ebből kifolyólag ezeknek a rendszereknek megbízható működése és biztonsága létfontosságú. Ugyanakkor az információs rendszerek biztonságos működését veszélyeztető támadások nagyságrendje, gyakorisága és a hatása folyamatosan erősödik.

A statisztikai adatok alapján a 2017-es év első felében globálisan közel kétmilliárd adatrekord került illetéktelen eltulajdonításra, milliós károkat okozva ezzel a köz és magánszektornak egyaránt. Az eltulajdonított adatok huszonegy százaléka (404.244.346 adatrekord) a közszektorból származik. [1] Az illegális adatszerzés mellett számos egyéb információbiztonsági támadásnak vannak kitéve a közszféra szervezetei, többek között: szolgáltatásmegtagadással járó támadás, weblaprongálás, káros szoftverek, adathalászat, kéretlen levelek, jogosulatlan hozzáférés.

A szolgáltató állam közigazgatásának információs rendszere, az abban előállított, tárolt és továbbított adatok, valamint a rendszert használó személyek és szervezetek biztonsága érdekében szükséges, hogy a magyar közigazgatás rendelkezzen azokkal a minimumképességekkel, amelyekkel a megfelelő szintű védelem biztosítható. Ennek érdekében szükséges, hogy a fejlesztési programok szerves részét alkossák az információbiztonsági szabályok, valamint a területhez kapcsolódó kockázatfelmérési és kezelési elvek, megoldások. A következőkben röviden bemutatásra kerülnek a kockázatmenedzsmenttel kapcsolatos alapvető fogalmak és elvek.

2 KOCKÁZATFELMÉRÉS ÉS KEZELÉS: ELVEK, FOGALMAK

Miért fontos a kockázatmenedzsment a közigazgatási folyamatok tervezésekor és a modernizáció során? Akkor lehet sikeres egy modernizációs folyamat, ha minél teljesebb mértékben eléri a stratégiában megfogalmazott célokat. A célok eléréséhez egyrészt nélkülözhetetlen, hogy a célok világosan legyenek megfogalmazva, mérhető, követhető legyen az akciók végrehajtása. Másrészről azonban elengedhetetlen, hogy a stratégia végrehajtói, a vezetők jó döntéseket hozzanak, minimalizálva a kudarc lehetőségét. A kockázatok egyértelmű felmérése és kezelése segít a bizonytalanság csökkentésében támogatva a döntés-előkészítést és végrehajtást.

A tudományos gondolkodás és kutatás kiindulópontját mindig a vizsgált terület fogalomrendszerének áttekintése adja, így érdemes megvizsgálni legalább a kockázat fogalmát anélkül, hogy a fogalmi keretek tisztázása kapcsán túl mélyre merülnénk a kérdésben. A kockázat, kockázatmenedzsment, kockázatkezelés, kockázatértékelés fogalmak egyaránt használatosak a köz- és magánszférában, azonban a kifejezések értelmezése nem egységes. A kockázat definíciója eltérő az egyes tudományterületek és elméletek, mint például a pszichológia, orvostudomány, közigazgatás, pénzügy, szociológia megközelítésében. [2]

„A kockázat annak lehetősége, hogy egy olyan esemény történik meg, amely negatívan hat a célok elérésére.” [3]

„A kockázat általánosságban valamilyen esemény, tevékenység vagy tevékenység elmulasztása, amely a jövőben valószínűleg bekövetkezik, és ha bekövetkezik, akkor ennek általában negatív hatása van az adott szervezet céljainak elérésre.” [4]

„A kockázat valamely cselekvéssel, vállalkozással járó veszély, kár, baj, kellemetlenség lehetősége.” [5]

„A kockázat a bizonytalanság hatása a célokra.” [6]

Ezekből a meghatározásokból is világosan látható a kockázat fogalmaknak tartalmilag közös elemei: egy lehetségesen bekövetkező esemény és az esemény hatása(i), melyek veszélyeztetik a szervezet működését, az adott feladat, projekt végrehajtását. Az információbiztonság területén, a fogalmi keretek tisztázásához, az információbiztonsági rendszer kiépítéséhez és a kapcsolódó kockázatmenedzsment feladatok végrehajtásához érdemes követni a Nemzetközi Szabványügyi Testület (International Organisation for Standardisation, ISO) egységes iránymutatásait. [7] Az ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek című szabvány tartalmazza a kockázatmenedzsment [8] alapelveit, valamint a kockázatfelmérés és –értékelés lépéseit. A következőben ezek kerülnek bemutatásra.

2.1 A kockázatmenedzsment alapelvei

A kockázatmenedzsment lényegének megértéséhez és a kockázatmenedzsment stratégiai-szervezeti szintű megjelenítéséhez elsőként tisztában kell lenni a mögöttes alapelvekkel. A kutatás során így a stratégiai dokumentumok elemzésekor nagy hangsúlyt fektettem az alapelvek vizsgálatára, keserve a kockázatmenedzsment látásmód megjelenését ezen dokumentumokban.

A kockázatmenedzsment főbb alapelvei a következők:

A kockázatmenedzsment feladata az *értékek létrehozása és védelme*. A kockázatkezelés hozzájárul a célok kimutatható eléréséhez és a teljesítmény javításához a szervezet számos területén.

A kockázatmenedzsment *minden szervezeti folyamatnak részét alkotja*. A kockázatkezelés soha sem különül el a szervezet lényego folyamataitól és feladataitól, ellenkezőleg, a stratégiai tervezéstől a projektmenedzsmenten keresztül a változások kezeléséig minden területen áthatja a szervezeti működést.

A kockázatmenedzsment *a döntéshozatal szerves része*. A kockázatértékelés hozzájárul ahhoz, hogy a szervezet vezetői megalapozott döntéseket hozzanak, hiszen támogatja a valid információn alapuló releváns döntési alternatívák kidolgozását.

A kockázatmenedzsment központi feladata a *bizonytalanság fogalmának értelmezése*, természetének explicit módon történő megfogalmazása.

A kockázatmenedzsment *rendszerszerű, strukturált és időszerű*. A strukturált kockázatfelmérési és értékelési rendszer hozzájárul a hatékonysághoz, konzisztens, összehasonlítható és megbízható adatokat eredményez.

A kockázatmenedzsment *az elérhető legpontosabb tényeken, információkon alapu*l, többek között: korábbi adatok, tapasztalat, érdekelt felek visszajelzései, megfigyelései, előrejelzései és szakértői vélemények.

A kockázatmenedzsment *szervezetre szabott*, igazodik az egyéni igényekhez. A szervezet külső és belső környezetével, valamit a kockázati profiljával összhangban kell megalkotni.

A kockázatkezelési terv *megalkotásakor figyelembe kell venni a humán és kulturális tényezőket*, képességeket, látásmódokat, valamint a szervezetben dolgozó és azzal kapcsolatba kerülő külső személyek szándékait.

A kockázatmenedzsment *transzparens és inkluzív* folyamat, a megfelelő időben és mértékben szükséges az érdekel felek, kiváltképp a döntéshozók bevonása. Így a kockázatkezelés mindig releváns, időszerű lesz, a kockázati kritériumrendszer pedig figyelembe veszi a döntéshozók nézőpontjait.

A kockázatmenedzsment *dinamikus, ismétlődő és rugalmasan alkalmazkodik a változásokhoz*. A kockázatmenedzsmentnek olyan állandó folyamatnak kell lennie, amely érzékeli a szervezetben történő változásokat és folyamatosan alkalmazkodik hozzájuk. Számításba veszi, hogy a kockázatot jelentő tényezők, események változhatnak, eltűnhetnek és jöhetnek újak.

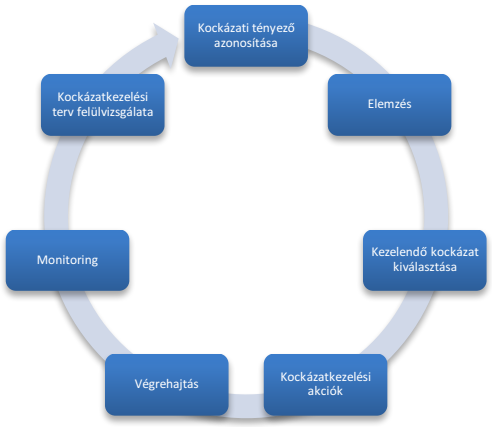
A kockázatmenedzsment *hozzájárul a szervezet folyamatos fejlődéséhez*.

2.2 A kockázatkezelési ciklus

Akárcsak a stratégiai tervezés, a kockázatkezelés ciklikus folyamat. Egyetlen szervezet sem állandó, még a kiszámíthatóságon alapuló bürokratikus közigazgatási szervezetrendszer is folyamatosan fejlődik, a belső és a külső környezete megújul. Ennek okán különböző időpontokban más és más tényezők jelentenek kockázatot egy adott szervezet számára, így a szervezeti működés fenntartása érdekében nem elegendő egyetlen alkalommal létrehozni egy kockázatkezelési tervet, majd a teendők listájáról „kihúzni”.

A kockázatkezelési ciklus a következő elemekből épül fel:

1. kockázati tényezők feltárása,
2. a feltárt kockázati tényezők elemzése,
3. a kezelendő kockázatok kiválasztása,
4. a kiválasztott kockázatokra kockázatkezelési akciók megfogalmazása
5. a kockázatkezelési feladatok végrehajtása,
6. nyomon követési és monitoring feladatok
7. a monitoring tevékenység során feltárt hiányosságok kezelése



1. ábra Kockázatkezelési ciklus elemei (saját szerkesztés)

A fogalmi alapvetés, valamint az alapelvek megismerése után a tanulmány további része a szolgáltató állam modell szerepét vizsgálja a digitális állam kiépítésével kapcsolatban.

3 A SZOLGÁLTATÓ ÁLLAMMODELL SZEREPE

Az állam és végrehajtó szervezetrendszerének szerepéről az állam- és közigazgatáselmélet területén végeláthatatlan viták folytak, s folynak napjainkig. A tudományos diskurzus során kiemelkedők azonban olyan szakaszok, ahol a közigazgatás lényegi tevékenysége sajátos karakterisztikát mutat. Napjainkban ezt a kiemelkedő szerepet a szolgáltató állam modell tölti be.

A szolgáltató állam koncepciója Max Weber szerint a kapitalizmus közigazgatásra gyakorolt hatásaként jött létre. Véleménye szerint a kapitalizmus támasztotta fel az állandó, megbízható, szilárd, hatékony, intenzív és racionálisan kiszámítható közigazgatás iránti igényt. [9]

WEBER elméletéből levezetve GAJDUSCHEK György megállapította, hogy a bürokratikus szervezetekben a kiszámíthatóság és a hatékonyság mindig egymással fordítottan arányosan van jelen, es a közigazgatás számára a kiszámíthatóság minden esetben prioritást élvez a hatékonysággal szemben. [10] Tehát a szolgáltató állam közigazgatásában, bár nagy mértékben mennek végbe modernizációs folyamatok, ezek végrehajtásakor mindig a kiszámíthatóságnak kell jellemeznie az átmenetet. A kockázatfelmérési és kezelési elvek

Todd RAMSEY A szolgáltató állam [11] című művében kifejti, hogy a szolgáltató állam, szemben a korábbi modellekkel (pl. éjjeliőr állam, jóléti állam), alapvetően proaktív, az ügyfél elvárásainak megfelelő, igény szerinti szolgáltatásokat nyújt, miközben gyakran támaszkodik a partnerekre, beszállítókra. Ramsey idézett művében a szerint határozza meg a szolgáltató államot, hogy a közigazgatási modernizáció mely ismérvek mentén zajlik. Hat egymással összefüggő ismérvet állapított meg, melyek a következők:

- a koncepció,
- a szervezeti kultúra,
- a működési modell,
- a technológiai infrastruktúra,
- az átalakítási menetrend és
- a távlatos gondolkodás.

Az információbiztonsági kockázatfelméréssel és kezeléssel kapcsolatban a legfontosabb ismérvek a szolgáltató állam működési modellje és a technológiai infrastruktúra. Egy szervezet által létrehozott értékeket a működési folyamatok adják. A szolgáltató típusú szervezetben a tevékenységek és a folyamatok a maximális ügyfélelégedettség elérésére optimalizáltak. Napjaink fejlesztési csapdája lehet azonban, hogy gyakran nem a lényegi (core) folyamatok és alaptevékenységek modernizációja, hanem a kiegészítő folyamatok és tevékenységek (non-core) fejlesztése történik meg, a kockázatmenedzsment teljes nélkülözésével. Ezért fordulhat elő az az állapot, hogy egy látszólag fejlett hivatal valójában közel áll az összeomláshoz, feladatait képtelen ellátni. [12] Fontos, hogy a technológiai infrastruktúra fejlesztése mindig a szervezet működési elveinek, folyamatainak kidolgozását kövesse.

Minél nagyobb egy állam, és minél szélesebb a feladatköre, annál jobban ki van téve a támadásoknak. Ez a megállapítás többszörösen igaz a szolgáltató állam modell tekintetében, hiszen a közigazgatás feladatköre egyre szélesebbé válik, továbbá a működés és az ügyintézés fókusza átkerül az offline térből az online térbe. A szolgáltató állam ügyfélorientáltsága tévesen elhamarkodott lépésekre ösztönözheti a jogalkotókat, azt eredményezve, hogy a digitális állam kiépítésének mihamarabbi elérése, mint cél mellett eltörpülnek az információbiztonsági, valamint az időigényes kockázatfelmérési és elemzési kérdések.

A továbbiakban vizsgálat tágyát képzik azon stratégiai dokumentumok, amelyek a digitális állami kiépítésével foglalkoznak, valamint a nemzeti biztonság kérdéseiről rendelkező szabályozások, tervek.

4 KOCKÁZATFELMÉRÉSI ÉS ÉRTÉKELÉSI ELVEK A STRATÉGIAI DOKUMENTUMOKBAN

Közpolitikai szempontból a stratégia egy meghatározott cél, állapot elérése érdekében végrehajtandó cselekvések, akciók hosszú távú terve. [13] A stratégiai dokumentum a cselekvések végrehajtása érdekében felelősöket jelöl ki, az akciókhoz erőforrásokat rendel. A stratégiai tervezés során a cél eléréséhez szükséges cselekmények részletes és módszertani szempontból következetes kidolgozása történik meg, beleértve a stratégia értékeléséhez és finomhangolásához szükséges folyamatokat is.

A Magyary-program keretében kialakításra került új stratégiai irányítási rendszer [14] azt a célt szolgálja, hogy a stratégiai szemlélet a kormányzati tervezés részévé váljon, a stratégiai dokumentumok pedig egy egységes hierarchikus rendet alkossanak. A döntéshozók és a végrehajtásban résztvevő személyek egyre inkább igénylik a stratégiai döntéstámogatás kialakítását, működtetését.

Miért fontos a kockázatkezelési elvek megjelenése a nemzeti szintű és ágazati stratégiai dokumentumokban?

Egy állam a hosszú távú céljait nemzeti stratégiai dokumentumokban fekteti le. Ezen dokumentumoknak tartalmazniuk kell a célok eléréséhez szükséges terveket, valamint az ezt megakadályozni képes kockázatokat. A közigazgatás egyes szerveinek célrendszerei csak akkor lehetnek egységesek, ha egy felsőbb szintű nemzeti dokumentum tartalmazza a fő irányvonalakat, keretrendszerként szolgál az alsóbb szintű dokumentumok elkészítéséhez. Hasonlóképpen az egyes szervezetek csupán önmagukra nézve állapíthatnak meg kockázati tényezőket, azonban egy országos szintű dokumentum átfogó képet tud nyújtani a fenyegetésekről, országos kockázati tényezőkről és mintaként szolgál az egyes közigazgatási szervek, hatóságok számára.

4.1 A digitális állam kiépítéséhez és az információbiztonsághoz kapcsolódó stratégiák

Digitális Nemzet Fejlesztési Program (NIS és Zöld Könyv)

„A jelenleg zajló Digitális Nemzet Fejlesztési Program elsősszámú dokumentuma a Nemzeti Infokommunikációs Stratégia 2014-2020 (NIS) [15] kijelölte a hazai informatikai és távközlési szektor fejlesztésének súlypontjait, és a digitális ökoszisztéma elemeinek (digitális gazdaság, elektronikus szolgáltatások, szükséges infokommunikációs infrastruktúra, az elektronikus szolgáltatásokat igénybe vevők bővítendő köre) összehangolt fejlesztését irányozta elő.

A Digitális Magyarország főbb céljai:

szupergyors internet elérhetővé tétele;

- a helyi közösségek, valamint a teljes magyar közösség összetartozásának erősítése a digitális technológia révén;
- az állam által nyújtott szolgáltatások fejlődése;
- az ország versenyképességének növelése a digitális szolgáltatások, valamint a digitális készségek terjedésének elősegítése által; valamint
- a digitális infokommunikációs alkalmazások, szolgáltatások elterjesztésének támogatásán keresztül az életminőség javítása minden élethelyzetben (magában foglalva a biztosságtudatosságra való oktatást).

A Digitális Nemzet Fejlesztési Program második kapcsolódó dokumentuma a Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól. [16] A Zöld Könyv akciótervi dokumentum, célja egyrészt a Nemzeti Infokommunikációs Stratégiában meghatározott intézkedések részletesebb kifejtése, az egyes intézkedések céljának, operatív teendőinek, becsült forrásigényének, az intézkedéstől várt eredmények és megvalósításért felelős intézmények megjelölése, másrészt a 2014-2020-as uniós tervezési ciklusban az érintett Operatív Programok keretein belül megvalósításra kerülő intézkedések koncepcionális megalapozása.

Nemzeti Biztonsági Stratégia

A magyar Kormány 2012. február 15-én fogadta el a hazai stratégiai rendszer legmagasabb szintjén álló dokumentumát, Magyarország Nemzeti Biztonsági Stratégiáját (NBS). [17] A Nemzeti Biztonsági Stratégia célja, az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése. Az elemzés alapján a stratégia meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.

Nemzeti Kiberbiztonsági Stratégia

A Nemzeti Kiberbiztonsági Stratégia [18] hivatott Magyarország kiberbiztonsági keretrendszerét felállítani és kijelölni az országos szintű kockázati tényezőket.

Logikai szempontból szoros összefüggésben áll több felső szintű dokumentummal, közvetlenül hivatkozik az Alaptörvényre és a Nemzeti Biztonsági Stratégiára, azonban nincsenek letisztázva a közvetlen kapcsolódási pontok a digitális állam kiépítésével kapcsolatban, mivel a Digitális Nemzeti Fejlesztési Program később jelent meg és a stratégiák összhangjának biztosítása nem történt meg.

Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014-2020

A dokumentum az egész közigazgatás fejlesztésére vonatkozóan határoz meg feladatokat, azzal a céllal, hogy a szolgáltató állam minél teljesebb kiépítése megvalósuljon hazánkban. A stratégia hatásterületei: a szolgáltató közigazgatás szervezési feltételeinek fejlesztése, a közigazgatás emberi-erőforrás gazdálkodásának fejlesztése, a közszolgáltatások színvonalának javítása, valamint a digitális állam felépítése.

4.2 Kockázatkezelési elvek megjelenése a digitális állam kiépítéséhez és az információbiztonsághoz kapcsolódó stratégiákban

Az alábbi táblázat összefoglalja, hogy milyen kockázatkezelési, -felmérési elvek jelennek meg az információbiztonság területén a nemzeti stratégiai dokumentumokban.

1. táblázat: Kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban (saját szerkesztés)

Kockázatkezelési elvek megjelenése a stratégiai dokumentumokban	
Nemzeti Infokommunikációs Stratégia	A dokumentum SWOT elemzés alapján megállapítja, hogy kockázati tényező az állampolgárok internetes szolgáltatásokkal szembeni bizalmatlansága. A kockázati tényezővel kapcsolatban a tudatosító programokat jelöli meg kezelési módszerként.
Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól	A Zöld Könyv a NIS biztonság horizontális tényező tekintetében kiemeli, hogy a tervezett akciók hozzájárulnak a magyar közigazgatás elektronikus információbiztonsági szintjének emelkedéséhez, egyúttal a kockázatok csökkennek.
Nemzeti Biztonsági Stratégia	A stratégia 31. pontjában elsődleges feladatként határozza meg a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérését és priorizálását.

Nemzeti Kiberbiztonsági Stratégia	A stratégia bár a 4. pontjában említi a kibertérből érkező fenyegetések és az információs hadviselés kockázatát, nem tűz ki célokat és cselekvési tervet sem állít fel a kockázatok mérséklésére. Nem említi ezen kívül a kiberbűnözés kockázatát, különböző lehetséges vállfajait, valamint Magyarország kitettségét, fenyegetettségének mértékét az egyes kiberbűncselekmények tekintetében.
Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014-2020	Bár a stratégia fő célja a digitális állam kiépítése, az akciók között nem foglalkozik a kockázati tényezők felderítésével, értékelésével. Feladatként kijelöli az internetes szolgáltatásokkal kapcsolatos biztonsági kockázatok tárgyszerű megismertetését az állampolgárokkal, azonban a tudatosító tevékenység végzésének kijelölése nem minősül kockázatkezelési elvnek.

5 Összegzés

Az irodalomkutatás, a jogszabályok és stratégiai dokumentumok vizsgálatát követően megállapítható, hogy a szolgáltató állam modell kialakulása, valamint a digitális állam kiépítésére tett erőfeszítések megkövetelnék az országos stratégiai dokumentumokban a kockázatkezelési irányelvek megjelenését, azonban sajnálatos módon a kockázatmenedzsmenttel kapcsolatos rendelkezések nem csak az információbiztonság területén, hanem teljes mértékben hiányoznak ezekből a dokumentumokból.

A kockázatkezelési szempontok mellőzése a nemzeti szintű stratégiai dokumentumokból azt eredményezi, hogy az információbiztonság területén a közigazgatásban nem alakul ki egységes nézőpont, feladat és célrendszer, így az egyes közigazgatási szervezetek kockázatkezelési tervei struktúrájukban és szemléletmódjukban heterogének, horizontális nézőpontok nem jelennek meg bennük.

A fenyegetettségek és a célkitűzések megalapozottságának érdekében országos információbiztonsági kockázatelemzés és értékelés elvégzése szükséges. Az Európai Parlament és Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS Irányelv) című dokumentum meghatározza a nemzeti kiberbiztonsági stratégiák legfontosabb témáit. A rendelkezés külön pontként jelöli a kockázatok feltárására szolgáló kockázatértékelési terv elkészítését, a kockázatkezelési elvek megjelenítését. Úgy vélem a jogszabály alapján elkészítendő nemzeti szintű kockázatértékelés és kockázatkezelési terv megoldást jelenthet a tanulmányban feszegetett problémára.

Irodalomjegyzék

[1] Gemalto Breach level index: Findings from the first half of 2017 http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[2] VASVÁRI Tamás: Kockázat, kockázatészlelés, kockázatkezelés. Pénzügyi Szemle. 2015. 1. sz.

[3] Committee of sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management — Integrated framework, 2004 http:// www.coso.org/-ERM.htm

[4] Pénzügyminisztérium, Belső kontroll kézikönyv (útmutató), 2010 http://allamhaztartas.kormany.hu/belso-kontroll-szakmai-anyagok

[5] A magyar nyelv értelmező szótára I–VII. Kötet, Akadémiai Kiadó, Budapest 1962

[6] MSZ 13073:2014 Kockázatkezelés és –felmérés. Szakszótár.

[7] ISO 31000-es szabványcsoport, magyar nyelvű címekkel:
MSZ 13073:2014 Kockázatfelmérés és -kezelés. Szakszótár
MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek
MSZ EN 31010:2010 Kockázatkezelés. Kockázat-felmérési eljárások

[8] A kockázatmenedzsment/kockázatkezelés (Risk Management) nem más, mint „egy szervezet kockázattokkal kapcsolatos összehangolt irányítási és felügyeleti tevékenységei.”

[9] WEBER, Max: Gazdaság és Társadalom, KJK, Budapest, 1987

[10] GAJDUSCHEK György: A bürokrácia jelentései; In Közigazgatás szorítóban (szerk. Horváth M. Tamás) Unió, Budapest, 1998

[11] RAMSEY, Todd: On demand government – continuing the e-governmental journey, IBM Press, Lewisville, 2004

[12] BUDAI Balázs Benjámin: Az E-közigazgatás elmélete, Akadémiai Kiadó, Budapest, 2009.

[13] STEINER, George A.: Strategic Planning, Simon&Schuster, New York, 1979, o. 12-34.

[14] A Magyary Program Stratégiai Irányítási Rendszerrel kapcsolatos intézkedési tervéről bővebb információ: http://magyaryprogram.kormany.hu/strategiai-iranyitasi-rendszer, [online], 2017, Magyaryprogram.kormany.hu

[15] Digitális Nemzet Fejlesztési Program (1631/2014. (XI. 6.) Korm. határozat)

[16] Zöld Könyv http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Zöld%20Könyv.pdf [2018-06-04]

[17] 1035/2012. (II. 21.) Kormány határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[18] 1139/2013. (III. 21.) Kormány határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról