DOI: 10.38146/BSZ.2018.2.6

NAGYNÉ DR. TAKÁCS VERONIKA

Információbiztonsági kockázatmenedzsment a Nemzeti Infokommunikációs Szolgáltató Zrt. szemszögéből

A közigazgatás fejlesztésének évszázados története során a témával foglalkozók számos alkalommal fordultak az üzleti világban bevált megközelítésmódhoz, módszerekhez, technikákhoz. A közigazgatási munkaszervezés és a teljesítményértékelés során – megfelelő transzformációval – sor került a mennyiségi (ügyintézési határidőre, meghatározott idő alatt elintézett/elintézendő ügyek számára stb. vonatkozó), majd a minőségi (az ügyfél elégedettségét célként megfogalmazó) elvárások átvételére, érvényesítésére.

A technikai, majd az informatikai, infokommunikációs eszközök[1] alkalmazása a közigazgatási tevékenység tervezése, szervezése, irányítása során újabb szempont – az adatok, információk, valamint az azt kezelő eszközök védelmének – egyre hangsúlyosabb figyelembevételét tette szükségessé. Az információvédelem követelménye nemcsak belső (szervezeten belüli), hanem a jogalkotó által megfogalmazott külső követelményként is megjelent.

A jogalkotói elvárás természetesen nem öncélú, hanem a nemzetközi tendenciákra adott válasz. Ismét egy, az üzleti világból vett példa: az Allianz Global Corporate & Specialty a vállalati kockázatokat évente kiadott felmérésében elemzi. A negyven ország több mint nyolcszáz kockázatkezelőjének és biztosítási szakértőjének bevonásával a 2016-os évről összeállított dokumentum szerint *„a kiberbiztonsági események […] bekerültek a három vezető kockázatnem közé”*[2]. Az elemzés a kiberbiztonsági események körébe sorolja a kiberbűncselekményeket, az adatokat érintő támadásokat és a számítástechnikai meghibásodásokat.[3]

Az, hogy a közigazgatási szervezetrendszer által kezelt és feldolgozott adatok – az állampolgárok, a közigazgatási szervek és a gazdasági szereplők számára is – értéket képviselnek, szakmai és jogi szempontból is elismert és

1 Jelen tanulmány a témában tapasztalható fogalmi következetlenségek tisztázására nem vállalkozik, a továbbiakban az infokommunikációs eszközök kifejezést használja.
2 Allianz Kockázati Barométer 2016. Allianz.hu, 2016. január 28., 3. o. https://www.allianz.hu/hu/sajtoszoba/kockazati-barometer-2016.html/
3 Uo. 4. o.

sokszor hivatkozott tény. Elegendő utalni a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény adatvagyon-fogalmára, vagy a későbbiekben hivatkozott szabványok vagyontárgyfogalmára. A jogszabály szerint *„nemzeti adatvagyon: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége”*[4]. A szabványok alapján *„vagyontárgy […] bármi, ami a szervezet számára érték”*[5]*;* elsődleges vagyontárgy a működési folyamatok és tevékenységek, valamint az információ (a kezelt adatok és dokumentumok, továbbá a működéshez szükséges adatok és dokumentumok), másodlagos vagyontárgy a hardver, szoftver, hálózat, személyzet, elhelyezkedés, szervezeti struktúra.[6]

Ha valamilyen értéktárgyat, vagyonelemet – jelen tanulmány tárgya tekintetében az adatokat és az infokommunikációs rendszereket – védeni szükséges, a védelmet, nem utolsósorban az eredményesség és a költséghatékonyság érdekében, meg kell tervezni. Ebben nyújthat segítséget – figyelemmel az infokommunikációs rendszerek sérülékenységére és az esetükben azonosítható fenyegetésekre – a kockázatfelmérés. A védelem megvalósítása során pedig a már azonosított kockázatok kezelése (is) történik.

Jelen tanulmány először a témával kapcsolatos alapvetéseket tekinti át, ez után az ISO/IEC 27005:2011 (E) szabvány[7] kockázatmenedzselésre vonatkozó ajánlásait ismerteti[8], kitérve a magyar információbiztonsági jogszabályokkal – az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel (Ibtv.) és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelettel (technológiai rendelet) – közös pontokra, majd néhány konkrét észrevé-

---

4 A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 1. § 1. pont, http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=133022.228523

5 MSZ ISO/IEC 27001:2006, 21. o.

6 ISO/IEC 27005:2011 (E) B függeléke, 33. o.

7 ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

8 Jelen tanulmány szabványismertetéssel foglalkozó fejezetei felhasználják a szerzőnek a 2015 decemberében, a Nemzeti Közszolgálati Egyetem *Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára* című minősített képzése keretein belül készített dolgozatának *(Egy, az Ibtv. hatálya alá tartozó szervezetnél alkalmazásra kerülő [közelebbről meg nem határozott] levelező rendszer kockázatfelmérésének végrehajtása az ISO/IEC 27000-es szabványcsoportban foglaltak alapján, figyelemmel az Ibtv. és technológiai rendelete elvárásaira)* a megállapításait.

telt, javaslatot fogalmaz meg (a hivatkozott jogszabályokra is tekintettel) a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. mint a magyar közigazgatás meghatározó infokommunikációs szolgáltatója szemszögéből.

A tanulmány hangsúlyosan a kockázatfelmérés végrehajtásának előkérdéseivel foglalkozik, a kockázatkezelés tekintetében az elméleti háttér bemutatására szorítkozik, és nem tér ki a gyakorlati megvalósítás kérdéseire. Egyrészt azért, mert amíg a kockázatfelméréssel kapcsolatos szakmai konszenzus nem alakul ki, a nem egységesen felmért és értékelt kockázatok kezeléséről több szervezetet érintő javaslatok megfogalmazása idő előttinek tűnik. Másrészt pedig azért, mert az Ibtv. a védelmi intézkedések vonatkozásában kötelezően végrehajtandó előírásokat rögzít, ami meglehetősen szűkíti a kockázatkezelés „játékterét”; szélsőséges esetben annak eldöntésére, hogy a szervezet az erőforrások hiányában még meg nem valósított védelmi intézkedéseket – a kétévenkénti biztonságiosztály-emelési kötelezettségre is tekintettel – milyen sorrendben tervezi és valósítja meg. A tanulmány szándékosan nem tér ki a technológiai rendeletben foglalt védelmi intézkedések tartalmával, teljesítésével összefüggő kérdésekre sem.[9]

A kockázatról és menedzseléséről általában

„Minden szervezet szembesül olyan külső és belső tényezőkkel, hatásokkal, amelyek bizonytalanná teszik céljai elérését, illetve a célok elérésének időpontját. Ennek a bizonytalanságnak a hatását nevezzük kockázatnak.”[10] A szervezetek menedzselik (felmérik és kezelik) a kockázatokat. A kockázatmenedzsment alkalmazható az egész szervezetre, egyes területeire, különböző szintjeire, speciális funkcióira, projektjeire, tevékenységeire.

Az előbbi mondatok az MSZ ISO 31000:2015 szabvány bevezetőjéből származnak és kellően általánosak ahhoz, hogy segítsék a téma gyors áttekintését és a tanulmány szempontjából legfontosabb gondolatok felidézését.[11]

A kockázatok tehát magukban hordozzák a bizonytalanságot, amit az egyes szervezeteknek a saját jellemzőik (céljaik és körülményeik) alapján va-

9 Utóbbi kérdéskörrel kapcsolatban lásd például Nagyné dr. Takács Veronika: Az Ibtv. és végrehajtási rendeletei alkalmazásával és alkalmazhatóságával összefüggő kérdések. Bolyai Szemle, 2014/4., 76–88. o.

10 MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek. 5. o.

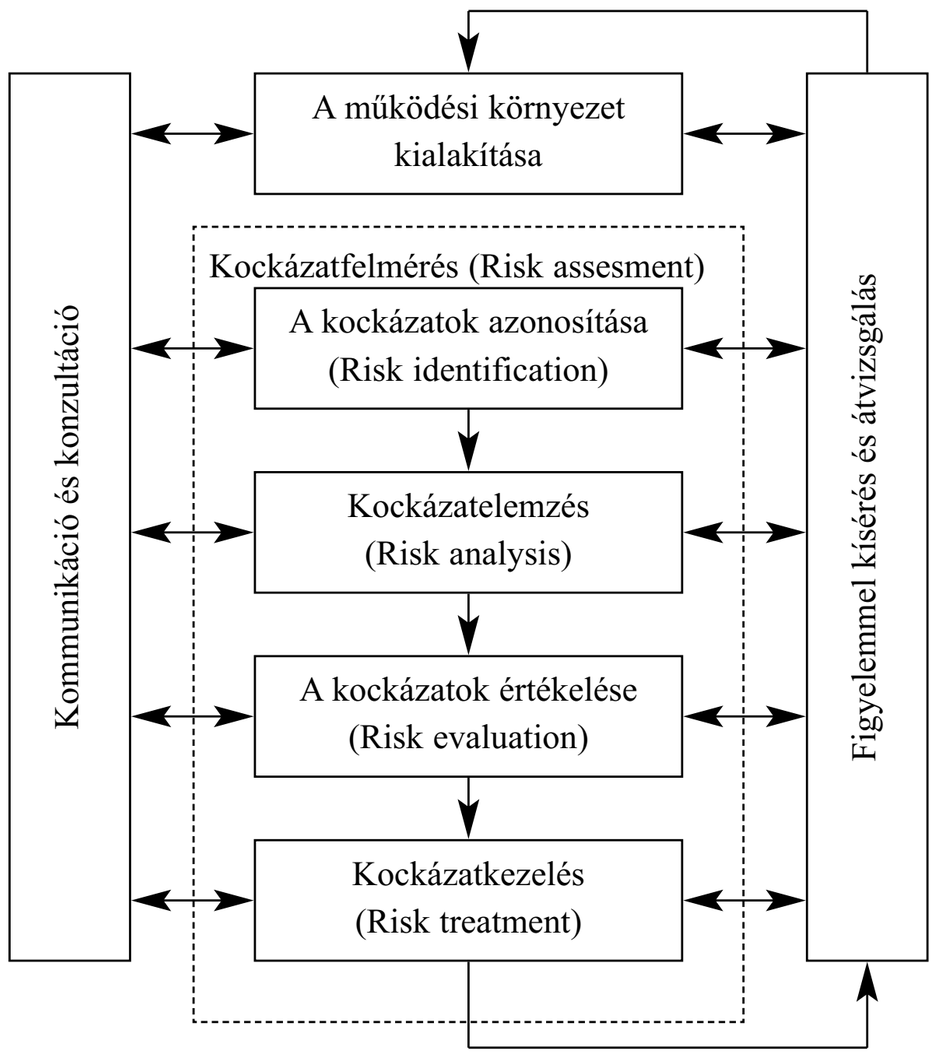
11 A kockázat számos definíciójának értékelésével, a kockázatkutatás elméletével és történetével a tanulmány nem foglalkozik. A tárgyban lásd például Vasvári Tamás: Kockázat, kockázatészlelés, kockázatkezelés – szakirodalmi áttekintés. Pénzügyi Szemle, 2015/1., 29–48. o.

lamiképpen mégis meg kell mérniük, ki kell számítaniuk és ez után kezdeniük kell velük valamit. A kockázatfelmérés az élet számos területén jelentős hagyományokat felmutató tevékenység, olykor külön szakma, kialakult módszertanokkal. Ugyanez igaz a kockázatkezelés elméletére és gyakorlatára is.

A kockázatmenedzsment folyamata – az MSZ ISO 31000:2015 szabvány alapján – az *1. számú ábrá*n látható.

1. számú ábra

A kockázatmenedzsment folyamata az MSZ ISO 31000:2015 szabvány alapján[12]



Az információbiztonsági kockázatmenedzsment a közigazgatásban

Az információbiztonsági kockázatmenedzsment célja – az előbbi definíció értelemszerű szűkítésével – az adott szervezet vagy szervezetek infokommunikációs rendszereinek tervezésével, fejlesztésével, üzemeltetésével és használatával, valamint kivezetésével összefüggő kockázatok felmérése és kezelése.

12 A szerző szerkesztése.

Az információbiztonsági kockázatmenedzsment-rendszer kialakítása, működtetése és folyamatos korrekciója az információbiztonsági irányítási rendszer kiépítésének egyik első lépése; utóbbi elméletével és gyakorlatával a tanulmány (terjedelmi okok miatt) nem foglalkozik.

Az információbiztonsági kockázatmenedzsment-rendszer kiépítése lehet egy szervezet saját döntése alapján megvalósuló tevékenysége; a magyar közigazgatási szervek és a közigazgatás működését támogató egyes nem közigazgatási szervezetek esetében – az Ibtv. óta – ez jogszabályban előírt kötelezettség.

Az Ibtv. a kockázatmenedzsment-folyamat elemeit, tartalmát nem részletezi; a technológiai rendelet a kockázatelemzési módszertan alkalmazását általában írja elő a következők szerint: *„Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.”*[13]

Jelenleg még nem áll rendelkezésre egységes, központilag kidolgozott kockázatelemzési módszertan, így minden szervezet szembesül a módszertan kiválasztásának, kidolgozásának (testre szabásának) nem könnyű feladatával.

A tanulmány a továbbiakban az ISO/IEC 27000-es szabványcsoport kockázatelemzést tárgyaló elemeit[14] ismerteti. A 27000-es szabványcsoport kiválasztása mellett szóló érv, hogy egyes tagjai magyar szabványokká váltak, így magyar nyelven is hozzáférhetők, következetes alkalmazásuk hozzájárulhat a jelenleg tapasztalható értelmezésbeli különbségek, terminológiai pontatlanságok felszámolásához, továbbá az Ibtv. indokolása is tartalmaz a szabványcsoport alkalmazhatóságára vonatkozó utalást.[15]

A szabvány rövid tartalmi ismertetésének célja nem utolsósorban az, hogy segítséget nyújtson a közös megközelítéshez, kiindulási alapot teremtsen egy

13 1. melléklet a 41/2015. (VII. 15.) BM rendelethez, 1.2. bekezdés. http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.332228

14 MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve, ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

15 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény indokolása. Részletes indokolás a 24. §-hoz.

kockázatfelmérést célzó együttműködés, tárgyalás vagy egy szakértő bevonására irányuló beszerzés előkészítéséhez. Fontos hangsúlyozni, hogy a fejezetben foglaltak nem tekinthetők kockázatelemzési módszertannak – ez a szabványnak sem célja, hiszen mindössze „keretrendszert" kíván nyújtani –, csak segítséget adnak ahhoz, hogy egy módszertan elkészíthető, vagy egy elkészített módszertan „megítélhető" legyen.

A tanulmány az Ibtv. és a technológiai rendelet előírásain túl a következő szabványokban foglaltakat alkalmazza:

– MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.
– MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.
– ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

A kockázatmenedzsment lépései az ISO/IEC 27005:2011 (E) szabvány szerint

Az *1. számú ábrá*n bemutatott kockázatmenedzsment-folyamatot részletezi és értelmezi a címben szereplő szabvány. A folyamat lépéseit és az egyes lépésekkel kapcsolatban megfontolandó legfontosabb kérdéseket a fejezet vázlatosan ismerteti a következők szerint.

1. A működési környezet kialakítása

Meg kell határozni a kockázatmenedzsment-folyamat

– külső/belső összefüggéseit és célját; ezekből következően
– hatókörét és határait;
– alapvető értékelési kritériumait és alkalmazott módszereit/megközelítést (kockázatértékelési, hatásértékelési, kockázatelfogadási kritériumok);
– felelősét és folyamatát.

A kockázatértékelési kritériumok meghatározásánál figyelembe veendő:

– a szakmai folyamatok stratégiai értéke;
– az érintett információ-vagyontárgyak kritikussága;
– a jogi, szabályozási és szerződéses kötelezettségek;

– a bizalmasság, sértetlenség, rendelkezésre állás működési és szakmai jelentősége;
– az érintettek elvárásai, véleménye;
– a szervezet presztízse, jó hírnév elvesztésének következményei.

2. A kockázatfelmérés

Választani kell a kétféle megközelítés közül:

– a magas szintű kockázatfelmérés a tevékenységek fontosságát és időrendjét veszi alapul, és mivel különböző (például pénzügyi) okokból nem lehet minden intézkedést (kontrollt) egyszerre megvalósítani, csak a legkritikusabb fenyegetésekre koncentrál;
– a részletes kockázatfelmérés mélységi értékelés, ami jelentős idő- és erőforrás-ráfordítást, szakértői tudást igényel, és amelynek során minőségi és mennyiségi jellemzők is használhatók (az előbbire példa a mérsékelt, jelentős kifejezések használata, az utóbbira például a pénzügyi mutatók).

A szabvány fontos megjegyzése, hogy idő előtti a kockázatfelmérés, ha az intézkedések bevezetését csak egy-két éven belül tervezik.

3. A kockázatazonosítás (öt azonosítási folyamatot tartalmaz)

a) Vagyontárgyak azonosítása

A szabvány – ajánlásként, azaz nem kötelező jelleggel – a következő vagyontárgyak azonosítását javasolja (vagyontárgy minden, ami a szervezet számára értéket képvisel):

– elsődleges: működési folyamatok és tevékenységek; információk (kezelt, illetve a működéshez szükséges adatok és dokumentumok);
– másodlagos: hardver; szoftver; hálózat; személyzet; elhelyezkedés; szervezeti struktúra.

b) Fenyegetések és forrásaik azonosítása

A fenyegetésekkel kapcsolatos információk beszerezhetők a vagyontárgyak tulajdonosaitól, a felhasználóktól, biztonsági, információvédelmi szakemberektől, bármilyen más forrásból (például különböző módszertanokból). A korábbi biztonsági incidensek tapasztalatai az egyes fenyegetések relevanciájának megítéléséhez nyújthatnak segítséget. Mindazonáltal ügyelni kell arra, hogy a fenyegetések folyamatosan módosulnak, különösen, ha a külső környezet vagy maga az infokommunikációs eszköz, rendszer változik.

A fenyegetések (a szabvány példálózó jelleggel több mint negyvenet nevesít)[16] eredetük szerint lehetnek az emberi tevékenységtől függetlenek (környezetiek, K) vagy az emberi tevékenységgel összefüggők, ezen belül véletlenek (V) vagy szándékosak (Sz). Az *1. számú táblázat* a szabvány által felsoroltakból néhány jellemzőbbet idéz.

1. számú táblázat

Példák a fenyegetésekre az ISO/IEC 27005:2011 (E) szabvány szerint

Típus	Fenyegetés	Eredet
Fizikai kár	Tűz	K, V, Sz
Fizikai kár	Berendezés megsemmisülése	K, V, Sz
Természeti jelenség	Földrengés	K
Információ kompromittálódása	Lehallgatás	Sz
Műszaki hiba	Berendezés rosszul működése	V
Nem engedélyezett tevékenység	Jogosulatlan adatfeldolgozás	Sz
Működés veszélyeztetése	Jogosultság nem engedélyezett átengedése	Sz

c) A létező és tervezett védelmi intézkedések (kontrollok) azonosítása

A létező vagy a tervezett kontrollok figyelembevétele munka- és költségmegtakarítást eredményezhet (például a nem indokolt intézkedések bevezetésének elkerülésével). A már létező kontrollok azonosításakor meg kell győződni arról, hogy azok valóban jól működnek, ellenkező esetben újabb sérülékenységet okozhatnak.

A szabvány által elvárt tevékenység végrehajtásához az MSZ ISO/IEC 27002:2011 szabványban felsoroltak adhatnának támpontot. Az információbiztonsági kockázatmenedzsment-rendszer kiépítéséhez a 27002:2011 szabvány 11 fejezetben 39 fő biztonsági kategóriában 132 kötelezően teljesítendő intézkedést sorol fel, az egyes intézkedésekhez bevezetési útmutatót és egyéb információt fűz. Megjegyzendő, hogy a technológiai rendelet 4. mellékletében szereplő Védelmi intézkedés katalógusban három fő csoportban (adminisztratív, fizikai és logikai védelmi intézkedések), 21 témakörben, 186 intézkedés szerepel (egyes intézkedések további alábontásokat tartalmaznak). A két kontrolljegyzék csak részben feleltethető meg egymásnak. Figyelemmel arra, hogy a jogszabály az Ibtv. hatálya alá tartozó szervek esetében kötelező, egyértelmű, hogy a technológiai rendelet katalógusában foglaltakat teljesíteni szükséges.

16 ISO/IEC 27005:2011 (E) C függeléke, 42. o.

d) A sérülékenységek azonosítása

A sérülékenység önmagában nem okoz kárt, utóbbinak feltétele, hogy a fenyegetés a sérülékenységet kihasználja. Az a sérülékenység, amelyhez nem azonosítható fenyegetés, nem igényel kontrollt (védelmi intézkedést), azonban folyamatosan figyelemmel kell kísérni, mivel e tekintetben bármikor bekövetkezhet változás. Figyelemmel kell lenni arra is, hogy egy nem megfelelően megvalósított kontroll (védelmi intézkedés) maga is sérülékenységet okozhat.

Az előzőkből következik, hogy amennyiben egy fenyegetéssel összefüggésben nem azonosítható sérülékenység, a fenyegetés nem jelenthet kockázatot. A szabvány a különböző vagyontárgyakhoz – példálózó jelleggel – több mint nyolcvan fenyegetést, illetve sérülékenységet sorol fel. A *2. számú táblázat* vagyontárgyanként egyet-egyet idéz.[17]

2. számú táblázat

Példák sérülékenységre és fenyegetésre az ISO/IEC 27005:2011 (E) szabvány szerint

Vagyontárgy típusa	Példa sérülékenységre	Példa fenyegetésre
hardver	nem védett tároló	berendezés ellopása
szoftver	tesztelés elmaradása	jogosultsággal visszaélés
hálózat	nem védett kommunikációs csatorna	lehallgatás
személyzet	biztonságtudatosság hiánya	felhasználói hiba/hibás működés
elhelyezkedés	árvízveszélyes területen elhelyezés	árvíz
szervezet	nincs vagy nem megfelelő az SLA[18]	szolgáltatáskiesés

e) A következmények azonosítása

A vagyontárgyak bizalmassága, sértetlensége és rendelkezésre állása elvesztésének következményeit kell meghatározni. Ezek lehetnek

– eredményesség csökkenése;
– kedvezőtlen működési feltételek;
– szakmai tevékenységgel összefüggő negatív hatás;
– jó hírnév elvesztése;
– kár.

A következményeket a technológiai rendelet is részletezi (ez a második, a jogalkotó által részletesebben kifejtett terület; lásd később).

17 ISO/IEC 27005:2011 (E) D függeléke, 45–48. o.

18 SLA: Service Level Agreement (szolgáltatásiszint-megállapodás; az ügyfél és a szolgáltató megállapodása a nyújtandó szolgáltatás lényeges minőségi elemeiről).

4. A kockázatelemzés (két felmérési és egy definíciós folyamatot tartalmaz)

A kockázatelemzés – a vagyontárgyak jelentőségétől, az ismert sérülékenységek és a szervezetnél korábban bekövetkezett biztonsági incidensek menynyiségétől, terjedelmétől függően – különböző részletezettséggel, mélységben valósulhat meg. A kockázatelemzés lehet minőségi vagy mennyiségi vagy a kettő kombinációja. A minőségi elemzés a lehetséges következmények nagyságának és bekövetkezési valószínűségüknek a meghatározásához skálát használ (javasolt a háromfokozatú: alacsony–közepes–magas). Előnye a könnyen érthetőség, hátránya a szubjektív skálázás.

A mennyiségi elemzés számszerűsített értékeket tartalmazó skálát alkalmaz a következmények és a bekövetkezési valószínűségek vonatkozásában, az elemzés minősége a rendelkezésre álló adatok pontosságától és teljességétől függ; előnyei és hátrányai ebből a tényből fakadnak.

a) A következmények felmérése

Az előző lépésekben végrehajtott azonosítások után a szakmai, szervezeti tevékenységet érintő következmények (hatások) meghatározására kerül sor, figyelemmel a vagyontárgyak bizalmassága, sértetlensége és rendelkezésre állása elvesztésének következményeire.

A vagyontárgyak és a bekövetkezhető hatások értékelése a folyamat legérzékenyebb szakasza, mivel különböző jellegű vagyontárgyak és különböző jellegű következmények összevetésén alapuló, egyedi értékelést tartalmaz. Az értékelés lehet minőségi vagy mennyiségi (ha az érték pénzben kifejezhető).

Az érték meghatározásának alapja lehet

– a vagyontárgy beszerzésének/előállításának költsége, helyettesítésének vagy újbóli beszerzésének/előállításának költsége vagy nem materiális érték (például szervezet elismertsége);
– a bizalmasság, sértetlenség, rendelkezésre állás biztonsági esemény miatti sérüléséből, elveszéséből eredő költségek (helyreállítási költségek, működésre, működési környezetre ható következmények).

Az azonosított vagyontárgyak értékét és a bekövetkezhető hatást a következő értékelési kritériumok szerint célszerű meghatározni:

– belső működés megszakadása;
– a szervezet által nyújtott szolgáltatás megszakadása;
– külső fél működésének megszakadása;
– társadalmi, kormányzati válság;
– jogszabályok megsértése;

– belső rendelkezések megsértése;
– szerződésszegés;
– jogi (büntető-) eljárások a szervezettel szemben;
– ügyfelek, partnerek, társadalom bizalomvesztése;
– ügyfelek, partnerek személyes adataival, személyiségi jogaival összefüggő sérelem;
– alkalmazottak vagy ügyfelek, partnerek személyi sérülésének lehetősége;
– pénzügyi, anyagi veszteségek;
– ügyfelek, partnerek veszteségei.

Az értékelési kritériumok rögzítése mellett fokozatokat is meg kell határozni (jellemzően három–tíz fokozatú skálát célszerű használni, ügyelve arra, hogy a túlzott differenciálás nehézségeket okozhat). A szabvány ötfokozatú (0–4) skálát ajánl.
Ugyancsak figyelemmel kell lenni a vagyontárgyak közötti függőségekre (például az adatok sértetlenségére vonatkozó kritérium vonatkozik az azokat kezelő rendszerelemekre is az adatok teljes életciklusa alatt, a rendszerelemek [hardver, szoftver] sértetlensége függ a környezeti biztonsági feltételek – áramellátás, légkondicionálás – teljesülésétől). Az egymástól függő vagyontárgyak esetében a magasabb értéket kell figyelembe venni.
Egyes vagyontárgyakból a szervezet több példányt (másolatot, tartalékot) is őrizhet, az értékelésnél figyelembe kell venni, hogy ezek a vagyontárgyak könnyen helyettesíthetők.
A vagyontárgyakat érhető hatások felmérése során figyelemmel kell lenni arra, hogy egy biztonsági esemény hatásának mértéke nem minden esetben azonos az érintett vagyontárgy értékével, emiatt a két fogalmat meg kell különböztetni.
A hatás lehet azonnali (működési) és jövőbeli (stratégiai). Az azonnali hatás lehet közvetlen (például helyreállítási költségek) vagy közvetett (például jogszabályok, egyéb szabályozó eszközök előírásainak megsértése).
A hatások felmérésének eredménye ugyanazon vagyontárgy esetében a későbbiekben változhat a beépített kontrollok következtében. A szabvány a hatások értékelésére ötfokozatú (0–4: nagyon alacsony–alacsony–közepes–magas–nagyon magas) skálát ajánl.
A technológiai rendelet 1. melléklete – iránymutatásként – az érték és a hatás kategóriáját összevonva a rendszer biztonsági osztályba sorolásához ad szempontokat. A szabvány nemcsak a bekövetkezhető hatások kiválasztását (azonosítását), hanem azok „skálázását” is a szervezetre bízza, így a

szabvány javaslatai alapján a technológiai rendeletből megismert „fokozatok” előzetesen nem azonosíthatók. A *3. számú táblázat* a két „segédlet” felfogásbeli különbségét is mutatja (kiemelve a mindkettőben egyértelműen azonosítható, javasolt szempontokat).

b) A bekövetkezési valószínűség felmérése

A szabvány szerint meg kell határozni a biztonsági esemény (incidens-szcenárió) bekövetkezésének valószínűségét. A felmérés történhet minősé-

3. számú táblázat

Lehetséges következmények a technológiai rendelet és az ISO/IEC 27005:2011 (E) szabvány szerint

Biztonsági osztály	Bekövetkezhető káresemény nagysága	Technológiai rendelet 1. melléklet	ISO/IEC 27005:2011 szabvány B függeléke
1.	jelentéktelen	– rendszer nem kezel jogszabály által védett adatot; – nincs bizalomvesztés, a probléma szervezeten belül marad és megoldható; – közvetlen és közvetett kár a szervezet költségvetéséhez képest kicsi.	– ügyfelek, partnerek személyes adataival, személyiségi jogaival összefüggő sérelem; – belső működés megszakadása; – ügyfelek, partnerek, társadalom bizalomvesztése; – pénzügyi, anyagi veszteségek.
2.	csekély	– személyes adat sérülhet; – működési szempontból csekély értékű adat vagy rendszer sérülhet; – társadalmi-politikai hatás a szervezeten belül kezelhető; – közvetlen és közvetett kár eléri a szervezet költségvetésének egy százalékát.	lásd 1. biztonsági osztálynál
3.	közepes	– különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek; – működési szempontból érzékeny adat vagy rendszer sérülhet; – egyéb, jogszabállyal védett adat sérülhet; – bizalomvesztés a szervezeten belül vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek; – közvetlen és közvetett kár eléri a szervezet költségvetésének öt százalékát.	lásd 1. biztonsági osztálynál, valamint: – belső rendelkezések megsértése.

Biztonsági osztály	Bekövetkezhető káresemény nagysága	Technológiai rendelet 1. melléklet	ISO/IEC 27005:2011 szabvány B függeléke
4.	nagy	– különleges személyes adat nagy mennyiségben sérülhet; – személyi sérülések esélye megnőhet; – működési szempontból nagy értékű adat(tömeg), üzleti titok vagy rendszer (jelentősen) sérülhet; – jogszabályok betartása elmaradhat; – bizalomvesztés a szervezeten belül, a vezetésben felelősségre vonást kell alkalmazni; – közvetlen és közvetett kár eléri a szervezet költségvetésének tíz százalékát.	lásd 1. biztonsági osztálynál, valamint: – jogszabályok megsértése.
5.	kiemelkedően nagy	– különleges személyes adat kiemelten nagy mennyiségben sérülhet; – emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be; – a nemzeti adatvagyon helyreállíthatatlanul megsérülhet; – az ország, a társadalom működőképességének fenntartását biztosító létfontosságú rendszer rendelkezésre állása nem biztosított; – súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek; – működési szempontból nagy értékű üzleti titok, kiemelten érzékeny adat(tömeg) vagy rendszer (jelentősen) sérülhet; – közvetlen és közvetett kár eléri a szervezet költségvetésének tizenöt százalékát.	lásd 1. biztonsági osztálynál, valamint: – társadalmi, kormányzati válság.

gi vagy mennyiségi elemzéssel. A cél annak megállapítása, hogy egy biztonsági esemény (egy sérülékenység fenyegetés általi kihasználása) milyen gyakran, illetve milyen könnyen következhet be (lásd *4. számú táblázat*).

4. számú táblázat

Lehetséges bekövetkezési valószínűségek az ISO/IEC 27005:2011 (E) szabvány szerint

Fenyegetés bekövetkezési valószínűsége	Alacsony (A)			Közepes (K)			Magas (M)		
Sérülékenység szintje	A	K	M	A	K	M	A	K	M
Incidens bekövetkezési valószínűsége	0	1	2	1	2	3	2	3	4

A felmérés során figyelemmel kell lenni a következőkre:

– a különböző fenyegetések bekövetkezési gyakoriságára vonatkozó statisztikák;
– az egyes fenyegetések forrásainak – folyamatosan változó – jellemzői (képességek, egyes sérülékenységek kihasználását érintő tapasztalatok, trendek);
– a sérülékenységek jellemzői egyenként és összegezve;
– a létező kontrollok hatékonysága.

c) A kockázati szint meghatározása

A kockázatelemzés – minőségi vagy mennyiségi – értéket rendel a kockázat bekövetkezési valószínűségéhez és következményéhez. A becsült kockázat egy biztonsági esemény (incidensszcenárió) bekövetkezési valószínűségének és következményeinek kombinációja *(5. számú táblázat)*.

5. számú táblázat

Lehetséges kockázati szintek az ISO/IEC 27005:2011 (E) szabvány szerint

		Incidens bekövetkezési valószínűsége				
		0	1	2	3	4
Vagyon-	0	0	1	2	3	4
tárgy	1	1	2	3	4	5
vagy	2	2	3	4	5	6
hatás	3	3	4	5	6	7
értéke	4	4	5	6	7	8

Alacsony kockázat: 0–2 Közepes kockázat: 3–5
Magas kockázat: 6–8.

5. A kockázatértékelés

A becsült kockázatokat a kockázatértékelési (kockázatelfogadási) kritériumok alapján rangsorolni kell, ez szolgál majd a kockázatkezelési intézkedésekre vonatkozó döntések alapjául.

A kockázatértékelés során azon fenyegetések rangsorolása történik meg, amelyek esetében

– a sérülékenység és fenyegetés együtt azonosítható; és
– nincs még intézkedés.

A kockázatértékelés során a döntések sok esetben az elfogadható kockázati szintre alapoznak, de az alacsony vagy közepes kockázatok felhalmozódása jelentősebb, beavatkozást igénylő helyzetet is kialakíthat.

6. A kockázatkezelés

Idetartoznak mindazon tevékenységek, amelyek a kockázatok csökkentését célozzák, a következők szerint:

– a megfelelő kontrollok alkalmazása (kockázat forrásának megszüntetése, a bekövetkezési valószínűség vagy a hatás csökkentése stb.);
– a kockázatok tudatos és tárgyilagos elfogadása, vállalása;
– a kockázatok elkerülése (nem kezdik el vagy nem folytatják a kockázathoz vezető tevékenységet);
– a kockázatok áthárítása, megosztása további partnerrel, partnerekkel (beleértve a szerződéskötést és a kockázatfinanszírozást).

A kockázatkezelés következtében új kockázatok keletkezhetnek vagy a korábbi kockázatértékelés eredménye változhat.

A kockázatkelés során a különböző kockázatkezelési formák nem zárják ki egymást, kombinálhatók, egy kockázatkezelési forma több kockázatra is vissza tud hatni.

A szervezet vezetői általi döntés elősegítése érdekében

– össze kell állítani a kockázatkezelési tervet, amely tartalmazza, hogyan mérték fel a kockázatokat és hogyan vetették azokat össze a kockázatelfogadási kritériumokkal;
– rögzíteni kell a maradványkockázatokat.

A szervezet vezetői általi döntés eredménye az elfogadott kockázatok listája, erre (is) tekintettel a döntést dokumentálni kell.

7. Kommunikáció és konzultáció

A kommunikáció során a kockázatfelmérés és -kezelés eredményeit meg kell osztani a döntéshozókkal és az egyéb érintettekkel, a további teendők hatékony és eredményes végrehajtása és a teendők megindokolása, elfogadtatása érdekében. Ügyelni kell arra, hogy a kommunikáció kétirányú legyen, formájában igazodjon a szervezeti kultúrához és vegye figyelembe az intézkedések sürgősségét.

8. Figyelemmel kísérés és átvizsgálás

A kockázatok nem statikusak, emiatt folyamatosan figyelemmel kell kísérni

– a kockázatokat és tényezőiket (vagyontárgyak értéke, hatások, fenyegetések, sérülékenységek, bekövetkezési valószínűségek) a változások felfedése érdekében;
– a kockázatmenedzsment folyamatát a szükséges módosítások meghatározása érdekében.

A NISZ Zrt. szolgáltatói szerepe és információbiztonsági feladatai

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. – jogszabályi kijelölés alapján – a magyar közigazgatás meghatározó szolgáltatója[19], jogelődeivel együtt fél évszázados múltra tekint vissza.

Elődei az 1964-ben alapított Konjunktúra- és Piackutató Intézet (Kopint) és az 1968-ban létrehozott Datorg Külkereskedelmi Adatfeldolgozó és Szervező Rt., amelyek összevonásával 1987-ben jött létre a Kopint-Datorg Konjunktúra-, Piackutató és Informatikai Intézet. 2005 júliusától a vállalat egyedüli tulajdonosa a magyar állam lett, azóta zártkörű részvénytársaságként működik. 2007 óta fő tevékenysége teljes körű infokommunikációs szolgáltatások nyújtása az állami és a közigazgatási szervek számára. 2008-ban a tu-

19 A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) kormányrendelet; a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) kormányrendelet; egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet; a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) kormányrendelet, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.

lajdonosi jogokat a Magyar Nemzeti Vagyonkezelő Zrt. vette át, a társaság neve 2011-től NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Legnagyobb megrendelői a közigazgatási szervek, de gazdálkodó szervezetek, vállalkozások és magánszemélyek is igénybe veszik egyes szolgáltatásait.[20]

A NISZ Zrt., mint központosított informatikai és elektronikus hírközlési szolgáltató, az Ibtv. és végrehajtási rendeletei hatálya alá tartozó szervezet, ezen túlmenően – jelentőségére tekintettel – a jogalkotó önálló jogszabályban[21] további információbiztonsági feladatokat határozott meg számára. A külön jogszabályban meghatározott feladatok között szerepel az információbiztonsági irányítási rendszer kialakítása, az infokommunikációs tevékenységgel kapcsolatos nyilvántartások vezetése (szolgáltatások, azok végfelhasználói, üzemeltetői, fejlesztői, hozzáférési jogosultságaik, a szolgáltatások biztosításához szükséges vagyonelemek, igénybe vett külső szolgáltatások stb.), külön hangsúlyt kap az azonosítási és hozzáférés-kezelési tevékenység, a szolgáltatások biztonsági állapotának folyamatos ellenőrzése és a biztonsági események kezelése, valamint a folyamatos kockázatkezelés.

Észrevételek és javaslatok

Az előzőekben felsorolt feladatokat a NISZ Zrt. értelemszerűen csak a szolgáltatásait igénybe vevő szervekkel (ellátotti kör) együttműködve tudja végrehajtani, és ugyanez a helyzet az ellátotti kör szemszögéből is. A feladat- és felelősségmegosztás szükségességét az Ibtv. rögzíti[22], ugyanakkor a feladatelhatárolásra, illetve a közösen végrehajtandó feladatok, tevékenységek azonosítására nem született iránymutatás, a kérdést az érintett feleknek kell rendezniük.

A feladatok közös ellátásának igénye (és célszerűsége) mellett a – fogalmi, tartalmi – egységesség követelményének érvényesítéséről is szükséges lenne dönteni.

Jelenleg sem a jogszabályi környezet, sem a szakirodalom, sem az ezzel foglalkozó szakértői kör nem tud teljes körű és könnyen adaptálható kockázatfelmérési módszertant ajánlani a közigazgatás számára. A megfelelő módszertan kiválasztása és alkalmazása tehát nem könnyű feladat, különösen

20 http://www.nisz.hu/hu/rolunk

21 A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendelet.

22 Ibtv.11. § (1)–(3) bekezdés. http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.339954

azon kisebb – jellemzően önkormányzati – szervek esetében, ahol az informatikai tudással, képesítéssel felvértezett munkatársak létszáma nagyon alacsony; olykor mindössze egy munkatárs lát el ilyen jellegű feladatokat.

A megfelelő létszám hiánya mellett nehézséget jelenthet a feladat az egyes szervezetek ezzel a kérdéssel korábban nem foglalkozó, munkaidejükben jellemzően másfajta tevékenységet végző alkalmazottai számára is, hiszen a főleg külföldi szakirodalom feldolgozása után, példálózó segédletek áttekintését követően a saját szervezetükre vonatkozó, egyediesített és szakmailag korrekt, ráadásul hatóság által számon kérhető kockázatfelmérést kell végrehajtani.

Felvetődhet a feladat végrehajtásának kiszervezése külső vállalkozó számára. Ha egy szervezet így dönt, nem eshet a feladatkipipálás csapdájába; nem szerencsés a feladatot egy külső cég összeollózott sablonok alkalmazásával készített „eredménytermékével" letudni. A kiszervezés hasznos lehet, ha a szervezet „megveszi" a kockázatelemzési tudást, amit a továbbiakban használni is akar és megteremti a saját – szervezetismerettel bíró és így az egyediesítést és az alkalmazható eredményt garantáló – belső erőforrásokat a kockázatfelmérés végrehajtásához.

Mindezzel természetesen – bár egyedi jó megoldások születhetnek – a kockázatfelmérési megközelítés és gyakorlat még nem lesz egységes a közigazgatásban. A különböző módszertanok, ajánlások egyedi kombinációinak létrehozása nem feltétlenül célravezető, ráadásul – a szervezetrendszer egészét tekintve – erőforrás-igényes. Makroszinten – például a közigazgatás vagy csak a központi államigazgatás vagy csak az önkormányzatok szintjén – célszerű lenne egységes (részben testre szabható) módszertant kialakítani és alkalmazni és ehhez megfelelő segédleteket biztosítani.

A megfelelő módszertan kiválasztása mellett a módszertan alkalmazásának megfelelőségére is figyelemmel kell lenni. A kockázatazonosítási folyamatban, a vagyontárgyak azonosításakor, a szervezet által a feladatellátáshoz használt (a NISZ Zrt. esetében: üzemeltetett) elektronikus információs rendszerekről az értékeléshez szükséges minden (leíró) adatnak – naprakészen – rendelkezésre kell állnia, beleértve az adatgazdára vonatkozó konkrét adatokat, hiszen ő tud (köteles) nyilatkozni a kezelt, feldolgozott adatok értékéről, az elektronikus információs rendszer szervezetben betöltött szerepéről, jelentőségéről. Ráadásul ezek az adatok ebben a kontextusban még csak egy szervezetről szólnak; az infokommunikációs szolgáltató szemszögéből az említett adatoknak „szervezet közötti" szinten is következeteseknek, összemérhetőknek kellene lenniük. A NISZ Zrt. által ellátott intézmények száma meghalad-

ja a kétszázötvenet; a társaság nyilvántartásai alapján mintegy ezerötszáz alkalmazásról van szó, amelyek adatgazdai értékelése szervezetenként történt (vagy nem történt) meg; ehhez kell a szolgáltatások tartalmát és a jogszabályok által előírt információvédelmi intézkedéseket meghatározni úgy, hogy például csak a levelezőrendszerre vonatkozó értékelések a 3. és az 5. biztonsági osztály kategóriái között szóródnak.

A kockázatfelméréshez is szükséges kötelező vagy ajánlott leltárak és nyilvántartások összeállításának, tartalommal feltöltésének eltérő módszertana mellett a szervezeti kultúrák sokféleségéből adódó további különbözőségeket is figyelembe kell venni, gondoljunk például a szabályozási vagy szerződés-előkészítési hagyományok, szokások, eljárásrendek eltéréseire. Ha már a szervezeten belüli – belső – szabályozási rendszerek eltérő felfogásban kezelik a feladatok és a felelősségek meghatározásának, megfogalmazásának kérdéseit, hogyan lehet ezt az ellátotti kör tekintetében a szolgáltató részéről egységessé tenni úgy, hogy az mindkét oldal (és az egyik oldal sok szereplőjének) megelégedésére szolgáljon? Megoldásként felvetődhet a 309/2011. kormányrendelet alapján a 1469/2011. (XII. 23.) kormányhatározattal létrehozott Informatikai Felhasználói Munkacsoport[23] keretein belüli egyeztetések lehetősége is.

A szervezetek közötti egyeztetéseknek természetesen akkor lehet eredményük, ha a kockázatfelméréssel megbízott vagy megbízandó munkatársak a szervezeteken belül megfelelő képzést, felkészítést kapnak a feladatok elvégzéséhez. E feltétel teljesíthetőségének vizsgálatakor ismét felvetődik a szervezetenkénti önálló végrehajtás és azt követő konszolidáció vagy az előre, „központilag” elkészített módszertan és ütemterv szerinti haladás lehetőségei közötti választás. A NISZ Zrt. jelenleg a saját és az ellátotti körbe tartozó, együttműködő intézmények adatszolgáltatásaiból származó információk feldolgozása, konszolidálása alapján végzi a jogszabályok által előírt információbiztonsági feladatokat, a már említett feladat- és felelősségmegosztás megvalósításához még sok a tennivaló.

JOGSZABÁLYOK

A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény.

23 A 309/2011. (XII. 23.) kormányrendelet 5. § (1) bekezdése szerint a munkacsoport *„a központi szolgáltatási megállapodásban foglalt követelmények meghatározását és ellenőrzését”* végzi, koordinációs és konzultációs fórumként is működik, működhet.
http://njt.hu/cgi_bin/njt_doc.cgi?docid=140272.342120

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendelet.

A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) kormányrendelet.

A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) kormányrendelet.

Egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet.

A központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) kormányrendelet.

A központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.

1469/2011. (XII. 23.) kormányhatározat az Informatikai Felhasználói Munkacsoport létrehozásáról.