ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Jogi és közigazgatási ismeretek

Elektronikus információbiztonsági vezető szakirányú hallgatóknak

dr. Bodó Attila Pál

Nemzeti Közszolgálati Egyetem

Budapest, 2014

TARTALOMJEGYZÉK

Előszó

Jelen tananyag célja, hogy a hallgató számára a jogi alaptan és a közigazgatási jog alapjai témakörét érintően segítséget és kitekintést nyújtson a jog és a közigazgatás rendszerszemléletű értelmezéséhez és áttekintéséhez. Ennek megfelelően nem célja a tananyagnak az állam és a jog eredetének és kialakulásának, a jogi alaptan és a közigazgatási jog általános szabályrendszerének teljes körű és mindenre kiterjedő bemutatása, a közigazgatási alap- és szakvizsga tananyagának megismétlése. A tananyagban a fenti tárgykörök alapkérdéseinek az áttekintésére olyan mélységben kerül sor, amely ahhoz szükséges, hogy a hallgató az elektronikus információbiztonság szabályozási környezetét a jog- és a közigazgatás rendszerében, átfogó szemlélet alapján legyen képes elhelyezni. Ezen alapvetés mentén:

- a Jog, jogrendszer, alapfogalmak fejezet célja, hogy bemutassa a normák sajátosságait, a jog és az állam összefüggéseit, a kapcsolódó alapfogalmakat;
- a Jogalkotástan fejezet célja, hogy bemutassa a jogalkotás alapvető követelményeit és a jogforrási hierarchiát, a jogforrási hierarchiában elfoglalt helye és a hatályos joganyag alapján az elektronikus információbiztonság szabályozási környezetét;
- a Közigazgatási jog alapjai fejezet célja, hogy bemutassa a közigazgatás ismérveit és sajátosságait, felvázolja a közigazgatás helyét az államszervezetben;
- a Közigazgatási szervek fejezet célja, hogy bemutassa a közigazgatási szervek sajátosságait és a hatályos joganyag alapján az elektronikus információbiztonság szervezetrendszerét a magyar közigazgatásban.

Bízom benne, hogy jelen tananyag sikerrel hozzájárul az elektronikus információbiztonság jogi és közigazgatási vetületének rendszerszemléletű áttekintéséhez.

A szerző

1. Jog, jogrendszer, alapfogalmak

A jog és a jogrendszer rendszerszemléletű megközelítését támogató tudományelméleti alapvetés rögzítése, a tudományos gondolkodás történeti bemutatása jelen tananyag keretein túlmutat, a tananyag értelmezéséhez szükséges általános ismereteket, mint meglévő alapokat használjuk fel. Ami a jog és a jogrendszer tudományelméleti megközelítését illeti, abból kell kiindulni, hogy az ismeretanyag tárgyát a társadalom állami és jogi jelenségei, azok működésének a szabályszerűségei adják. Az állam- és jogtudományok általános jellemzése alapján elmondható, hogy azok az állami és jogi jelenségek minden összefüggését, a társadalom és a politikai-jogi berendezkedés egészét, az állam és az állami szervek tevékenységét vizsgálják. Ezen szemlélet alapján az állam- és jogtudományok rendszerén belül megkülönböztetjük az általános (pl. állam- és jogtörténet), illetve az ágazati állam- és jogtudományokat (pl.: büntetőjog). Előzőek az állammal és a joggal, mint egésszel foglalkoznak, utóbbiak az állam és a jog egyes részterületeit vizsgálják, főként a jogrendszer tagozódását követve. Nem elmélyedve a rendszertani elhelyezésben a jog és a jogrendszer alapfogalmainak megvilágításához a következőkben az állam jellemzői kerülnek meghatározásra.

1.1. Az állam sajátosságai és az állami szervek rendszere

Az állam, mint működő szervezetrendszer fogalmának meghatározása helyett, a jogi alapok rendszertani elhelyezése érdekében, az állam sajátosságait célszerű felsorolás szintjén rögzíteni. Ezek azok a jellemzők, amelyek minden állam esetében, koronként változóan, eltérő intenzitással ugyan, de mindig jelen vannak. Ennek tükrében a következő sajátosságok[1] rögzíthetők:

1.) Az állam történeti kategória, mivel fejlődését történeti korszakok jellemzik, fejlődési útja a társadalom szerkezeti változásaival párhuzamosan vizsgálható.

2.) Az állam létrejötte objektív társadalmi szükséglet, mivel az állam szerepvállalása nélkül a társadalom és a gazdaság mechanikus folyamatai, a társadalmi viszonyok felbomlanának.

3.) Az állam társadalmi rendeltetését funkcióin keresztül, a társadalmi szükségletekhez igazodva, feladatellátása során, az állami tevékenység különböző formái útján valósítja meg, melynek állandóságát intézményesített formája biztosítja.

[1] Szilágyi Péter: Jogi alaptan (2003. Bp. Osiris Kiadó) 157. oldal

4.) Az állam a társadalom politikai berendezkedésének központi intézménye. Ennek keretében az állam a fizikai erőszakkal való kényszerítés jogszerűen elismert alkalmazásának a kizárólagosságával és az ehhez kialakított intézményrendszerrel rendelkezik, amely során korlátozhatja a társadalom tagjainak cselekvési szabadságát.

5.) Az állam a néptől és társadalomtól elkülönült, szuverenitással rendelkező közhatalom, és mint ilyen a társadalom egészére kiterjedő hatalmat gyakorol, jogrendszerét és szervezetrendszerét önállóan alakítja, független és önrendelkezési jogosultsággal rendelkezik, nincs alárendelve más államnak. Önállóságát gazdasági függetlensége biztosítja.

6.) Az állam a munkamegosztás külön ágát képező sajátos szervezetrendszerrel rendelkezik, összefüggő rendszert alkot. Szervezetrendszeréhez kapcsolódó tagjai, az államapparátus, megfelelő szempontok alapján kiválasztott, sajátos tevékenységet végző embercsoport.

Az állam fentiekben említett sajátosságai közül az állam, mint közhatalom működéséhez kapcsolódó szervezetrendszert szükséges részletesebben kifejteni.

Az *állami szervek rendszere*[2] jogilag szabályozott egységes rendszert alkot, különböző szintű és típusú szervekből épül fel. Azokat a szerveket tekintjük állami szerveknek, amelyek tevékenységüket közhatalom birtokában végzik, a társadalomra és tagjaira nézve kötelező, állami kényszerrel kikényszeríthető döntéseket hozhatnak és az állami kényszert alkalmazhatják. Az állami szervek típusait megkülönböztethetjük feladatuk, tevékenységük és munkamódszerük, alá- és fölérendeltségen alapuló egyedi szervezeti felépítésük, illetve tevékenységük jogi szabályozása alapján. Ezen tulajdonságok figyelembevételével *hét fő állami szervtípust*[3] különböztetünk meg:

1. *Fegyveres és rendvédelmi szervek.* Speciális feladatellátásuk, hogy fizikai erőszak alkalmazásával vagy az azzal való fenyegetéssel felszámolják az állam ellen irányuló támadásokat. A belső rend fenntartása és a külső támadásokkal szembeni védekezés mellett ellátnak honvédelmi és rendészeti államigazgatási tevékenységet is. Feladataikat általában a honvédség és a rendvédelmi szervek (pl.: rendőrség, polgári nemzetbiztonsági szolgálatok, tűzoltóság, büntetés-végrehajtási testület) útján gyakorolják.

2. *Közigazgatási szervek*, melyek tevékenysége általánosan szervező-végrehajtó-rendelkező tevékenységként jellemezhető, mivel feladataik ellátása során általános jelleggel kötelező döntéseket hoznak, jogalkalmazást végeznek, esetenként szervezési és

[2] Jogi alaptan 186-187. oldal
[3] Jogi alaptan 188-196. oldal

jogalkotási tevékenységet is ellátnak. Két lényeges fajtáját az államigazgatási szervek és az önkormányzati igazgatási szervek alkotják.

3. *Bíróságok,* mint az igazságszolgáltatás szervei. Azokban az ügyekben, ahol valamilyen jogvita áll fenn, tárgyalásos eljárás útján feltárják a jogvita alapjául szolgáló tényállást és a jog szabályait alkalmazva eldöntik a jogvitát és megállapítják a jogkövetkezményeket, melyek kötelező érvényűek. Feladatuk az igazságszolgáltatás gyakorlása során a jog szabályainak alkalmazása és érvényre juttatása. Eljárásuk során alapvető elv a bírói függetlenség elve, melynek lényege, hogy ítélkező tevékenységük során a bírákat a döntés tartalmára vonatkozóan nem utasíthatják, tevékenységük során csak a jogszabályoknak vannak alávetve.

4. *Törvényességi felügyeleti-ellenőrző szervek.* Ezen elkülönült csoport alapvető feladata a vizsgálat és ellenőrzés, amely célja az esetleges jogsértések feltárása és a kapcsolódó intézkedések megtétele. Idesorolhatóak például az ügyészi szervek, melyek sajátos feladata a törvényesség érvényesülésének biztosítása a társadalom életének minden területén. Ide tartoznak továbbá az ún. pénzügyi ellenőrző szervek (pl. Állami Számvevőszék) és az alapvető jogok védelmét ellátó szervek, személyek (pl. ombudsman).

5. A *külkapcsolatok szervei*, melyeket sajátos diplomáciai tevékenység és igen szigorú centralizáltság jellemez (pl. követségek, konzulátusok, diplomaták).

6. *Az állami képviseleti szervek.* Feladatuk, hogy kifejezzék és érvényesítsék a választók érdekeit, biztosítsák az állami szervek felett a társadalom politikai ellenőrzését. Mindig testületi szervek és mindig a társadalom választójoggal rendelkező tagjai által választottak, alá-fölé rendeltségük elsősorban az általuk alkotott jogszabályok hierarchiájában fejeződik ki. Fő feladatuk a törvényhozás, ezért törvényhozó szerveknek is nevezik őket.

7. *A területi önkormányzatok*, melyek önállósággal rendelkező helyi képviseleti szervek, alárendeltségük csak a jogszabályoknak való alárendeltséget jelenti. Feladatuk a helyi közügyek intézése, a helyi közigazgatás ellátása.

Az állami szervek egységes rendszert alkotnak[4] politikailag, mivel azonos politikai célok érdekében tevékenykednek, szervezetileg, mivel az alkotmányos rendet a hierarchikus felépítettsége biztosítja, jogilag, melyet az egységes jogi szabályozás biztosít.

[4] Jogi alaptan 198. oldal

1.2. A jog fogalma és sajátosságai, a társadalmi és a jogi norma, a jogtétel

A jog fogalmának definíció szerinti meghatározására sok elméleti megközelítés ad támpontot, ezek részletes kifejtését mellőzve, alapvetésként abból a tudományosan és általánosan is elfogadott tételből indulunk ki, amely a jog magatartásjellegét hangsúlyozza. Mindehhez szükséges azonban meghatározni a magatartásszabályokra vonatkozó sajátosságokat, azaz a társadalmi normákat.

A *társadalmi normák*[5] olyan magatartás-előírások, amelyek a több lehetséges magatartás közül előírják a helyeset és a követendőt, ezáltal értékelést fejeznek ki, az előírt magatartás be nem tartása esetére hátrányos következményt helyeznek kilátásba. A társadalmi normák olyan magatartásmintát fejeznek ki, melyek befolyásolják az emberek viselkedését. Jellemző rájuk az általános és a tartós időbeli érvényesség, azaz a rögzített előírás a társadalom tagjainak meghatározott körében kötelező, azokat ott be kell tartani, és nem egyszeri magatartásokra, hanem ismétlődő helyzetekre vonatkoznak. Kapcsolódik hozzájuk szankció, a normasértés hátrányos következménye, továbbá érvényesüléseként a kényszer lehetősége, a hátrány elszenvedésével való fenyegetettség. Fontos kiemelni, hogy csak azok az előírások lehetnek társadalmi normák, amelyek mint elvárások reálisak és amelyeket az esetek többségében ténylegesen be is tartanak vagy szankcionálnak, vagyis ténylegesen érvényesülnek.

A társadalmi norma három alapvető mozzanata tehát a magatartás megfogalmazása, annak normatív minősítése (tilos, kötelező vagy megengedett), és normasértés esetén az előírt következmény által történő szankcionálás. Mindezek figyelembevételével a társadalmi normák négy alapvető funkciót töltenek be:[6]

1. előírt magatartásmintát nyújtanak a társadalom tagjai számára, hogy adott esetben mi a helyes, követendő magatartás,
2. közreműködnek a konfliktusok rendezésében,
3. értékelési alapot teremtve lehetővé teszik a magatartások értékelését,
4. az előírt magatartásminta felhasználásával lehetőséget biztosítanak a magatartások előzetes becslésére.

A társadalmi norma szerepéből kiindulva, ha a jog fogalmát a legegyszerűbben szeretnénk meghatározni, azt mondhatjuk, hogy a jog nem más, mint *magatartásszabályok összessége*.

[5] Jogi alaptan 208-211. oldal
[6] Jogi alaptan 212. oldal

Precízebb meghatározást keresve azt mondhatjuk, hogy *a jog olyan magatartási szabályok és azokhoz kapcsolódó egyéb magatartás-előírások (elvek, célmeghatározások) összessége*[7], amelyek

a) keletkezése állami szervekhez kötődik, azokat az állam bocsátja ki és szükség esetén szankcionálja azok megsértését,

b) az adott társadalomban kötelezőek, vagyis általános érvényesség jellemző rájuk,

c) érvényesülését az állami szervek kényszerrel is biztosíthatják.

Kiegészítő megjegyzésként rögzíteni szükséges, hogy a jog általános érvényessége nem jelenti azt, hogy minden egyes jogi norma mindenkire nézve azonos módon lenne kötelező, mivel bizonyos jogi normák kizárólag egy meghatározott címzetti körre vonatkoznak, az általános érvényesség nem azonos a jogi normák címzettjeinek általánosságával. Ehhez hasonlóan a jog tényleges érvényesülésére az esetek túlnyomó többségében önkéntes jogkövetés révén, állami szervek közreműködése nélkül kerül sor, ettől függetlenül szükséges, hogy a jog nem követése esetén fennálljon az állami érvényesítés, a kényszerítés lehetősége is. A jog tényleges érvényesülését az a tény dönti el, hogy az emberek az adott magatartásszabálynak megfelelően cselekednek-e vagy sem.

A jog definíciójának rögzítése elsősorban a jog norma jellegét, azaz a társadalmi normák jogra jellemző vonásait hangsúlyozza, emellett azonban vannak olyan további lényeges vonások, melyek a jog fogalmának a meghatározásához elengedhetetlenek. Ezen további *sajátosságok*[8] közül – főbb elemekként – ki kell emelni, hogy a jog:

a) a magatartások szabályozásának társadalmi szükségleteként jelenik meg, a jognak tehát társadalmi rendeltetése van;

b) a társadalom jogi jelenségeinek funkcionálisan összefüggő rendszere, amely jogintézményekből, jogszabályokból, a jogalkotás és a jogalkalmazás szerveiből és az emberi magatartásokból áll, ezt nevezzük *jogi rendszer*nek (amely nem azonos a jogrendszerrel);

c) maga is társadalmi viszony, más, nem jogi társadalmi viszonyok jogviszonyok formájában történő rögzítése és azok védelme;

d) történeti kategória, az állam történeti fejlődése és kialkaulása során jött létre, folyamatosan változik.

[7] Jogi alaptan 213. oldal
[8] Jogi alaptan 217-219. oldal

A jog legkisebb, még önmagában értelmes egysége, amely teljes, értelmezhető, követhető, alkalmazható magatartásszabályt alkot a *jogi norma*[9], a szabályozás logikai egysége. A *jogtétel*[10], másképp fogalmazva a jogi mondat, a nyelvi megfogalmazás és megjelenés egysége, s mint nyelvtanilag értelmezhető egység, egy paragrafus, illetve egy bekezdés alkothat egy jogtételt. Azok a jogtételek alkotnak egy jogi normát, amelyek egymáshoz való kapcsolódása annyira szoros, hogy önállóan nem lennének értelmezhetőek, ezért egy jogi norma egyszerre több jogtételből is állhat.

1.3. A jogi norma szerkezete, fajtái, érvényessége

A jogi norma, mint legkisebb logikai egység tartalmát tekintve egyrészt céltételezést tartalmaz, amely célja, hogy a meghatározott magatartások létrejöjjenek vagy ezzel ellenkezőleg, ne jöjjenek létre, másrészt, mint magatartási szabály előírja, hogy bizonyos körülmények fennállása esetén meghatározott magatartást kell tanúsítani, azaz rögzíti a magatartás jogi minősítését, vagyis a kötelezővé, a tilossá vagy a megengedetté nyilvánítását. Előírja továbbá, ha a rögzített magatartás megvalósul, vagy nem valósul meg, akkor bizonyos jogkövetkezményeknek kell beállniuk, azaz megteszi a jogkövetkezmények kilátásba helyezését.

A jogi norma tartalmához igazodva szerkezeti elemekre[11] tagolható az alábbiak szerint:

1) *A hipotézis (feltétel)* a magatartás körülményeinek, szituációjának a megfogalmazása, amely azt fejezi ki, hogy mikor, milyen körülmények között kell vagy szabad a szabályozott magatartás alanyának meghatározott és a diszpozícióban megfogalmazott magatartást tanúsítania, illetőleg attól tartózkodnia.
2) *A diszpozíció (rendelkezés)* azt fejezi ki, hogy a hipotézisben megfogalmazott feltételek bekövetkezése esetén a jogi norma címzettjének milyen magatartást kell, lehet vagy szabad tanúsítania, amely együttesen tartalmazza a jogi norma címzettjét, a magatartást és annak jogi minősítését.
3) A *jogkövetkezmény* lehet szankció, amely a diszpozícióban előírt magatartás nem követése esetére a címzett számára hátrányos, negatív következményeket helyez kilátásba, vagy lehet joghatás, amely a megfelelő magatartás tanúsításának esetére a címzett számára pozitív következményeket helyez kilátásba.

[9] Jogi alaptan 223. oldal
[10] Jogi alaptan 223. oldal
[11] Jogi alaptan 254. oldal

A jogi normákon belül két fő csoportot különböztetünk meg, az ún. regulatív jogi normákat, amelyek közvetlenül szabályozzák a jogi norma alanyainak a magatartását úgy, hogy azokat minősítik és jogkövetkezményeket helyeznek kilátásba, illetve a feladatkijelölő jogi normákat, melyek elsősorban az új társadalmi viszonyok kialakítására és átalakítására, valamint szervezeti magatartások szabályozására alkalmas jogi normák.[12] Utóbbiak alkalmazása az államigazgatási jogra jellemző megoldás volt, szerepük folyamatosan csökken.

A regulatív jogi normákon belül további alfajokat – alapvetően a szerkezeti elemekre történő tagoláshoz igazodóan – különböztethetünk meg:

a) A rendelkezés (diszpozíció) és a jogkövetkezmény kapcsolata[13] alapján a jogi norma lehet *tiltó norma,* amely valamely magatartástól való tartózkodást ír elő, *parancsoló norma,* amely valamely magatartás követését írja elő, valamint *megengedő norma,* amely valamely magatartás tanúsítását megengedi, de ahhoz jogkövetkezményt társít joghatás vagy szankció formájában.
b) A hipotézis (feltétel) és a rendelkezés (diszpozíció) kapcsolata alapján[14] a jogi norma lehet *meghatározott tartalmú*, amely tartalmazza a hipotézis és a diszpozíció meghatározását (pl.: büntetőjogi tényállások) és *nem meghatározott tartalmú,* amely a hipotézis és a diszpozíció meghatározását más jogi normákra való hivatkozással teszi meg. Utóbbi két típusa a keretszabály és az utaló norma. *Keretszabály* esetén a jogi norma tartalmát más jogszabályok töltik ki (pl.: más jogszabályra történő utalással), az *utaló jogi norma* valamely jogszabály pontosan meghatározott rendelkezését veszi át.
c) A kötelező erő alapján[15] a jogi norma lehet *kógens*, amely kötelező erejétől közös megegyezéssel sem lehet eltérni (pl.: büntetőjogi normák), *diszpozitív (engedő),* amely kötelező erejétől való eltérést a jog a felek kölcsönös megegyezése alapján engedi (pl.: polgári jog normák), *ajánló,* amelynek előírásai közvetlenül nem kötelezőek, a jogszabály csupán ajánlja az azoknak megfelelő magatartást.
d) A jogkövetkezmények alapján a jogi norma lehet *joghatás* és *szankció*.

A jogi normák *érvényessége* a jogi norma kötelező erejét, annak alkalmazását jelenti, tételes jogi feltételei azonban már a jogszabályok érvényességéhez kapcsolódnak. Emellett érvényességi kellék a jogi norma *hatálya* is, amely meghatározott időben és területen,

[12] Jogi alaptan 263. oldal
[13] Jogi alaptan 256-257. oldal
[14] Jogi alaptan 264. oldal
[15] Jogi alaptan 264. oldal

meghatározott személyek számára előírt kötelezést jelent. Ennek alapján megkülönböztetjük a *jogi normák időbeli, területi és személyi hatályát*, ezek szintén a jogszabályok érvényességéhez kötődnek.

1.4. A jogrendszer fogalma és tagozódása, a magyar jogrendszer jogágai

A *jogrendszer* egy adott állam érvényes jogi normáinak és ahhoz kapcsolódó egyéb jogi előírásainak (jogelvek, célmeghatározások) a rendezett összessége.[16] Fontos kiemelni, hogy a jogrendszer fogalma nem azonos és nem keverendő össze a jogi rendszer fogalmával (vö. 1.2. alcím).

A jogrendszer felosztásának, rendszerezésének alapvető módszertanát általában a jogágakra tagozódás adja, amely alapját a jogi normák eltérő tartalma, a szabályozott magatartások sajátosságai képezik, így a felbontás egységét a szabályozás tárgya és módszere adja. A jogrendszeren belül a *jogág*[17] a jogi normák hasonló tartalommal és formával jellemezhető, azonos vagy hasonló jellegű magatartásokat azonos módszerrel szabályozó összefüggő csoportja. A jogágak jellemző vonása[18], hogy a szabályozott magatartása azonos, illetőleg hasonló jellegű, ezáltal azonos szabályozási módszert alkalmazhat. Minden jogág közös és azonos jelentésű alapfogalmakkal rendelkezik, a jogviszonyok sajátos fajtáiban és a jogalkalmazás sajátos formáiban érvényesülnek, ezért sajátos jogszabály-értelmezési elvek vonatkoznak rájuk.

Jogintézmények[19] alatt az azonos társadalmi viszonyt szabályozó jogi normák együttesét értjük. A jogintézmény lényegét képező szabályok általában egyértelműen valamelyik jogág (pl.: tulajdon esetében a polgári jog) részét képezik, ezekhez a normákhoz azonban további, más jogághoz tartozó normák is kapcsolódhatnak, ezáltal a jogintézmények jelentős része keresztezi a jogágak határait. A *jogterület*[20] a jogi normák összekapcsolódó és elkülöníthető összessége, amelyik egy jogintézménynél szélesebb, de a jogág kritériumaival nem rendelkezik. Jogterület létrejöhet egy-egy jogágon belül, amikor a jogi normákat erős kapcsolódás és hasonlóság jellemzi (pl.: öröklési jog a polgári jogon belül) vagy több jogágat

[16] Jogi alaptan 318. oldal
[17] Jogi alaptan 322. oldal
[18] Jogi alaptan 322. oldal
[19] Jogi alaptan 322. oldal
[20] Jogi alaptan 323. oldal

részben átfedve, amikor is az eltérő tartalmú, de azonos vagy hasonló társadalmi viszonyokra vonatkozó jogi normákat fog össze (pl.: gazdasági jog).

A jogrendszer alapvetően tehát jogágakra tagozódik, egyes szorosan összetartozó jogágak olyan csoportokat alkothatnak, melyekből *ún. vegyes szakjogágak* jöhetnek létre.

Fentiek alapján a magyar jogrendszer az alábbi felosztás szerint sorolható jogágakba:

a) Közjogi jogágak: amelynél az egyik ágon mindig a közhatalom szerepel, erős alá-fölérendeltségi viszony áll fenn a felek között. Ide soroljuk:
   - az alkotmányjogot,
   - a közigazgatási jogot,
   - a pénzügyi jogot,
   - a büntetőjogot (anyagi büntetőjog, büntetőeljárási jog, büntetés-végrehajtási jog),
   - a polgári eljárásjogot (peres és peren kívüli eljárások).

b) Magánjogi jogágak: melyben a felek egyenrangúak és a közhatalom közhatalmi minőségében nincs jelen a jogviszonyban. A jogviszonyokat a felek a jogszabályok keretein belül közös megegyezéssel szabadon alakíthatják. Ide soroljuk:
   - a polgári jogot (pl.: dologi jog, kötelmi jog, társasági jog; szellemi alkotások joga, öröklési jog, családi jog),
   - a nemzetközi magánjogot,
   - az agrárjogot (mezőgazdasági jog).

c) Vegyes szakjogágak: a felek egyenrangúak és szabadon alakíthatják viszonyaikat, de az állam a gyengébbik fél védelmében beavatkozik a jogviszonyokba és kötelezettségeket, garanciákat ír elő. Ide soroljuk: a munkajogot, a társadalombiztosítási vagy a szociális jogot.

d) Ún. „külső jogok”, ide soroljuk a nemzetközi közjogot és az európai (közösségi) jogot, melyek nem részei a belső jogrendszernek.

2. Jogalkotástan

A jogalkotástannak, mint a jogszabályok létrejöttét folyamatában vizsgáló önálló tárgynak a célja, hogy összefoglalja a jogalkotáshoz szükséges elméleti és gyakorlati ismereteket. A rendszertani elhelyezés érdekében ezen széleskörű ismeretek közül – az államra és a jogrendszerre vonatkozó alapvetések birtokában – szükséges a jogalkotás alapvető követelményeinek, a jogszabályra, mint a jogalkotás egységére vonatkozó sajátosságoknak és a jogforrási hierarchiának a főbb elvek mentén történő ismertetése. Ezeknek az alapoknak az ismeretében kerülhet sor a hatályos joganyag alapján az elektronikus információbiztonság szabályozási környezetének a bemutatására és a magyar jogrendszerben történő elhelyezésére.

2.1. A jogalkotás fogalma és a jogalkotói jog, a jogalkotás alapvető követelményei

A *jogalkotás* a jogalkotó hatáskörrel felruházott állami szerveknek az a tudatos és kizárólagos tevékenysége, amely jogi normák létrehozására irányul és amely során a jogalkotó szervek közvetlenül jogszabályok létrehozására törekszenek.[21] Ez esetben az állami szervek tudatos tevékenysége, maga a *jogalkotás a jogforrás alapja, amely az alábbi jellemzőkkel* írható körül[22]:

a) Szándékolt, akaratlagos és egyben megváltoztatható folyamat, abban különböző társadalmi, egyéni akaratok fejeződnek ki és kapcsolódnak össze, a társadalmi lehetőségek közötti tudatos, szándékos választásokat tartalmaz.
b) A jövőben előforduló bekövetkezhető esetekre megfogalmazott jogi normákból áll, olyan szabályozást jelent, amely érvényessége általában a jövőre szól.
c) A korábbi jogi szabályozás kritikájából, valamint általános politikai értékelésekből és célkitűzésekből kiinduló következtetéseket tartalmaz.
d) Általánosan, kötelező jelleggel és általános érvényességgel megfogalmazott és kihirdetett jogi normákból áll, melyek a társadalom minden tagjára nézve vagy a személyek túlnyomó többsége számára érvényes, követendő normaként jelennek meg.
e) Érvényessége, kötelező ereje magából az alkotás akarati aktusából fakad.
f) Alkalmas arra, hogy a politikai törekvéseket az általánosság szintjén juttassa érvényre.
g) Stabil, de kevésbé rugalmas, mert tartalmi általánossága miatt alaposabb előkészítést és

[21] Jogi alaptan 238. oldal
[22] Jogi alaptan 238-239. oldal

több időt igényel, továbbá politikai jellege miatt politikai ellentétek is fékezhetik a jogalkotó szervek működését.

h) Logikailag rendezett, nyelvileg szabatosan meghatározott és rögzített formában jön létre.

i) A laikusok számára is áttekinthető és könnyebben megismerhető.

A jogalkotói jogot az alapján tudjuk megkülönböztetni, hogy milyen állami szerv jogalkotó tevékenységéről van szó. Ez alapján a *jogalkotásnak két fajtáját* különböztetjük meg[23]:

a) A *törvényhozás* általában a legfelső állami szervek jogalkotásra irányuló tudatos jogalkotói tevékenységét jelenti, amelyet rendszerint a legfelső népképviseleti szervek, a parlamentek végeznek az államfő közreműködésével.

b) A *rendeletalkotás* minden olyan nem törvényhozási jogalkotási tevékenység, amelyet általában a parlamentnek alárendelt közigazgatási szervek végeznek. Három fő alfaja a *kormányzati rendeletek*, melyeket általános hatáskörű kormányzati szervek (pl.: kormány) alkotnak, az *ágazati rendeletek*, melyeket a közigazgatás egy-egy ágát irányító miniszterek alkotnak, és az *önkormányzati rendeletek*.

A jogalkotás alapvető követelményeit a jogalkotásról szóló 2010. évi CXXX. törvény (a továbbiakban: Jat.) II. fejezete szabályozza, az abban leírtak olyan axiómákat tartalmaznak, amelyek a jogalkotóra nézve kötelező jelleggel bírnak. A rendelkezések[24] szerint a jogszabály:

a) a címzettek számára egyértelműen értelmezhető szabályozási tartalommal kell, hogy rendelkezzen;

b) az ún. visszaható hatály tilalma alapján alkotható meg;

c) hatálybalépésének időpontját úgy kell megállapítani, hogy elegendő idő álljon rendelkezésre a jogszabály alkalmazására való felkészülésre;

d) megalkotásakor biztosítani kell, hogy a jogszabály:

da) megfeleljen az Alaptörvényből eredő tartalmi és formai követelményeknek,

db) illeszkedjen a jogrendszer egységébe,

dc) megfeleljen a nemzetközi jogból és az európai uniós jogból eredő kötelezettségeknek,

dd) megfeleljen a jogalkotás szakmai követelményeinek;

e) nem ismételheti meg az Alaptörvény vagy olyan jogszabály rendelkezését, amellyel a jogszabály az Alaptörvény alapján nem lehet ellentétes;

f) szabályozása nem lehet indokolatlanul párhuzamos vagy többszintű;

[23] Jogi alaptan 240-241. oldal

[24] A jogalkotásról szóló 2010. évi CXXX. törvény (a továbbiakban: Jat.) 2. §

g) megalkotására adott felhatalmazásban meg kell határozni a felhatalmazás jogosultját, tárgyát és kereteit.

A jogalkotással szemben támasztott további követelmény[25], hogy:
a) az azonos vagy hasonló életviszonyokat azonos vagy hasonló módon, szabályozási szintenként lehetőleg ugyanabban a jogszabályban kell szabályozni,
b) a felhatalmazás jogosultja a jogi szabályozásra másnak további felhatalmazást nem adhat,
c) a felhatalmazás jogosultja a jogszabályt köteles megalkotni, feltéve, hogy a felhatalmazást adó jogszabályból kifejezetten más nem következik,
d) a szabályozás tárgykörébe tartozó alapvető jogintézmények, jogok és kötelezettségek alapvető szabályainak megállapítására, a jogszabály egészének végrehajtására, valamint olyan tárgykör szabályozására, amit a felhatalmazást adó jogszabály nem szabályoz, nem lehet felhatalmazást adni.

Jogalkotási alapelv a visszaható hatály tilalma, amely szerint jogszabály a hatálybalépését megelőző időre nem állapíthat meg kötelezettséget, kötelezettséget nem tehet terhesebbé, valamint nem vonhat el vagy korlátozhat jogot, és nem nyilváníthat valamely magatartást jogellenessé[26]. Mind a jogbiztonság követelményével és ezáltal a jogállamisággal ellentétes, és rendkívüli körülményektől eltekintve igazságtalan is, ha a megvalósítás idején jogszerű magatartást később jogellenessé nyilvánítanak és ahhoz szankciót fűznek.

2.2. A jogszabályok érvényessége, a jogérvényesülés, a jogszabály értelmezés

A *jogszabály* a jogalkotásnak az egysége, az egy jogalkotási aktussal elfogadott jogtételek, azokon keresztül jogi normák és más jogi előírások összessége.[27] Az a jogi norma tekinthető érvényesnek, amelyet olyan jogszabályba foglalt jogtételek alkotnak, amelyek megfelelnek az érvényesség tételes jogi feltételeinek. Ezen pozitív jogi feltételek[28] alapján érvényességi kellék, hogy a jogszabály:

a) illeszkedjék a jogforrások hierarchiájába;
b) megfelelő jogalkotási jogkörrel felruházott szerv, megfelelő eljárása során kerüljön megalkotásra;

[25] Jat. 3-5. §-ai
[26] Jat. 2. § (2) bekezdés
[27] Jogi alaptan 225. oldal
[28] Jogi alaptan 261. oldal

c) megfelelő módon kerüljön kihirdetésre.

A Jat. szerint a jogszabályokat Magyarország hivatalos lapjában a Magyar Közlönyben kell kihirdetni, a minősített adatot nem tartalmazó közjogi szervezetszabályozó eszközt a Magyar Közlönyben kell közzétenni. A Magyar Közlönyt a kormányzati portálon történő elektronikus dokumentumként való közzététellel kell kiadni, szövegét hitelesnek kell tekinteni.[29]

További érvényességi kellék a jogi norma hatálya is. Az *időbeli hatály* kezdő időpontját, a hatálybalépés napját a jogszabályban kell meghatározni.[30] A kezdő időpont a kihirdetést követő valamely nap lehet. Ha a szabályozás célja másként nem érhető el, akkor a hatálybalépés lehet a kihirdetés napja (órában meghatározva), vagy arról külön törvényben kell rendelkezni. Ha naptári nap nem határozható meg, akkor a hatálybalépés valamely jövőbeli feltétel bekövetkeztének időpontjához is köthető. A hatálybalépés időpontját úgy kell meghatározni, hogy megfelelő felkészülési idő álljon rendelkezésre a jogszabály alkalmazására és arra, hogy a jogszabály címzettjei a megváltozott jogi környezethez alkalmazkodni tudjanak. Az időbeli hatály kapcsán ki kell emelni, hogy a kihirdetés és a hatálybalépés közötti megfelelő időtartam biztosítása a jogállamiság garanciális eleme, amely időszak alatt a jogszabály érvényes ugyan, de még nem hatályos. A jogszabályok *területi és személyi hatálya* összetartozik. A személyi hatály jogelméleti értelmében a területi hatály alóli kivételeket jelenti, és nem közvetlenül a jogszabályok címzettjeinek a körét szabja meg, hanem hogy ki lehet egyáltalán címzett.[31] Jogszabály területi hatálya Magyarország területére, ehhez kapcsolódóan személyi hatálya Magyarország területén tartózkodó személyekre és a magyar állampolgárokra, az önkormányzati rendelet területi hatálya a helyi önkormányzat közigazgatási területére, személyi hatálya az ezen a területen tartózkodó személyekre terjed ki. Ettől eltérő esetben a jogszabályban kifejezetten rendelkezni kell a területi és személyi hatályról.[32]

A jogszabály hatálya akkor szűnik meg, ha azt más jogszabály hatályon kívül helyezi, vagy ha a jogszabályt az Alkotmánybíróság vagy a bíróság megsemmisíti.[33]

A jog csak akkor tölti be társadalmi rendeltetését, ha ténylegesen érvényesül, ezért *jogérvényesülés*ről akkor beszélhetünk, ha a jogszabály az emberek magatartásában ténylegesen megvalósul, azaz a jogszabályok címzettjei követik az előírásokat vagy a normák

[29] Jat. 25. § és 26. § (1)-(2) bekezdés
[30] Jat. 7. §
[31] Jogi alaptan 263. oldal
[32] Jat. 6. §
[33] Jat. 10. §

megsértése esetén a kilátásba helyezett szankciókat ténylegesen alkalmazzák.[34] A jogérvényesülés alkalmával a jogszabályokban meghatározott előírások személyek vagy szervezetek jogaiként és kötelezettségeiként, a jogalanyok magatartásának formájában jelennek meg. Ezeket a magatartásokat abból a szempontból, hogy megfelelnek-e a jogszabályok előírásainak, *két nagy csoportra*[35] bonthatjuk:

1) *jogkövetés*, ha valamely magatartás a jogszabályok előírása szerint megy végbe, automatikusan, külső szerv közreműködése nélkül, és nem sért semmilyen jogi normát;
2) *jogsértés*, ha az adott magatartás jogellenes, azaz ellentétes valamilyen jogszabályi rendelkezéssel vagy azt megsérti. Ez esetben a jogérvényesülés a kilátásba helyezett szankció alkalmazását jelenti, általában állami kényszer segítségével. Valamennyi jogsértő magatartás közös vonása az adott magatartás társadalomra veszélyessége.

Jogsértés esetén a jog érvényesülése és a szankció alkalmazása összekapcsolódik annak a kérdésnek az eldöntésével, hogy szükség van-e jogérvényesítésre. A *jogérvényesítés* a jogellenes állapot megszüntetésére vagy a jogsértés jogkövetkezményeinek a megvalósítására irányul, melyet az erre feljogosított állami szervek végeznek el, amely tevékenységet *jogalkalmazásnak* nevezzük. A jogérvényesítést és a jogkövetést egyrészt logikai mellérendeltség jellemzi, mivel jogkövetés esetében nincs szükség a jog érvényesítésére, és a jog érvényesítése esetén nem beszélhetünk jogkövetésről, másrészt logikai alá-fölérendeltség jellemzi, mert a jogérvényesítés a jogosultak és a jogalkalmazók szempontjából egyben jogkövetés is.[36]

A jogszabályok alkalmazása és értelmezése során három alapelvet kell figyelembe venni: 1. a magasabb szintű jogszabály lerontja az alacsonyabb szintű jogszabályt, 2. a későbbi jogszabály lerontja a korábbi jogszabályt, 3. a különös jogszabály lerontja az általános jogszabályt.[37] A *jogszabály értelmezése* olyan tudatos megismerő tevékenység, amely a jogi norma, mint magatartásszabály tartalmának a feltárására irányul, mindig gyakorlati tevékenységhez és adott tényállásokhoz kapcsolódik.

A jogszabály-értelmezésnek sajátos módszerei[38] vannak, a *nyelvtani* (a jogszabály szótani és mondattani elemzése), a *logikai* (a fogalmak és kijelentések viszonyára vonatkozó törvényszerűségek és elvek feltárása), a *rendszertani* (a jogszabályt a jogintézmény, a jogág és a jogrendszer részeként elemzik) és a *történeti értelmezés* (a jogi norma céljának, valamint

[34] Jogi alaptan 280. oldal
[35] Jogi alaptan 281. oldal
[36] Jogi alaptan 282. oldal
[37] Jogi alaptan 308. oldal
[38] Jogi alaptan 314. oldal

a jogalkotó szándékának a vizsgálatára kerül sor), melyeket általában együttesen használnak.

A jogszabály-értelmezés eredménye[39] lehet *kiterjesztő* (ha a jogszabály tartalma és terjedelme tágabb, vagyis az az esetek és viszonyok szélesebb körére terjed ki), *helybenhagyó* (ha a jogszabály tartalma és terjedelme azonos) és *megszorító* (ha a jogszabály tartalma és terjedelme szűkebb annál, mint ami megállapítható volt) értelmezés.

2.3. A jogforrás és a jogforrási hierarchia

A jogforrás különböző jogszabályoknak (és azon keresztül a jogi normáknak) a jogrendszerben elfoglalt sajátos helyét, szerepét fejezi ki.[40] A jogforrások hierarchiája a jogrendszer egységét biztosítja[41], ennek keretében:

a) a jogszabályok között hierarchiát hoz létre, az ellentmondásokat a magasabb hierarchikus szint elsőbbsége alapján oldja meg;
b) az állami hierarchia magasabb szintjén álló állami szerv által kibocsátott jogszabállyal nem lehet ellentétes az alacsonyabb szinten elhelyezkedő állami szerv által alkotott jogszabály, azt nem módosíthatja és nem helyezheti hatályon kívül;
c) a jogforrások hierarchiájába ütköző jogszabály érvénytelen, azaz az érvénytelen jogszabály nem rendelkezik kötelező erővel.

A magyar jogforrási hierarchiát Magyarország Alaptörvényének T) cikke tartalmazza. Az Alaptörvény rendelkezése szerint jogszabály:

a) a törvény,
b) a kormányrendelet,
c) a miniszterelnöki rendelet,
d) a miniszteri rendelet,
e) a Magyar Nemzeti Bank elnökének rendelete,
f) a Nemzeti Média- és Hírközlési Hatóság és a Magyar Energetikai és Közmű-szabályozási Hivatal, mint önálló szabályozó szerv vezetőjének rendelete,
g) az önkormányzati rendelet,
h) a Honvédelmi Tanács rendkívüli állapot idején kiadott rendelete,
i) a köztársasági elnök szükségállapot idején kiadott rendelete.

[39] Jogi alaptan 315.oldal
[40] Jogi alaptan 225. oldal
[41] Jogi alaptan 245. oldal

Alapvetés, hogy jogszabály nem lehet ellentétes az Alaptörvénnyel. Az Alaptörvény ugyanakkor rögzíti azt is, hogy általánosan kötelező magatartási szabályt kizárólag az Alaptörvény és az Alaptörvényben megjelölt, jogalkotó hatáskörrel rendelkező szerv által megalkotott és a Magyar Közlönyben kihirdetett jogszabály állapíthat meg. Az Alaptörvény T. cikke vezette be az ún. sarkalatos törvény fogalmát, amely olyan törvény, amelynek elfogadásához és módosításához a jelen lévő országgyűlési képviselők kétharmadának szavazata szükséges.

A Jat. bevezeti az ún. közjogi szervezetszabályozó eszköz fogalmát, amely szerint a normatív határozatot és normatív utasítást kell közjogi szervezetszabályozó eszköznek tekinteni.[42]

a) A normatív határozatok (melyek különböznek az egyedi ügyekben hozott határozatoktól) célja, hogy az irányító szerepet betöltő testületi jellegű állami szervek szabályozzák saját szervezetüket, működésüket, megállapítsák a feladatkörükbe tartozó terveket. A Jat. szerint[43]:
   a) az Országgyűlés,
   b) a Kormány és más testületi központi államigazgatási szerv (pl.: a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2) bekezdés b) pontja szerinti kormánybizottság),
   c) az Alkotmánybíróság,
   d) a Költségvetési Tanács

   szervezetét, működését, tevékenységét, valamint cselekvési programját normatív határozatban szabályozhatja.

   Ilyen jogosultsággal rendelkezik továbbá a helyi önkormányzat képviselő-testülete a saját tevékenysége és cselekvési programja és az általa irányított szervek szervezete és működése vonatkozásában, valamint a nemzetiségi önkormányzat képviselő-testülete a saját és az általa irányított szervek esetében.
b) A normatív utasítás célja, hogy az arra jogszabály alapján feljogosított személy vagy szerv (pl.: miniszter, országos hatáskörű szerv vezetője) jogszabályban meghatározott irányítási jogkörében a közvetlen irányítása alá tartozó szervek szervezetét, működését, tevékenységét szabályozza. A Jat. szerint[44]:
   a) a köztársasági elnök,
   b) a miniszterelnök,

[42] Jat. 1. §
[43] Jat. 23. § (1)-(3) bekezdés
[44] Jat. 23. § (4) bekezdés

c) a központi államigazgatási szerv vezetője (kivéve a Kormány és más testületi központi államigazgatási szerv),
d) az Országos Bírósági Hivatal elnöke,
e) a legfőbb ügyész,
f) az alapvető jogok biztosa,
g) a Magyar Nemzeti Bank elnöke,
h) az Állami Számvevőszék elnöke,
i) a fővárosi és megyei kormányhivatal vezetője,
j) a polgármester, a főpolgármester, a megyei közgyűlés elnöke és a jegyző

normatív utasításban szabályozhatja a vezetése, az irányítása vagy a felügyelete alá tartozó szervek szervezetét és működését, valamint tevékenységét.

Törvényben meghatározott tárgykörben normatív utasítást adhat ki az Országgyűlés, a köztársasági elnök, az Alkotmánybíróság, az alapvető jogok biztosa, a Nemzeti Média- és Hírközlési Hatóság és a Magyar Energetikai és Közmű-szabályozási Hivatal, valamint a Miniszterelnökség és a minisztérium hivatali szervezetének vezetője, amely a szerv állományába tartozó személyekre kötelező.[45]

A közjogi szervezetszabályozó eszköz jogszabállyal nem lehet ellentétes, jogszabály rendelkezése nem ismételhető meg benne. A közjogi szervezetszabályozó eszközökre vonatkozó kiadási jogosultság nem befolyásolja az egyedi határozat vagy egyedi utasítás kiadására vonatkozó jogát az arra feljogosított személynek, szervnek.[46]

Törvényi felhatalmazás alapján kiadott, az állami szerv vagy köztestület tevékenységét és működését szabályozó más jogi eszköz jogszabállyal és közjogi szervezetszabályozó eszközzel nem lehet ellentétes.

2.4. Az elektronikus információbiztonság a magyar jogrendszerben

Napjainkban a társadalmi és gazdasági folyamatok főként információs hálózatokon keresztül kerülnek bonyolításra, amely főáram létrehozott egy új fogalmat, a kibertér fogalmát. A globális kibertér létező valóság, globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és

[45] Jat. 23. § (5) bekezdés
[46] Jat. 24. §

információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.[47] A kibertér veszélyforrásai, az onnan érkező támadások és káros hatások egyre nagyobb biztonsági kockázattal járnak és kihatnak a kapcsolódó elektronikus információs rendszerekre is. Az állam és a társadalom működését lehetővé tevő informatikai infrastruktúrák védelme, a biztonság megerősítése és fenntartása kormányzati és társadalmi igénnyé, ezáltal kiemelt feladattá vált. Jelen alcím az elektronikus információbiztonság újonnan kialakított szabályozási környezetének középpontba helyezésével és a kapcsolódó egyéb szabályozások felhívásával – a rendszertani megközelítésre fókuszálva – mutatja be az elektronikus információbiztonság hatályos jogi környezetét. A fejezet fő célja, hogy rávilágítson a terület főbb szabályaira és sajátosságaira, a részletszabályok megismeréséhez szükséges hivatkozások megadása mellett.

2.4.1. Magyarország Nemzeti Kiberbiztonsági Stratégiája

A törvényalkotás egyik előfeltétele az a stratégiai tervdokumentáció, amelyben az egyes szakterületeket érintően megfogalmazott célok és azok elérésének lehetséges módjai meghatározásra kerülnek. A kiberbiztonság[48] területét illetően ez a dokumentum a 2013 márciusában elfogadott *Magyarország Nemzeti Kiberbiztonsági Stratégiája*[49] (a továbbiakban: Kiberstratégia). A Kiberstratégia a globális kibertér részét képező magyar kibertér[50] szabad, jogállami és biztonságos működését Magyarország alapvető értékének és érdekének tekinti. A rögzített nemzeti célok és cselekvési területek a magyar kibertérre vonatkoznak, amelynek biztonságos és megbízható környezetnek kell lennie az egyének és közösségek, a gazdasági szereplők, a jövő generációi, valamint az elektronikus közigazgatás számára.[51] Elérendő nemzeti célként került rögzítésre a nemzeti adatvagyon megfelelő szintű védelme és annak igénye, hogy Magyarország a magyar kibertér fenyegetése, támadása, illetve vészhelyzet és vétlen információszivárgás esetén hatékony megelőzési, észlelési, reagálási, válaszadási és helyreállítási képességekkel rendelkezzen.[52]

[47] Ibtv. 1. § 22. pont
[48] Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez – Ibtv. 1. § (1) bekezdés 26. pont.
[49] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm. határozat (a továbbiakban: Kiberstratégia)
[50] Magyar kibertér: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne - Ibtv. 1. § (1) bekezdés 35. pont
[51] Kiberstratégia 8. pont
[52] Kiberstratégia 9. pont

A kitűzött célok eléréséhez és a kiberbiztonság megfelelő szinten tartásához, folyamatos fejlesztéséhez a Kiberstratégia kilenc cselekvési területet azonosít, továbbá rögzíti azokat a kormányzati eszközöket, kompetenciákat és erőforrásokat, amelyekkel Magyarország már rendelkezik.[53] A nemzeti cselekvési területek között külön jelentősége van a *kormányzati koordinációnak* (részletesen a 4.2.1. alcím alatt), amely fő célja a kormányon belüli, továbbá az állami, gazdasági, tudományos és civil szereplők közötti együttműködés koordinációjának elősegítése és a végrehajtás figyelemmel kísérése testület útján.

A további cselekvési területek között szerepel az *Együttműködés* (a kormányzat, a civil, a gazdasági és a tudományos területek képviselőinek részvételével), a *Szakosított intézmények* működtetése a kibervédelem területén (speciális szakértelemmel és hatáskörrel rendelkező szervezetek útján), a többlépcsős *Szabályozás*, Magyarország aktív szerepének további erősítése a *Nemzetközi együttműködés*ben, a *Tudatosság*növelés támogatása, az *Oktatás, kutatás-fejlesztés* (a kiberbiztonság szakterületének beépítése az oktatásába, stratégiai együttműködés kialakítása az állam és a tudományos kutatóhelyek között), a *Gyermekvédelem* (a biztonságos online környezet megteremtése) és a *Gazdasági szereplők motivációja* (ösztönzés a magas szintű kiberbiztonsági védelem kialakítására az infokommunikációs eszközgyártók és szolgáltatók esetében).

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

A Kiberstratégia cselekvési területei között szereplő többlépcsős szabályozási környezet kialakítása során az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és a felhatalmazása alapján megalkotott számos végrehajtási rendelet megteremtette a kibervédelem általános jogi alapjait Magyarországon.

2.4.2.1. Az Ibtv. alapvetése, fogalmi rendszere és hatálya

Az Ibtv. a megelőzést, a biztonságot és a védelmet, mint alapelveket már a preambulumban hangsúlyozza, az ott megjelenő *fenyegetés*[54] *bizalmasság*[55], *sértetlenség*[56] és *rendelkezésre*

[53] Kiberstratégia 10. és 11. pont
[54] Ibtv. 1. § (1) bekezdés 19. pont
[55] Ibtv. 1. § (1) bekezdés 8. pont
[56] Ibtv. 1. § (1) bekezdés 39. pont

állás[57] az értelmező rendelkezések között önálló fogalomként kapnak helyet, amelyek a jogi szabályozás keretét alkotják. Azt a tulajdonságot, amely arra vonatkozik, hogy az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és jogosultságuk szintje szerint ismerhetik meg és használhatják fel bizalmasságnak, az elektronikus információs rendszer rendeltetésének megfelelő használhatóságát, valamint az adat hitelességét és származásának ellenőrizhetőségét sértetlenségnek nevezzük. Az elektronikus információs rendszer jogosultság szerinti elérhetőségét és a kezelt adatok felhasználhatóságát tekintjük a rendelkezésre állás követelményének.

Az egységes jogértelmezés és a jogalkalmazás érdekében az Ibtv. olyan szakkifejezésekre építve rögzíti az értelmező rendelkezéseket, melyeket már a gyakorlatban alkalmaznak és amelyeknek jelentős része igazodik a szakterület nemzetközi dokumentumaiban foglaltakhoz, az ISO/IEC 27000-es szabványsorozathoz és a Common Criteria (Közös Követelmények) elveihez. (Az Ibtv. értelmező rendelkezéseinek kivonatát az 1. melléklet tartalmazza.)

A védelem biztosítása olyan alapkövetelmény, amely indokolja, hogy az Ibtv. magát a védelmi feladatokat[58] is rögzítse, így védelmi feladatok alatt a *megelőzést*[59], a *korai figyelmeztetést*[60], az *észlelést*[61], a *reagálást*[62], és az *eseménykezelést* kell érteni. Ez a tartalom a gyakorlatban is alkalmazott védelmi módszerre, az ún. PreDeCo (Preventive-Detective-Corrective) elvre épít, amely az elvárt védelmi hatás eléréséhez három összefüggő és egymást kiegészítő részre, a megelőző (preventív), a felismerő (detektív) és az elhárító (korrektív) intézkedésekre helyezi a hangsúlyt. A védelmi intézkedéseknek *ún. kockázatokkal arányos védelem*[63] útján szükséges megvalósulniuk, azaz a védelmi intézkedésekre fordított költségeknek arányosnak kell lenni a fenyegetések által okozható károk értékével. Az Ibtv. rögzíti a védelem különböző formáit, az *adminisztratív*[64], a *fizikai*[65] és a *logikai*[66] védelmi intézkedéseket, amelyeknek támogatniuk kell a védelmi feladatok ellátását. Az Ibtv. általános biztonsági követelményként rögzíti az elektronikus információs rendszereknek azt az állapotát, amely során a teljes *életciklus*ban[67] meg kell valósítani, hogy az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és

[57] Ibtv. 1. § (1) bekezdés 38. pont
[58] Ibtv. 1. § (1) bekezdés 46. pont
[59] Ibtv. 1. § (1) bekezdés 36. pont
[60] Ibtv. 1. § (1) bekezdés 32. pont
[61] Ibtv. 1. § (1) bekezdés 17. pont
[62] Ibtv. 1. § (1) bekezdés 37. pont
[63] Ibtv. 1. § (1) bekezdés 31. pont
[64] Ibtv. 1. § (1) bekezdés 6. pont
[65] Ibtv. 1. § (1) bekezdés 20. pont
[66] Ibtv. 1. § (1) bekezdés 34. pont
[67] Ibtv. 1. § (1) bekezdés 16. pont

rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása *zárt*[68], *teljes körű*[69], *folytonos*[70] és kockázatokkal arányos védelmére kerüljön sor.[71] Ezen védelmi intézkedések célja, hogy a biztonsági események[72] bekövetkezésének a valószínűsége és az okozott kár minimalizálható legyen. Ha sor kerül a biztonsági esemény bekövetkezésére az azonnali észlelés és az eseménykezelés[73] kiemelt fontosságú, ehhez hiteles dokumentálás, felszámolás és kárfelmérés, továbbá a felelősség megállapítása szükséges.

Az Ibtv. a tárgyi hatály megállapításához rögzíti, hogy alkalmazásában mit tekint elektronikus információs rendszernek. E szerint elektronikus információs rendszernek[74] kell tekinteni:

1. az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttesét, ezen belül:
   a) a számítástechnikai rendszereket és hálózatokat;
   b) a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatokat, szolgáltatásokat;
   c) a rádiós vagy műholdas navigációt;
   d) az automatizálási, vezérlési és ellenőrzési rendszereket (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);
   e) az a)-d) pontok felderítéséhez, lehallgatásához vagy zavarásához használható rendszereket.
2. az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön, egymással összefüggő eljárásokkal azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.

A személyi hatály meghatározása az alkotmányos rend és a közigazgatás hatékony működésének fenntartása esetében kiemelt jelentőségű, valamint a nemzeti adatvagyon kezelését ellátó szervezetekre helyezi a hangsúlyt. A személyi hatály alá tartozó szervezetek körét[75] a 2. melléklet tartalmazza.

[68] Ibtv. 1. § (1) bekezdés 48. pont
[69] Ibtv. 1. § (1) bekezdés 44. pont
[70] Ibtv. 1. § (1) bekezdés 21. pont
[71] Ibtv. 5. § és Ibtv. 1. § (1) bekezdés 15. pont
[72] Ibtv. 1. § (1) bekezdés 9. pont
[73] Ibtv. 1. § (1) bekezdés 10. pont
[74] Ibtv.1. § (2) és (3) bekezdés
[75] Ibtv. 2. §

Az Ibtv. Magyarország területén kívül korlátozza az elektronikus információs rendszerekben történő adatkezelést és előírja, hogy a személyi hatály alá tartozó szervek és a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói – lásd 2. melléklet – az általuk kezelt, a nemzeti adatvagyon részét képező adatokat csak Magyarország területén üzemeltetett elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerben kezelhetnek.[76] Ez a tiltó rendelkezés nem terjed ki a Magyar Honvédségre.

Európai létfontosságú rendszerelem vagy nemzeti létfontosságú rendszerelem esetében az elektronikus információs rendszer – tekintettel arra, hogy az uniós szabályozás és az uniós országok nemzeti szabályozása megfelelő védelmet és ellenőrizhetőséget biztosít – az Európai Unió tagállamai területén is üzemeltethető.[77] Ez alól kivétel, ha az európai létfontosságú rendszerelem és a nemzeti létfontosságú rendszerelemben kezelt adat a nemzeti adatvagyon része, ez esetben az adatkezelés csak Magyarországon történhet.

Az Ibtv. a személyi hatálya alá tartozó szervek – lásd 2. melléklet – esetében biztosítja az Európai Unió területén üzemeltetett elektronikus információs rendszerekben történő adatkezelést is, amennyiben erre a Nemzeti Elektronikus Információvédelmi Hatóság engedélyével vagy nemzetközi szerződésben előírt kötelezettség alapján kerül sor.[78] Kivétel ez alól a Magyar Honvédség, ahol nemzetközi szerződés alapján, nemzetbiztonsági érdekből az Európai Unió területén kívül üzemeltetett elektronikus információs rendszerekben is kezelhetőek adatok. A rendészeti, honvédelmi, nemzetbiztonsági, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerek és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró vagy törvényi felhatalmazás alapján speciális feladatokat ellátó információs rendszerek esetében az Európai Unión belüli adatkezelést az irányítást ellátó miniszter rendeletében meghatározott és hatósági feladatot ellátó szervezeti egység engedélyezi.

2.4.2.2. Az elektronikus információs rendszerek biztonsági osztályba sorolása és a szervezetek biztonsági szintbe sorolása

Az elektronikus információs rendszer vagy rendszerelem, és az ezekben kezelt adatok kockázatokkal arányos védelmének kialakításához az Ibtv. hatálya alá tartozó szervezetnek minden egyes elektronikus információs rendszerre vonatkozóan a bizalmasság, a sértetlenség,

[76] Ibtv. 3. § (1) bekezdés
[77] Ibtv. 3. § (2) bekezdés
[78] Ibtv. 3. § (3) bekezdés

valamint a rendelkezésre állás alapján, önbesorolás útján, dokumentált módon, 1-től 5-ig terjedő számozással ellátott skálán el kell végeznie a biztonsági osztályba sorolást.[79] A biztonsági osztályba sorolás célja, hogy a felmért kockázatok[80] alapján az elektronikus információs rendszer védelmének elvárt erőssége meghatározásra kerüljön, amelynek a kockázatokkal és a ráfordított költségekkel arányosnak kell lennie. A besorolás alapján meghatározott biztonsági osztály alapján kell megvalósítani az elektronikus információs rendszer teljes életciklusában a zárt, teljes körű, folytonos és kockázatokkal arányos védelmet úgy, hogy a szervezetnek meg kell határoznia a külön rendeletben előírt logikai, fizikai és adminisztratív védelmi intézkedéseket. A védelem elektronikus információs rendszerenként eltérő lehet, azonban minden esetben támogatnia kell a megelőzést, a korai figyelmeztetést, az észlelést, a reagálást és a biztonsági események kezelését.[81]

A biztonsági osztályba sorolással párhuzamosan önértékelés útján, dokumentált módon kell elvégezni a szervezet biztonsági szintbe sorolását is, amely a szervezetnek arra a felkészültségi szintjére vonatkozik, hogy elektronikus információs rendszereinek védelmét a bizalmasság, a sértetlenség, és a rendelkezésre állás alapján hogyan, a kockázatokkal mennyire arányosan és költséghatékonyan biztosítja.[82] Az Ibtv. alapelvként rögzíti, hogy a szervezet biztonsági szintje azonos a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával, azzal, hogy meghatározásra kerül az a minimum alapbiztonsági szint, amelyet a szervezetnek el kell érnie. Az egyes szervezetekhez tartozó alapbiztonsági szinteket a 3. melléklet tartalmazza. Például: ha egy központi államigazgatási szerv olyan elektronikus információs rendszert kezel, melyben az információk bizalmassági, sértetlenségi és rendelkezésre állási besorolása 2-es, a szervezeti biztonsági szintje akkor is 3., mivel központi államigazgatási szerv esetében 3-as az alap biztonsági szint. Ha ennél a szervezetnél olyan elektronikus információs rendszert kezelnek, amely biztonsági osztályba sorolása eléri a 4. szintet, a szervezet biztonsági szintjét is a 4. szinten kell meghatározni.

A biztonsági osztályba és a biztonsági szintbe soroláshoz rendelt követelményeket az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és a biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet (a továbbiakban: technológiai rendelet) tartalmazza. Az elektronikus információs rendszerek biztonsági

[79] Ibtv. 1. § (1) bekezdés 11. pont és 7. § (1) és (2) bekezdés
[80] Ibtv. 1. § (1) bekezdés 28. pont
[81] Ibtv. 7. § (4) bekezdés
[82] Ibtv. 1. § (1) bekezdés 13. pont

osztályba sorolását a technológiai rendelet 1. mellékletében, a szervezet biztonsági szintbe sorolását a technológiai rendelet 2. mellékletében foglaltak szerint kell elvégezni. A megállapított biztonsági osztályhoz és biztonsági szinthez rendelt követelményeket a technológiai rendeletnek az „Adminisztratív, fizikai és logikai biztonsági követelmények" című 4. mellékletében meghatározott előírások alapján kell megvalósítani. A védelmi intézkedések körében meghatározott feltételek fennállása esetén a szervezet sajátosságaihoz igazodóan egyedi eltéréseket állapíthat meg, illetve egyes eljárásokat, mint helyettesítő biztonsági intézkedéseket alkalmazhat.[83] A besorolás elvégzéséhez kapcsolódó útmutatót a technológiai rendelet 3. melléklete tartalmazza. Speciális szabály, hogy ha az adott elektronikus információs rendszert több szervezet használja, az üzemeltetőnek kell gondoskodnia a technológiai követelmények érvényesítéséről, azzal, hogy a követelmények, feltételek, elvárások az érintett szervezet elektronikus információbiztonsággal kapcsolatos eljárásrendjébe beépüljenek.[84]

A kezdő alapállapot rögzítéséhez a már működő elektronikus információs rendszerek biztonsági osztályba sorolását és a szervezet biztonsági szintjének meghatározását első alkalommal az Ibtv. hatálybalépését követő egy éven belül, 2014. július 1-ig kell elvégezniük a szervezeteknek.[85] Az így megállapított biztonsági osztály és biztonsági szint alapján szükséges biztonsági intézkedések megtétele során a fokozatosság elve kerül érvényesítésre, mivel minden egyes következő, magasabb biztonsági osztályhoz és biztonsági szinthez rendelt biztonsági intézkedés kivitelezésére és az előírt biztonsági osztály és biztonsági szint elérésére két év áll rendelkezésre a szervezetek számára.[86] Ha például egy szervezet az önbesorolás alapján elektronikus információs rendszerét 2. biztonsági osztályba sorolja 2014 júliusában, azonban a reá irányadó érték a 4-es, akkor a szervezet biztonsági szintje is 4-es lesz. Ez esetben a 3-as biztonsági osztály és biztonsági szint elérésére 2 év – 2016 júliusáig –, a 4-es biztonsági osztály és biztonsági szint elérésére további 2 év áll rendelkezésére – 2018 júliusáig –, összesen tehát 4 év alatt kell a megfelelő biztonsági osztályt és biztonsági szintet a szervezetnek elérnie. Kiegészítő szabály, hogy ha a szervezet biztonsági szintje az

[83] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és a biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet (a továbbiakban: technológiai rendelet) 4. melléklet 2. pont.
[84] Technológiai rendelet 3. §
[85] Ibtv. 26. §
[86] Ibtv. 8. § (3) bekezdés és 10. § (4) bekezdés

önbesorolás alapján az 1. biztonsági szintet nem éri el, az 1. biztonsági szint eléréséhez szükséges intézkedéseket a vizsgálatot követő egy éven belül meg kell tenni.[87]

Főszabály, hogy a biztonsági osztályba és a biztonsági szintbe sorolást legalább háromévenként kell elvégezni, azonban az elektronikus információs rendszer biztonságát érintő – biztonsági osztályba sorolásnál jogszabályban meghatározott – változás vagy új elektronikus információs rendszer bevezetése esetén soron kívüli felülvizsgálatot kell elvégezni. Soron kívül kell felülvizsgálni a biztonsági osztályt a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás esetén.[88] A szervezetnek tehát folyamatában kell figyelemmel kísérnie a felmerült kockázatokat, ezért a kezdő állapot rögzítését követően a biztonsági osztályba és a biztonsági szintbe sorolást három éves időszakonként kell megismételni.

Az elektronikus információs rendszerek sajátosságait, a szervezet feladat- és hatáskörét figyelembe véve a szervezet vezetőjének lehetősége van arra, hogy az irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthasson az elektronikus információs rendszerre vonatkozóan vagy az irányadó biztonsági szintnél magasabb biztonsági szintet állapítson meg a szervezet esetében.[89] Ezen egyedi esetek körét – sajátos jellegük alapján – jogszabályi szinten nem indokolt és teljes körűen nem is lehet rögzíteni, így megalapozottságukat ellenőrzés keretében az arra jogosult hatóság vizsgálja. A hatóság a szervezet által megállapított biztonsági osztályt és biztonsági szintet felülbírálhatja és magasabb – indokolt esetben alacsonyabb – szintű besorolást is megállapíthat.[90] Ez a felülbírálati jogosítvány nem vonatkozik azonban a minősített adatokat kezelő elektronikus információs rendszerekre, valamint az ún. zárt célú elektronikus információs rendszerek és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró vagy törvényi felhatalmazás alapján speciális feladatokat (pl.: médiaszolgáltatási és elektronikus hírközlési tevékenység) ellátó elektronikus információs rendszerekre.[91]

A biztonsági osztályba és a biztonsági szintbe sorolás eredményét a szervezet informatikai biztonsági szabályzatában kell rögzíteni.[92] Ha a biztonsági osztályba és a biztonsági szintbe sorolás alkalmával a szervezet az adott elektronikus információs rendszerére vonatkozóan hiányosságot állapít meg, vagy megállapításra kerül, hogy a szervezet biztonsági szintje

[87] Ibtv. 10. § (3) bekezdés
[88] Ibtv. 8. § (1) és (2) bekezdés, 10. § (5) és (6) bekezdés
[89] Ibtv. 7. § (5) bekezdés és 9. § (3) bekezdés
[90] Ibtv. 8. § (6) bekezdés és 9. § (4) bekezdés
[91] Ibtv. 2. § (3) és (4) bekezdés
[92] Ibtv. 7. § (3) bekezdés és 10. § (8) bekezdés

alacsonyabb az előírt alap biztonsági szintnél, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie.[93] A cselekvési terv készítése az elektronikus információs rendszer biztonságát érintő változás vagy új elektronikus információs rendszer bevezetésekor elvégzett soron kívüli felülvizsgálat esetén is kötelező, amennyiben a felülvizsgálat eredménye alapján meghatározott biztonsági szint alacsonyabb, mint a szervezetre előírt alap biztonsági szint.[94]

2.4.3. Az elektronikus információbiztonsághoz kapcsolódó fontosabb törvények

1. Az Ibtv. szabályozási területéhez kapcsolódó további törvényi szabályozást a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) tartalmaz, mivel az Ibtv. tárgyi hatálya kiterjed az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemekre is. A szabályozás alapvető célja a veszélyeztetett létfontosságú rendszerek és létesítmények azonosítására és kijelölésükre vonatkozó alapszabályok és a veszélyeztetett területek, ágazatok rögzítése. Az Lrtv. ilyen veszélyeztetett ágazatnak tekinti az energetika, a közlekedés, az agrárgazdaság, az egészségügy, a pénzügy, az ipar, az infokommunikáció, a vízügy, a kormányzat és a közbiztonság ágazatát. A felsorolt ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna, létfontosságú rendszerelemnek tekintendő.[95] Alapvetően létfontosságúnak kell tekinteni minden olyan rendszert, rendszerelemet vagy létesítményt, amely a lakosság ellátása és a társadalom zavartalan működése szempontjából kiemelt jelentőségű, és sajátos tulajdonságai miatt nincs olyan helyettesítő eszköz, amely kiesés esetén pótolhatja működését. Az egyértelmű elhatárolás és a gyakorlati alkalmazhatóság szempontjából az Lrtv. rögzíti, hogy mit kell európai- és nemzeti létfontosságú rendszerelemnek tekinteni.[96] (Az Lrtv. értelmező rendelkezéseinek kivonatát az 1. melléklet tartalmazza.)

[93] Ibtv. 8. § (5) bekezdés és 10. § (2) bekezdés
[94] Ibtv. 10. § (7) bekezdés
[95] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) 1. § f) pont és 1-3. mellékletei
[96] Lrtv. 1. § c) és g) pont

Az ágazatokon belüli, ún. alágazatokra vonatkozó felosztást az Lrtv. 1-3. melléklete tartalmazza, azzal, hogy az energetika, mint speciális ágazati sajátosságokkal rendelkező szektor esetében különleges szabályok kerültek az Lrtv.-ben rögzítésre.[97]

A nemzeti létfontosságú rendszerelemmé történő kijelölés tagállami (nemzeti) hatáskör. A kijelölést az üzemeltető vagy a javaslattevő hatóság ún. azonosítási jelentés benyújtásával kezdeményezheti az ágazati kijelölő hatóságnál.[98] Az eljárás a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény rendelkezései szerinti hatósági eljárásnak minősül, amely során az ágazati kijelölő hatóság az ún. ágazati és horizontális kritériumok[99] alapján határozathozatallal dönt. A döntés során meghatározásra kerül az a határidő, amely időpontig az üzemeltetőnek biztonsági tervet kell kidolgoznia és rögzítésre kerülnek a létfontosságú rendszerelem védelmével összefüggő, a rendszerelem egyedi sajátosságaihoz, környezetéhez, a veszély mértékéhez igazodó feltételek.[100] Az európai létfontosságú rendszerelemek kijelölése nem nemzeti hatáskör, a kijelölési folyamat vagy Magyarországon belül, az üzemeltető vagy a javaslattevő hatóság kérelmére, vagy pedig valamely EGT-állam kezdeményezésére indulhat meg. A kijelölés legalább kettő tagállam együttműködését, megállapodását és nemzetközi szerződés megkötését igényli. A nemzetközi szerződésben foglaltak alapján az ágazati kijelölő hatóság határozatot hoz, amelyben rögzíteni kell az üzemeltető számon kérhető kötelezettségeit, azok végrehajtásának határidejét és ellenőrzését.[101]

A kijelölő hatóság határozata alapján az üzemeltetőnek kötelezettsége van arra nézve[102], hogy az előírt határidőn belül kidolgozza az üzemeltetői biztonsági tervet, azt megküldje a nyilvántartó hatóságnak és az ágazati kijelölő hatóságnak, továbbá a védelmet és annak folyamatos működését az abban rögzítettek alapján szervezze meg. További kötelezettsége, hogy kijelölje a megfelelő szakirányú végzettséggel rendelkező biztonsági összekötő személyt.[103] Az ágazati kijelölő hatóság az üzemeltető kötelezettségszegése esetén – a fokozatosság elvét szem előtt tartva – határozatban felszólítja az üzemeltetőt a kötelezettségek

[97] Lrtv. 10-12. §-ok
[98] Lrtv. 2. § (1) bekezdés
[99] Lrtv. 1. § a) és d) pont
[100] Lrtv. 1. § e pont és 2. § (3) bekezdés
[101] Lrtv. 3. §
[102] Lrtv. 6. § (1) és (3) bekezdés, valamint 7. §-a
[103] Lrtv. 6. § (7) bekezdés

betartására, kötelezi a biztonsági terv módosítására vagy új biztonsági terv készítésére, végső esetben 100 ezer forinttól 3 millió forintig terjedő bírságot szab ki.[104]

2. Bizonyos védelmi szempontok – kül- és belbiztonság, adat- és információvédelem – alapján szükséges, hogy az Ibtv. rendelkezései korlátok között érvényesüljenek, ezért a minősített adatokat kezelő elektronikus információs rendszereket érintően a minősített adat védelméről szóló 2009. évi CLV. törvényben (a továbbiakban: Mavtv.) meghatározott eltérésekkel kell az Ibtv.-t alkalmazni. Minden olyan szervnél, ahol a minősített adat kezelése elektronikus információs rendszerben történik, a Mavtv. és az Ibtv., valamint végrehajtási rendeleteiben meghatározott elektronikus biztonsági feltételeket – azaz a bizalmasság, sértetlenség és rendelkezésre állás figyelembevételével, a zárt, teljes körű, folytonos és kockázatokkal arányos védelmet –, és az adat minősítési szintjének megfelelő biztonsági feltételeket kell megteremteni.[105]

3. Az Ibtv. személyi hatálya kiterjed az adatok védelme terén kiemelt jelentőségű szabályozást tartalmazó, a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény szerinti nemzeti adatvagyon[106] adatfeldolgozóira is. Kiemelt cél a nemzeti adatvagyon körébe tartozó nyilvántartások biztonságának megteremtése, és a nyilvántartások jogszerű felhasználását akadályozó cselekmények bűncselekménnyé nyilvánításával azok megelőzése. A törvény végrehajtási rendelete[107] rögzíti a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóinak körét.

4. További kapcsolódó szabályozást az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény tartalmaz, amelyben az adatbiztonság és az adatok védelmére vonatkozó kötelezettség alapelvként jelenik meg és amely rögzíti az adatkezelés során elvárt adatbiztonsági előírásokat. A megfogalmazott alapelvekhez igazodóan az elektronikus információs rendszerben kezelt adatok védelmének speciális szabályait az Ibtv. tartalmazza.

5. Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény 2015. január 1-jén lép hatályba. Célja az eltérő állami

[104] Lrtv. 9. §-a és a Lrtv. vhr. 9. §-a
[105] A minősített adat védelméről szóló 2009. évi CLV. törvény 10. § (4) bekezdés
[106] Nemzeti adatvagyon: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége - a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 1. § 1. pont.
[107] A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet.

adatbázisokban kezelt adatok felhasználásának egycsatornássá tétele és a hatósági eljárások, adatigénylések egyszerűsítése. A törvény a megelőzést hangsúlyozva, a hatálya alá tartozó nyilvántartások együttműködési képességének biztosítása és az adatkapcsolatok biztonságának érdekében előírja, hogy a nyilvántartást vezető szervnek vagy személynek gondoskodnia kell a nyilvántartások elektronikus információs rendszerének tervezése, kialakítása és működtetése során az Ibtv. előírásainak való megfeleléséről.[108]

2.4.4. Nyilvántartási rendszer

Az információbiztonsággal kapcsolatos nyilvántartásokat a Nemzeti Elektronikus Információvédelmi Hatóság vezeti a szervezetek részére előírt bejelentési kötelezettség teljesítésével végzett adatszolgáltatás alapján. A nyilvántartás tartalmazza[109] a szervezet:

a) azonosításához szükséges adatokat,
b) elektronikus információs rendszereire (megnevezés, biztonsági osztály, technikai adatok), a szervezet biztonsági szintjére vonatkozó adatokat,
c) elektronikus információs rendszere(i) biztonságáért felelős személynek a személyazonosító adatait, elérhetőségeit, a feladatellátásához szükséges felsőfokú végzettségére és szakképzettségére vonatkozó adatokat,
d) informatikai biztonsági szabályzatát és
e) biztonsági eseményekkel kapcsolatos bejelentéseit.

A Hatóság a nyilvántartás adataiból – ha törvény eltérően nem rendelkezik – adattovábbítást nem végezhet, és a nyilvántartásból a szervezet által bejelentett adatokat az adat változásának, illetve a szervezet tevékenysége befejezésének bejelentését követő 5 év elteltével törölnie kell.[110]

A szervezeteknek az Ibtv. hatálya alá tartozó tevékenység megkezdését megelőző 8 napon belül kell eleget tennie a Hatóság részére történő adatközlési kötelezettségének, amely során meg kell küldeni az informatikai biztonsági szabályzatot, valamint – ha azzal a szervezet rendelkezik – a kiadott biztonsági tanúsítványt. A kötelezettség teljesíthető elektronikus úton (ÁNYK-űrlap benyújtás támogatási szolgáltatás igénybevételével vagy az elektronikus űrlapnak e-mailen való megküldésével), vagy postai úton. A Hatóság a beérkezett adatok alapján – ha szükséges hiánypótlási eljárás lefolytatását követően –, az adatokat

[108] Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény 3. §
[109] Ibtv. 15. § (1) bekezdés
[110] Ibtv. 15. § (4)-(6) bekezdés

nyilvántartásba veszi és a nyilvántartásba vételről tájékoztatja a szervezetet. A szervezetnek az adataiban bekövetkező változás bejelentéséről a változást követően, a tevékenység befejezéséről a tevékenység befejezését megelőzően, 8 napon belül kell gondoskodnia.[111]

Az Lrtv. szerint a létfontosságú rendszerekkel kapcsolatban a kijelölt ágazati nyilvántartó hatóság – a kijelölési eljárásban hozott hatósági határozat alapján – nyilvántartja és kezeli[112]:

a) az üzemeltetőre, a biztonsági összekötő személyre vonatkozó adatokat,
b) azon nemzeti létfontosságú rendszerelemek és azon európai létfontosságú rendszerelemek megnevezését, amelyek esetében Magyarország érintett fél,
c) az üzemeltetői biztonsági tervet,
d) az ágazati kijelölő hatóságnak azon határozatát, amely az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem kijelölése visszavonásáról rendelkezik.

2.4.5. Az elektronikus információs rendszerek védelmét biztosító főbb feladatok és kötelezettségek, a kapcsolódó felelősségi szabályok

2.4.5.1. Személyhez kötött főbb feladatok és kötelezettségek

A) Az Ibtv. az elektronikus információs rendszer védelmét biztosító kötelezettségek körében rendelkezik a *szervezet vezetőjének* szerepvállalásáról[113], aki munkáltatói jogkörében eljárva kinevezi, vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt, továbbá köteles gondoskodni az oktatásról és az információbiztonsági ismeretek szinten tartásáról.[114] Feladatkörében eljárva jóváhagyja az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe sorolását, továbbá felel a biztonsági osztályba sorolás és a biztonsági szint meghatározás jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.[115] Biztonsági esemény bekövetkezésekor a szervezet vezetőjének a feladata, hogy gondoskodjon a gyors és hatékony reagálásról, a biztonsági esemény kezeléséről. A szabályozás tárgykörét érintően feladata, hogy kiadja az informatikai biztonságpolitikát, meghatározza az informatikai biztonsági

[111] Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet
[112] Lrtv. 5. §
[113] Ibtv. 11. § (1) bekezdés és 12. §
[114] Ibtv. 11. § (1) bekezdés d) - f) pontok
[115] Ibtv. 7. § (3) bekezdés és 10. § (8) bekezdés.

stratégiát, továbbá ezen dokumentumok és a biztonsági osztályba és a biztonsági szintbe sorolás eredményének figyelembevételével kiadja az informatikai biztonsági szabályzatot.[116]

Ha a szervezet az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában, illetve adatkezelési vagy adatfeldolgozási tevékenységéhez vesz igénybe közreműködőt, a szervezet vezetőjének kötelezettsége arról gondoskodni, hogy az Ibtv.-ben foglaltak a létrejött jogviszony keretein belül szerződéses kötelemként teljesüljenek. E szabálytól eltérést azok az esetek képeznek, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe vennie.[117] Ez esetben az elektronikus információs rendszer védelmét szolgáló intézkedések végrehajtását a szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval és a szervezet vezetőjével együtt.[118]

B) Az *elektronikus információs rendszer biztonságáért felelős személy* a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladatok ellátásáért felel.[119] Ezen feladatokat csak büntetlen előéletű, a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel rendelkező személy láthatja el.[120] Feladatkörében eljárva előkészíti az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe történő besorolását, a besorolás eredményeinek figyelembevételével az informatikai biztonsági szabályzatot. Az elektronikus információs rendszerek tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában, illetve az adatkezelésben vagy az adatfeldolgozásban közreműködők igénybevétele során – át nem ruházható feladatkörében – biztosítja az Ibtv.-ben meghatározott követelmények teljesülését.[121]

C) Az *elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy*re vonatkozóan az Ibtv. – a képzésen való részvételre kötelezés mellett – külön feladatokat nem állapít meg. Ezek rögzítésére – az Ibtv. alapelveinek figyelembevételével – a szervezetre vonatkozó belső szabályozókban és a munkaköri leírásban kerülhet sor.

[116] Ibtv. 11. § (1) bekezdés c) és g) pont
[117] A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet és a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.
[118] Ibtv. 11. § (3) bekezdés
[119] Ibtv. 13. § (2) bekezdés.
[120] Ibtv. 13. § (8) bekezdés.
[121] Ibtv. 13. § (5) és (6) bekezdés.

2.4.5.2. Az információs rendszerekkel kapcsolatos bűncselekmények

Az elektronikus információs rendszerek biztonságos működése, a kezelt adatok, a felhasználók és az üzemeltetők védelme érdekében szükséges meghatározni azokat a magatartásszabályokat, amelyeket az állam büntetni rendel. A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) önálló tényállásként szabályozza az információs rendszerekkel kapcsolatos bűncselekményeket, ezzel is kiemelve az információs rendszerek megfelelő működtetéséhez és az abban foglalt adatok megőrzéséhez fűződő társadalmi érdek védelmének fontosságát. A Btk. alapján információs rendszer alatt az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezést, vagy az egymással kapcsolatban lévő ilyen berendezések összességét kell érteni.[122]

1. A Btk. XXV. fejezete „A minősített adat és a nemzeti adatvagyon elleni bűncselekmények" között nevesíti a minősített adattal visszaélést[123], a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekményt.[124]
A minősített adattal visszaélés bűncselekményt az valósítja meg, aki minősített adatot jogosulatlanul megszerez vagy felhasznál, illetve jogosulatlan személy részére hozzáférhetővé vagy jogosult személy részére hozzáférhetetlenné tesz. A bűncselekmény alapesetben vétségnek minősül, a büntetési tétel az adat minősítésének szintjétől függően szigorodik. Minősített esetként kezeli a jogalkotó, ha a bűncselekményt minősített adat felhasználására törvény alapján jogosult személy követi el, ez esetben az előkészület is büntethető. A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűntettet az valósítja meg, aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné teszi, az adatkezelés körébe tartozó művelet elvégzését akadályozza vagy lehetetlenné teszi.

2. A Btk. a vagyon elleni bűncselekmények között szabályozza *az információs rendszer felhasználásával elkövetett csalás*t[125]. A tényállás szerint a bűncselekményt az valósítja meg, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz. A büntetési tétel mértéke az okozott kár mértékétől függően változik.

[122] Btk. 459. § (1) bekezdés 15. pont
[123] Btk. 265. §
[124] Btk. 267. §
[125] Btk. 375. §

3. A Btk. önálló fejezetben – XLIII. fejezet – fogalmazza meg az információs rendszer elleni bűncselekményeket. A *tiltott adatszerzés* bűncselekmény azáltal valósul meg, hogy az elkövető a személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot jogosulatlan módon, a Btk. 422. §-ában felsorolt magatartások megvalósításával akarja megismerni. A bűntett minősített esetei a bűnszövetségben, az üzletszerűen, jelentős érdeksérelmet okozva vagy hivatalos eljárás színlelésével elkövetett cselekmények.

4. Az *információs rendszer vagy adat megsértése*[126] bűncselekmény elkövetője olyan személy lehet, aki jogosultság nélkül vagy jogosultságának kereteit túllépve követi el a szankcionált magatartást (információs rendszerbe való belépés és bent maradás). A bűncselekmény elkövetésére akkor kerül sor, ha a szankcionálandó magatartás további, nem kívánt következményekhez vezet, így ha az az információs rendszer működését akadályozza vagy az abban lévő adat megváltoztatására, törlésére, hozzáférhetetlenné tételére sor kerül.

5. Az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmény[127] tényállása akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, illetve az információs rendszer vagy adat megsértése bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja. A tényállással összefüggően büntethetőséget megszüntető oknak minősíti a Btk. az eljáró hatósággal való együttműködést (tevékenység hatóság előtti felfedése, az elkészített dolognak a hatóság részére történő átadása, a készítésben részt vevő más személy kiléte megállapításának lehetővé tétele).

[126] Btk. 423. §
[127] Btk. 424. §

3. Közigazgatási jog alapjai

A közigazgatási jog, mint önálló jogág a közigazgatási szerveknek, az egyik fő állami szervtípusnak a működését, szervezeti és intézményrendszerét és a közigazgatási jogviszony eljárásjogi alapját szabályozza. Az elektronikus információbiztonság szempontjából a közigazgatási jogon belül elsődlegesen a szervezetrendszert szükséges vizsgálni. A közigazgatás intézményrendszerében az elmúlt években lezajlott és jelenleg is folyamatban lévő változásokat figyelembe véve a közigazgatás rendszere elméleti alapjainak és az államigazgatási szervezetrendszer felépítésére vonatkozó főbb sajátosságoknak a rögzítésére kerül sor. A rendszertani elhelyezés érdekében szükséges meghatározni a közigazgatás sajátosságait és helyét az államszervezetben.

3.1. A közigazgatás sajátosságai és fogalma, helye az államszervezetben

A közigazgatás az igazgatásnak, mint szervező, összehangoló tevékenységnek egy *speciális szakigazgatási rendszer*e, alapvető feladata az állam döntéseinek előkészítése és végrehajtása. Mint integrált szakigazgatási rendszer más igazgatási rendszerekhez képest eltérő *sajátosságai*[128] vannak, melyek az alábbiakban határozhatóak meg:

a) a társadalomban létező legnagyobb szakigazgatási rendszer, olyan közigazgatási funkciókat teljesítő szervek rendszere, amely igazgatási tevékenysége kiterjed az egész társadalomra,
b) politikai hatalomnak alárendelt, annak céljait, feladatait valósítja meg, ugyanakkor relatív autonómia jellemzi ebben a kapcsolatban, mert önállóan gyakorolja hatáskörét a jogszabályok betartása mellett,
c) a társadalom igazgatását közhatalom birtokában látja el, adott esetben törvényes felhatalmazása van fizikai erőszak, azaz állami kényszer alkalmazására,
d) tevékenységét a jog szabályozza, melyet a jogállamiság szigorú követelményeinek érvényesülése jellemez,
e) működésében a fékek és egyensúlyok rendszere rendezőelvként jelenik meg.

[128] Fazekas Marianna – Ficzere Lajos: Magyar közigazgatási jog – általános rész (2002. Bp. Osiris Kiadó) 34-36. oldal

Fenti sajátosságok figyelembevételével rögzíthető, hogy a *közigazgatás* a társadalom legnagyobb integrált szakigazgatási rendszere, amely keretében a közigazgatási szervek állami közhatalom birtokában, hatáskörükben és illetékességi területükön eljárva kötelező döntést bocsátanak ki és annak végrehajtását állami kényszerrel is kikényszeríthetik.

A közigazgatás, mint állami tevékenység, és mint elkülönült hatalmi ág, az állami szervek rendszerében feladatellátásából és sajátosságaiból adódóan sajátos helyet foglal el, szerepe a hatalmi ágak felosztásához viszonyítva további sajátosságokat eredményez. A közigazgatás törvényhozáshoz való viszonyát vizsgálva megállapítható, hogy nincs hierarchikus viszony az Országgyűlés és a közigazgatás között, mivel az Országgyűlés nem adhat konkrét utasításokat a közigazgatási szervezetrendszerének. Kapcsolódási pont az Országgyűléshez, mint a választott népképviseleti szervek főhatalmához, a Kormánynak és a minisztereknek a felelőssége, valamint az Országgyűlés Kormány feletti ellenőrző tevékenységében található. Ugyanakkor a közigazgatásnak – jogszabály-előkészítési tevékenysége által – a parlamenti döntések előkészítésében játszott szerepe jelentős, mint ahogy a törvényhozói döntések végrehajtásában is meghatározó szerepe van. A közigazgatás és az államfő viszonyát vizsgálva kapcsolódási pont kizárólag a közigazgatás döntés-előkészítő tevékenységét illetően van, mivel a köztársasági elnök tevékenysége nem része a végrehajtó hatalomnak, hanem önálló, sajátos állami tevékenységfajta. Az igazságszolgáltatás és a közigazgatás kapcsolatában alapelvként érvényesül a két hatalmi ág teljes körű szétválasztása, amely a jogállamiság egyik garanciális eleme. Kapcsolat a közigazgatási döntések bírói kontroll intézményében található, amely lényege, hogy a közigazgatási döntések felülvizsgálata során hozott bírósági döntések a közigazgatási szervekre kötelezőek.

A közigazgatás a közhatalommal végzett igazgatási tevékenysége során jogalkalmazó és jogalkotó tevékenységét jognak alávetett módon folytatja, amely joghoz kötöttség az egyén és a közigazgatás közötti olyan viszonyt feltételez, melyben a közigazgatás sem törvény ellenében, sem törvényi felhatalmazás nélkül nem avatkozhat be a magánszférába. A közigazgatás a társadalom igazgatását a jog és az állam által meghatározott keretek között látja el. Feladatait elkülönült szervezetrendszer keretén belül, hivatásos közigazgatási személyzet, szakértői apparátus által látja el.

A közigazgatás tevékenységeit az alábbi fajták[129] szerint csoportosíthatjuk:

a) *Közhatalmi tevékenységek*: a közigazgatási jogalkotás és a hatósági jogalkalmazás.

[129] Magyar közigazgatási jog – általános rész 44-50. oldal

b) *Közhatalmat nem igénylő tevékenységek*: szervezetirányítás, belső igazgatás, gazdálkodás (költségvetési és vagyonkezelési tevékenység), materiális tevékenység (társadalmi tevékenység, pl.: közszolgáltatások ellátása).
c) *Nem közigazgatási jogi tevékenységek* (polgári jogi, pénzügyi jogi aktus, nemzetközi jogi tevékenység).

A közigazgatás szervezeti rendszerén belül az egyes szervezeteket az alábbiak szerint csoportosíthatjuk:[130]

1. A *hatáskör jellege szerint* megkülönböztethetünk általános és különös hatáskörű szerveket. Az általános hatáskörű szervek feladatköre valamennyi illetékességi területén jelentkező közigazgatási feladatra kiterjed (pl.: fővárosi és megyei kormányhivatalok), a különös hatáskörű szervek egy adott közigazgatási szakterülethez kapcsolódó feladatot látnak el (pl.: minisztériumok).
2. A *terület szerinti tagolódás* alapján vannak központi szervek, melyek illetékessége az egész államterületre kiterjed és vannak területi vagy helyi szervek, melyek illetékességi területe vagy az állam általános területi beosztásával egyező, vagy attól eltérő földrajzi területre, kisebb vagy nagyobb területi egységekre korlátozódik.
3. Az *irányítási viszony* alapján megkülönböztetjük közvetlenül a Kormány irányítása alatt álló szerveket (pl.: kormánybizottságok, minisztériumok, kormányhivatalok), közvetetten a Kormány irányítása alatt álló szerveket (pl.: központi hivatalok, rendvédelmi szervek országos parancsnokságai) és a Kormány irányítása alatt nem álló szerveket (pl.: autonóm jogállású szervek).
4. A *közigazgatás vezetés típusa* szerint egyszemélyi vagy testületi vezetés között tehetünk különbséget.

3.2. A magyar közigazgatási intézményrendszer és az államigazgatási alrendszer, a központi és területi államigazgatás szervei

A *közigazgatási intézményrendszer* jogszabályban rögzített közfeladatot ellátó szervek és a közigazgatási feladat- és hatáskörökkel rendelkező szervek együttese, amely nem azonos a

[130] Magyar közigazgatási jog – általános rész 131-132. oldal

közigazgatási szervezetrendszerrel. A közigazgatás intézményrendszerébe tartozik minden olyan szervezet vagy adott esetben magánszemély, amely olyan állami feladatot lát el, melyet az állam jogszabály alapján kötelezően vállal és ellátásáról a közigazgatás útján gondoskodik. Ide soroljuk azokat a szervezeteket és személyeket, amelyek a közszolgáltatások ellátásában részt vesznek. A magyar közigazgatási intézményrendszert bemutató ábrát a 4. melléklet tartalmazza.

Az intézményrendszeren belül megkülönböztetünk *közigazgatási feladatot ellátó közigazgatási szerveket* és *közigazgatási feladatot ellátó nem közigazgatási szerveket*. Utóbbiak közé tartoznak a közintézetek (pl.: kórház, iskola), a köztestületek (pl.: Magyar Tudományos Akadémia, gazdasági és szakmai kamarák), a közhasznú szervezetek (pl.: a még működő közalapítványok és a közhasznú gazdálkodó szervezetek), és a közfeladatot ellátó magánszemélyek (pl.: háziorvos). A közfeladatot ellátó közigazgatási szervek rendszerén belül (ezeket nevezzük *közigazgatási szervezetrendszernek*) alapvetően két alrendszert különítünk el, az *államigazgatási* és az *önkormányzati alrendszer*t. Az államigazgatási alrendszerbe besorolható, mégis külön célszerű jelölni a rendészeti igazgatást, mint sajátos államigazgatási formát, amely intézményei, a fegyveres szervek, kizárólagos jogosítvánnyal rendelkeznek az állami kényszer alkalmazására. Külön ki kell emelni az autonóm jogállású államigazgatási szerveket, melyek feladatellátásukhoz közhatalmi, közigazgatási jogosítvánnyal rendelkeznek, azonban nem tartoznak a kormány által irányított hierarchikus felépítésű államigazgatási szervek közé, ahogy az önálló szabályozó szervek sem.

A magyar közigazgatási intézményrendszer egyes részei közül a közigazgatási feladatokat elsődlegesen az államigazgatási alrendszert képező államigazgatási szervek látják el. Az államigazgatási alrendszer sajátossága, hogy a csúcsán álló állami szerv, a Kormány tevékenysége nem korlátozódik államigazgatási feladatok végrehajtására, kormányzati tevékenységének ellátása során befolyásolja az egész állami politika irányát. Az *államigazgatási szerv* az államigazgatás olyan elkülönült szervezete, amely jogszabályban meghatározott hatásköröket, közigazgatási jogosítványokat önállóan gyakorol, és ezért felelősséggel tartozik, más államigazgatási szervektől elkülönült szervezete van, élén felelős vezető (testület), amely a hatáskörök és közigazgatási jogosítványok címzettje.[131] Az államigazgatási szerv jellemzője, hogy költségvetésüket általában a felettes szervei állapítják meg és költségvetési szervként jogi személynek minősülnek.

[131] Magyar közigazgatási jog – általános rész 94. oldal

Az államigazgatási alrendszer *hierarchikus szervezetrendszer*ből épül fel. Az államigazgatási szervek rendszerén belül, minden szervtípus esetében különböző szintű, egymásnak alá-, illetve fölérendelt szervek működnek. Az államigazgatási szervtípusok – az egyes típusok sajátosságainak ismertetése nélkül – két csoportra oszthatók. Az *alapvető államigazgatási szervtípusokra*, melyek között megkülönböztetjük a Kormányt a és kormányzati szerveket, a központi államigazgatási szerveket (pl.: minisztériumok, központi hivatalok), és az államigazgatás területi szerveit. A *sajátos államigazgatási szervekre*, melyek közé tartoznak a konzultatív testületek (pl.: Nemzeti Bűnmegelőzési Tanács), az autonóm jogi státusú szervek (pl.: Gazdasági Versenyhivatal), a kvázi autonóm testületek (pl.: Magyar Akkreditációs Bizottság), a szakigazgatási intézmények (pl.: Állami Népegészségügyi és Tisztiorvosi Szolgálat), a szakértői típusú szervezetek (pl.: Igazságügyi Szakértői és Kutató Intézetek), a fegyveres testületek, rendészeti szervek (pl.: rendőrség) és az állami gazdálkodási, vagyonkezelési tevékenységet végző szervek (Magyar Nemzeti Vagyonkezelő Zrt.).

A magyar államigazgatás központi államigazgatási szervei[132] közé az alábbi szerveket soroljuk:

a) Kormány,
b) Kormánybizottság,
c) Miniszterelnökség,
d) minisztériumok,
e) autonóm államigazgatási szervek, ide tartozik a Közbeszerzési Hatóság, az Egyenlő Bánásmód Hatóság, a Gazdasági Versenyhivatal, a Nemzeti Adatvédelmi és Információszabadság Hatóság, a Nemzeti Választási Iroda,
f) kormányhivatalok, mint törvény által létrehozott, a Kormány irányítása alatt működő szervek, ide tartozik a Központi Statisztikai Hivatal, az Országos Atomenergia Hivatal, a Szellemi Tulajdon Nemzeti Hivatala, a Nemzeti Adó- és Vámhivatal,
g) központi hivatalok, mint kormányrendelet által létrehozott, miniszter irányítása alatt működő szervek (pl.: Bevándorlási és Állampolgársági Hivatal, Egészségügyi Engedélyezési és Közigazgatási Hivatal, Országos Meteorológiai Szolgálat, Magyar Bányászati és Földtani Hivatal, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, Magyar Államkincstár, Földmérési és Távérzékelési Intézet, Mezőgazdasági és Vidékfejlesztési Hivatal stb.)
h) rendvédelmi szervek (rendőrség, büntetés-végrehajtási szervezet – Büntetés-végrehajtás

[132] A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2)-(6) bekezdései.

Országos Parancsnoksága, hivatásos katasztrófavédelmi szerv – Országos Katasztrófavédelmi Főigazgatóság, polgári nemzetbiztonsági szolgálatok - Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat) és a Katonai Nemzetbiztonsági Szolgálat,

i) önálló szabályozó szervek (Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal).

A magyar államigazgatás területi államigazgatási szervei közé az alábbi szerveket soroljuk:

a) fővárosi és megyei kormányhivatalok (szervezeti egységei a törzshivatal, az ágazati szakigazgatási szervek, a járási, fővárosi kerületi hivatalok),
b) önálló területi szervek, mint a kormányhivatalok és egyes központi hivatalok területi szervei – melyek nem szakigazgatási szervei a fővárosi és megyei kormányhivataloknak (pl.: Nemzeti Adó- és Vámhivatal, Magyar Államkincstár, Bevándorlási és Állampolgársági Hivatal, Szociális és Gyermekvédelmi Főigazgatóság területi szervei, Magyar Bányászati és Földtani Hivatal bányakapitányságai, Klebersberg Intézményfenntartó Központ tankerületei),
c) önkormányzatok átruházott államigazgatási hatáskörben történő feladatellátása (pl.: szociális igazgatás területén a jegyző méltányossági ápolási díj megállapítására vonatkozó határozata).

4. Közigazgatási szervek

A közigazgatási intézményrendszer és az államigazgatási alrendszer felépítésének ismertetését követően szükséges a közigazgatási szervek sajátosságainak a meghatározása ahhoz, hogy az elektronikus információbiztonság szervezetrendszerét és szervezeteit elhelyezzük a közigazgatási szervek rendszerében. Elsődlegesen rögzíteni szükséges a közigazgatási szerv, mint önálló szervezet fogalmát és sajátosságait.

4.1. A közigazgatási szerv fogalma, jogképessége, szervezete

*Közigazgatási szerv*nek nevezzük a közigazgatás intézményrendszerén belül a csak közigazgatási feladatokat ellátó szervet, amely jogszabályban meghatározott közigazgatási feladatait, hatásköre és illetékességi keretein belül általános közhatalommal felruházva látja el. A közigazgatási szerv a közigazgatási szervezetrendszer legkisebb alapegysége. *Önálló közigazgatási szerv* az önálló, minden más állami szervtől elhatárolt hatáskörrel és önálló elhatárolt szervezettel rendelkező közigazgatási szerv, amely gazdasági önállóságának jellemzője, hogy a rá bízott anyagi eszközök felett maga rendelkezik.[133]

A közigazgatási szerv közigazgatási jogok és kötelezettségek alanya lehet, jogképességük létrehozásukkal keletkezik és megszüntetésükkel szűnik meg. Jogképességének elemei[134] közé tartozik:

a) törvényes jogrendben való létrehozása (alapítása és megszüntetése),
b) a közigazgatási tevékenységre való felhatalmazás alapján önálló feladatkörrel való rendelkezés és jogkör a közhatalom gyakorlásához,
c) a feladatkör ellátásához szükséges jogok és kötelezettségek összessége, azaz jogszabály által biztosított hatáskör,
d) illetékességi terület kijelölése, az azonos hatáskörű szervek közötti területi munkamegosztás céljából, amely alapján a közigazgatási szerv hatáskörét csak illetékességi területén gyakorolhatja.

[133] Magyar közigazgatási jog – általános rész 124. oldal
[134] Magyar közigazgatási jog – általános rész 125. oldal

A közigazgatási szerv szervezeti formáját tekintve speciális igazgatási munkaszervezettel rendelkezik, amelyre a következő sajátosságok jellemzőek:

a) a szervezet élén egyszemélyi felelős vezető áll, aki a hatáskörök és közigazgatási jogosítványok címzettje,
b) a feladatellátásra ügyintézési és ügyviteli tevékenység jellemző,
c) a feladatellátást fizetett hivatali apparátus végzi, jogviszonyuk jogi szabályozása és felelősségi rendszere sajátos,
d) a munkaszervezet működéséhez szükséges anyagi fedezetet költségvetésből biztosítják.

4.2. Az elektronikus információbiztonság szervezetrendszere a közigazgatásban

Az elektronikus információbiztonsággal foglalkozó szervezetek és közigazgatási szervek működésére vonatkozó részletszabályokat és a főbb feladatokat az Ibtv. és végrehajtási rendeletei tartalmazzák. Az Ibtv. szerinti szervezetrendszer ábráját az 5. melléklet tartalmazza.

4.2.1. Nemzeti Kiberbiztonsági Koordinációs Tanács[135]

A Kormány javaslattevő, véleményező szerveként, a kiberbiztonság kormányzati koordinációja érdekében a Miniszterelnökséget vezető államtitkár elnökletével létrehozásra került a Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács). A Tanácson belül végzi feladatellátását a kiberkoordinátor is, aki egyben az elnök általános helyettese.

A Tanács a kiberbiztonság területét érintő koordinációs feladatellátásán[136] túl figyelemmel kíséri a Kiberstratégiában meghatározott cselekvési területek végrehajtást és erről jelentést tesz a Nemzetbiztonsági Kabinetnek, valamint a cselekvési területekhez tartozó kormányzati intézkedéseket tartalmazó, ún. Nemzeti Kiberbiztonsági Akciótervet – készít, melynek elfogadásáról a Kormány dönt és melyet évente felül kell vizsgálnia. A Tanács tevékenységéről az elnök – legalább félévente – a miniszterelnöknek tartozik beszámolási kötelezettséggel.

[135] Ibtv. 21. §-a és a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet alapján.
[136] Ibtv. 21. § (2) bekezdés

A Tanács tagja a miniszterek által delegált 1 fő állami vezető, és a kiberkoordinátor. Az elnök felkérésére a Tanács munkájában az Állami Számvevőszék, a Magyar Nemzeti Bank, a Nemzeti Adatvédelmi és Információszabadság Hatóság, a Nemzeti Hírközlési és Informatikai Tanács, a Nemzeti Média- és Hírközlési Hatóság és a Magyar Energetikai és Közmű-szabályozási Hivatal elnöke is részt vehet. A Tanács munkáját javaslattételi joggal és véleményezési lehetőséggel a felkért szakmai, illetve nem kormányzati gazdasági vezetőkből álló Nemzeti Kiberbiztonsági Fórum, koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik. Kötelező jelleggel kerültek létrehozásra az eseménykezelés, a belbiztonság, az e-közigazgatás, az energetika, és a gyermekvédelem szakterületét kezelő munkacsoportok, de a Tanács felkérésére további munkacsoportok is létrehozhatóak. A munkacsoportok tagja a kiberkoordinátor, és az általa felkért állami szervek által delegált közszolgálati tisztviselők, valamint a kiberkoordinátor által felkért nem kormányzati szakértő.

A Tanács a kibertámadások kezelése és az elektronikus információbiztonság területén rendelkezik azzal a jogosítvánnyal, hogy az alkalmazandó legjobb gyakorlatokról a munkacsoportok javaslatára ajánlásokat adjon ki, melyek jellegükből adódóan jogi kötelező erővel nem rendelkeznek.

4.2.2. A hatóság és a szakhatóság

Az elektronikus információs rendszerek biztonságának felügyeletét – az Ibtv.-ben meghatározott kivétellel – az informatikáért felelős miniszter látja el, a Nemzeti Fejlesztési Minisztérium szervezeti keretei között létrejött, önálló hatósági jogkörrel rendelkező szervezeti egység, a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: Hatóság) útján.[137] Szakhatósági feladatokat a Nemzeti Biztonsági Felügyelet lát el.

A Hatóság és a szakhatóság feladatainak ellátására vonatkozó részletszabályokat a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet (a továbbiakban: Korm. rendelet) tartalmazza. Az Ibtv. felhatalmazása alapján az elkülönített, rendészeti, honvédelmi, nemzetbiztonsági, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerek[138] és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró vagy törvényi felhatalmazás

[137] Ibtv. 14. § (1) bekezdés
[138] Ibtv. 1. § (1) bekezdés 47. pont

alapján speciális feladatokat (pl.: médiaszolgáltatási és elektronikus hírközlési tevékenység) ellátó információs rendszerek esetében az irányítási feladatokat gyakorló miniszter saját hatáskörében eljárva, rendeleti úton szabályozza a hatósági és szakhatósági feladatok ellátását.[139] Ezen speciális ágazati szabályokat meghatározó miniszteri rendeletek[140] külön, ágazati szinten rögzítik, hogy mely személy vagy szervezet feladata és kötelezettsége a hatósági és szakhatósági feladatok ellátása. (A Korm. rendelet értelmező rendelkezéseinek kivonatát az 1. melléklet tartalmazza.)

4.2.2.1. A hatóság feladatellátása és eljárásának szabályai

A Hatóság az érintett szervezet által megküldött információk és a technológiai rendeletben meghatározott szempontok alapján végzi az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe sorolásának hatósági ellenőrzését, szükség esetén a megállapított biztonsági osztályt és biztonsági szintet felülbírálhatja.[141] Ha a felülbírálat során magasabb biztonsági osztályt vagy biztonsági szintet állapít meg, akkor az érintett szervezetnek a döntésnek megfelelő biztonsági osztályhoz és biztonsági szinthez igazodva kell meghatároznia, hogy az elvárt biztonsági intézkedések megtételére milyen ütemezéssel kerül sor. Ha az ellenőrzés során a Hatóság arra a következtetésre jut, hogy a bejelentett biztonsági osztálynál vagy biztonsági szintnél alacsonyabbat is alkalmazhat az érintett szervezet, akkor erre javaslatot tesz.[142]

Felügyeleti jogkörében eljárva éves ellenőrzési terv alapján a Hatóság ellenőrzést folytathat le, amely ellenőrzésére a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban. Ket.) hatósági ellenőrzésre vonatkozó szabályai az irányadóak, azzal, hogy eljárását a Korm. rendeletben[143] rögzítettek alapján folytatja le. Jogosult a központi, valamint uniós forrásból megvalósuló fejlesztési projektek információbiztonsági követelményei teljesülésének ellenőrzésére is, melynek során a szakhatóság véleményét is köteles beszerezni.

[139] Ibtv. 2. § (4) és (5) bekezdés
[140] A zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet, a Nemzeti Adó- és Vámhivatal elektronikus információs rendszerei biztonságának felügyeletéről és ellenőrzéséről szóló 34/2013. (VIII. 30.) NGM rendelet, a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet, a diplomáciai információs célokra használt zárt célú elektronikus információs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 3/2014. (II. 26.) KüM rendelet.
[141] Ibtv. 14. § és a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet (a továbbiakban: R.) 9. §
[142] R. 10. §
[143] R. 4. §

Az azonnali reagálás érdekében kormányzati információtechnológiai és hálózatbiztonsági információ-megosztási incidens-kezelési munkacsoport (a továbbiakban: incidens-kezelési munkacsoport) működtet[144], amely célja az azonnali információ megosztás mellett az elektronikus információbiztonság és a tudatosság növelése, valamint a legjobb gyakorlatok elterjesztése. Kiemelt feladata továbbá az egyes sérülékenységek, fenyegetések és incidensek korai felismerése és egységes, gyors, kormányzati szintű kezelése, annak érdekében, hogy a veszély, fenyegetés mielőbb elhárításra kerülhessen.

A biztonsági események bejelentését a Ket. szerint írásbelinek minősülő elektronikus úton – kivétel a minősített adatot tartalmazó bejelentés, melyet papír alapon – kell megtenni.[145] A bejelentés, valamint a kormányzati eseménykezelő központ értesítése alapján a biztonsági eseményeket a Hatóság köteles haladéktalanul megvizsgálni, és az elhárításhoz szükséges intézkedéseket megtenni. Ennek keretében közzéteheti a fenyegetés elhárítására szolgáló információkat, továbbá azokat a megismert biztonsági eseményeket, amelyek általános fenyegetést jelentenek a kiberbiztonságra, valamint tájékoztathatja az incidens-kezelési munkacsoportot azon biztonsági eseményekről és azok értékeléséről, amelyek a védelmi felkészültséget növelik. Ha a biztonsági esemény személyes adatokat, vagy azok bizalmasságát sértette, köteles értesíteni a Nemzeti Adatvédelmi és Információszabadság Hatóságot.[146] A Hatóság bármely hatásköre szerinti eljárási cselekményt haladéktalanul lefolytathatja, ha az a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és polgárai számára kiemelten fontos információs rendszereket súlyosan veszélyeztető fenyegetés elhárítását szolgálja.[147] A jelentős kihatással bíró kiberbiztonsági eseményről eseti jelentést köteles készíteni a Tanács részére.

Kérelem alapján engedélyezési eljárást folytat le az elektronikus információs rendszer Európai Unió tagállamaiban történő üzemeltetésére, amely alkalmával az adatkezelés jogi, szabályozási, valamint technikai és technológiai hátterét vizsgálja. [148] A kérelmet 90 nappal az adatkezelés megkezdése előtt kell benyújtani, az engedély hiányában az üzemeltetés nem kezdhető meg. Ez alól kivétel, ha az adatkezelésre vagy rendszerüzemeltetésre olyan nemzetközi szerződés alapján kerül sor, amelyben a magyar állam az egyik szerződő fél.

[144] R. 21. § (5) bekezdés
[145] Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet (a továbbiakban: NFM rendelet) 8. §
[146] NFM rendelet 9. §
[147] R. 5. §
[148] R. 6. § (2) és (3) bekezdés

Ennek tényéről a Hatóságot tájékoztatni kell, amely tájékoztatást eljárás lefolytatása nélkül tudomásul vesz.[149]

Feladatellátása során az ügyintézési határidő 60 nap, amely egy alkalommal további 30 nappal meghosszabbítható.[150] A Hatóság döntésének meghozatala előtt egyeztetést folytat le az eljárással érintett szervezettel, azonban határozatai ellen rendkívüli jogorvoslatként újrafelvételi eljárásnak nincs helye, továbbá a határozatok felügyeleti jogkörben való visszavonására, módosítására nincs lehetőség.[151]

4.2.2.2. A szakhatóság feladatellátása és eljárásának szabályai

A Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF), mint szakhatóság a Ket. szerint – igazgatási szolgáltatási díj ellenében – közreműködik a biztonsági osztályba és a biztonsági szintbe sorolásra, a Hatósághoz érkező bejelentések kivizsgálására vonatkozó hatósági eljárásban, valamint a Hatóság éves ellenőrzési terv alapján végzett ellenőrző tevékenységében.[152]

Az NBF látja el az elektronikus információs rendszerek, rendszerelemek sérülékenység-vizsgálatát, amely vizsgálatot a szervezet felkérésére a Hatóság eljárásától függetlenül is elvégezhet. A sérülékenységvizsgálat alapvető célja, hogy már a biztonsági esemény bekövetkezését megelőzően feltárja az elektronikus információs rendszer esetleges gyenge pontjait és a védelem hiányosságait, a feltárt hibák elhárítására vonatkozóan részletes megoldási javaslatokat dolgozzon ki.[153]

A sérülékenységvizsgálat[154] alkalmával az elektronikus információs rendszereknek, eszközöknek, eljárásoknak, és kapcsolódó folyamatoknak, valamint az ezeket kezelő személyek általános informatikai felkészültségének, és a szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának a vizsgálatára kerül sor, amely kiindulási pontját az előzetesen elkészített szakhatósági dokumentáció adja. Ebben a dokumentációban rögzítésre kerülnek az elvégezendő feladatok és célok, a technikai és személyi feltételek, az alkalmazott módszertan és a vizsgálat befejezésének várható időpontja. Az eltérő vizsgálati módszerek elvégzésére – külső vizsgálat (15 nap), webes vizsgálat (50

[149] R. 7. § (1) és (2) bekezdés
[150] R. 2. §
[151] R.3. § és 20. §
[152] Ibtv. 18. §
[153] Ibtv. 18. § és R. 12. §
[154] R. 13.-14. §

nap), belső vizsgálat (75 nap), vezeték nélküli hálózat vizsgálat (15 nap), 3G/GPRS vizsgálat (30 nap), emberi tényezőkön alapuló vizsgálat (30 nap) – a Korm. rendelet eltérő határidőket állapít meg. Ezen vizsgálati irányultságokhoz eltérő jogosultságok kapcsolódhatnak, így attól függően, hogy a vizsgálatot végző személynek van-e külön létrehozott felhasználói jogosultsága vagy sem, vagy éppen adminisztrátori jogosultsággal rendelkezik, három különböző jogosultsági fázist különböztet meg a Korm. rendelet.[155]

A sérülékenységvizsgálati szakhatósági állásfoglalás rendelkező része tartalmazza az intézkedési tervet, mely rövid-, közép- és hosszú távú intézkedéseket határoz meg az érintett szervezet számára. Rögzíti az intézkedések becsült idő- és költségigényét és a szakhatósági eljárás költségeit. Az indokolás részletesen kifejti a sérülékenységvizsgálat módszertanát, az eljárás során feltárt sérülékenységek részletes technikai információit és a javasolt megoldásokat.

Az NBF ellátja továbbá a biztonsági események adatainak műszaki vizsgálatát[156] is, melyet a Hatóság megkeresése vagy egyedi esetben felkérésre végez el. Ezen szakhatósági eljárás ügyintézési határideje 60 nap, amely egy alkalommal legfeljebb 30 nappal meghosszabbítható. Célja a biztonsági esemény bekövetkezte esetén az okok és a körülmények megismerése, az érintett elektronikus információs rendszerek meghatározása és a kárelhárítás.

Az NBF további feladata a hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatok szervezése. Emellett a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon az NBF felkérésre képviseli Magyarországot, koordinálja, irányítja a magyarországi felek részvételét.[157]

4.2.2.3. A hatósági, szakhatósági eljárás jogkövetkezményei

Az elektronikus információs rendszert veszélyeztető informatikai állapot észlelése esetén és a lefolytatott hatósági eljárás eredményétől függően a Hatóság – adott esetben a szakhatóság bevonásával – különböző jogkövetkezményeket alkalmazhat.

[155] R. 1.§ 1., 12, 13. pontok, 13. § (4) bekezdés
[156] R. 15. §
[157] Ibtv. 18. §

a) Írásbeli felszólítás, amely az érintett szervezet vezetőjének felszólítása határidő kitűzése mellett a mulasztás, a biztonsági követelmény megsértésének megszüntetésére, a kötelezettség teljesítésére.[158]
b) A felügyeleti szerv közreműködésre történő felkérése: csak költségvetési szerv esetében alkalmazható abban az esetben, ha a szervezet az írásbeli felszólításnak nem tesz eleget.[159]
c) Az azonnali intézkedés megtételére való kötelezés: abban az esetben, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget.[160]
d) Bírság kiszabása: 50 ezer forinttól 5 millió forintig terjedő összegben, amely jogkövetkezmény költségvetési szerv esetében nem alkalmazható[161].
e) Információbiztonsági felügyelő kirendelése: amelyre csak költségvetési szerv esetében kerülhet sor, ha a szerv felszólítás ellenére a jogszabályokban foglalt biztonsági követelményeket és az ezekhez kapcsolódó eljárási szabályokat nem teljesíti.[162] Az információbiztonsági felügyelő kirendelését a Hatóság indoklással ellátott, határozott időtartamra szóló javaslattal a nemzeti fejlesztési miniszternél kezdeményezheti. A kirendelés indokolt esetben legfeljebb egy alkalommal a folyamatban lévő intézkedések lezárásáig meghosszabbítható.[163]
f) A rövid-, közép- és hosszú távú intézkedési terv végrehajtása, amely a sérülékenységvizsgálati szakhatósági állásfoglalásban kerül meghatározásra.[164]
g) Hatósági eljárás lefolytatásának kezdeményezése, melyet az NBF szakhatósági eljárása során kezdeményezhet, ha azt állapítja meg, hogy a felkérésben megjelölt szerven kívül más szerv elektronikus információs rendszereinek, rendszerelmeinek sérülékenysége is felmerült, illetve más szerv biztonsági eseményei adatainak műszaki vizsgálata is indokolt.[165]

Az információbiztonsági felügyelő jogosult a szervezet által meghozott védelmi intézkedéseket véleményezni, adott esetben az intézkedéssel szemben kifogással élhet, azonban pénzügyi kötelezettségvállalásra nem jogosult.[166] A fenyegetés elhárítása érdekében intézkedéseket, eljárásokat javasolhat a szervezet részére, és feladatellátásával

[158] Ibtv. 16. § (2) bekezdés a) pont, (3) bekezdés a) pont, R. 17. § (1) bekezdés
[159] Ibtv. 16. § (3) bekezdés b) pont
[160] R. 17. § (2) bekezdés
[161] Ibtv. 16. § (2) bekezdés b) pont, R. 17. § (3) bekezdés
[162] Ibtv. 16. § (3) bekezdés c) pont
[163] R. 18. § (1) és (4) bekezdés
[164] R. 14. § (7) bekezdés
[165] R. 13. § (2) bekezdés, 15. § (2) bekezdés
[166] Ibtv. 17. § (2) bekezdés

összefüggésben tájékoztatást, adatszolgáltatást kérhet, dokumentumokba betekinthet.[167] A kirendelésére és visszahívására, az információbiztonsági felügyelő jogosítványaira és kötelezettségeire vonatkozó részletszabályokat a Korm. rendelet 18.-19. §-ai tartalmazzák.

4.2.3. A kormányzati eseménykezelő központ és más ágazati eseménykezelő központok

A biztonsági események kezelését szerte a világon eseménykezelő központok (Számítógépes Vészhelyzeti Reagáló Egység – Computer Emergency Response Team), ún. CERT-ek látják el. Az Ibtv.[168] és az eseménykezelő központok feladat- és hatáskörét megállapító kormányrendelet[169] alapján az eseménykezelő központok feladatai az általuk támogatott ágazat tekintetében a következők:

a) folyamatosan elérhető 24 órás ügyelet működtetése;
b) a bejelentett biztonsági események fogadása, kivizsgálása és kezelése, műszaki vizsgálatok elvégzése, az események elhárításának koordinálása;
c) napi rendszerességgel hálózatbiztonsági helyzetértékelések elvégzése;
d) biztonsági események adatainak gyűjtése, az észlelt, valamint az adatgyűjtés eredményeként a tudomására jutott sérülékenységekről, biztonsági esemény bekövetkezésének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről, a biztonsági eseményekről – személyes adatokat nem tartalmazó – nyilvántartást vezetése;
e) a biztonsági események adatainak haladéktalan továbbítása a kormányzati eseménykezelő központ részére;
f) a biztonsági eseményekről negyedévente jelentés készítése a Tanács részére;
g) a hazai és nemzetközi információbiztonsági irányokról elemzések és jelentések készítése a Tanács részére;
h) a nemzetközileg publikált sérülékenységek és a kritikus hálózatbiztonsági eseményekről magyar nyelvű azonnali figyelmeztetések közzététele a honlapon, és emellett tájékoztatás a tudomásukra jutott sérülékenységekről;
i) együttműködés az informatikai és hálózatbiztonsági védelemben érintett magyar nemzetbiztonsági szolgálatokkal és bűnüldöző szervekkel, iparági szereplőkkel,

[167] R. 19. §
[168] Ibtv. 20. §
[169] Az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelet (a továbbiakban: CERT vhr.).

j) részvétel az infokommunikációs biztonságra vonatkozó stratégiák és ágazati szabályozások előkészítésében,
k) hírlevelek kiadása, tájékoztatási célú, szemléletformáló kampányok szervezése.

Az eseménykezelő központok információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervezhetnek és nemzetközi felkérésre részt vesznek ezeken a gyakorlatokon.

Ágazati eseménykezelő központból több is létrehozható, erre az elkülönített, rendészeti, honvédelmi, nemzetbiztonsági, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerek és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró vagy törvényi felhatalmazás alapján speciális feladatokat (pl.: médiaszolgáltatási és elektronikus hírközlési tevékenység) ellátó információs rendszerek, valamint a Nemzeti Média- és Hírközlési Hatóság és a Magyar Energetikai és Közmű-szabályozási Hivatal esetében kerülhet sor.[170]

Az Ibtv.-ben foglalt biztonsági események kezelését a belügyminiszter irányítása alá tartozó Nemzetbiztonsági Szakszolgálat keretén belül működő kormányzati eseménykezelő központ (a továbbiakban: GovCert) látja el.[171] Az eseménykezelő központok hatáskörébe tartozó feladatokon, a hálózatbiztonsági feladatok kormányzati koordinációján és biztonsági események központi kezelésén túlmenően a GovCert további, kizárólagos feladata:

a) az ágazati eseménykezelő központok szakmai támogatása és tájékoztatásuk a nemzetközi szervezetektől tudomására jutott információbiztonságot érintő eseményekről, fenyegetésekről;
b) a kormányzati információtechnológiai, hálózatbiztonsági, és biztonsági eseménykezelési együttműködési fórum működtetése;
c) a kormányzati kiberbiztonsági tudatosság növelése érdekében tájékoztató, felkészítő tevékenység ellátása.

A kormányzati eseménykezelő központok nemzetközi együttműködésében, az európai kormányzati eseménykezelő csoport által akkreditált CERT-ként a GovCert képviseli Magyarországot. Az ágazati eseménykezelő központok részére lehetőség van arra, hogy a

[170] Ibtv. 19. § (2) bekezdés
[171] Ibtv. 19. § és 20. §

fenntartó döntése alapján akkreditáltassák magukat és ezáltal a nemzetközi együttműködésben részt vegyenek.

A Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (a továbbiakban: Központ), mint sajátos ágazati eseménykezelő központ ágazatokon átnyúló feladatellátást végez, mivel a honvédelmi szempontból létfontosságú rendszerek és létesítmények kivételével valamennyi kijelölt létfontosságú rendszerelem esetében – függetlenül attól, hogy az adott létfontosságú rendszerelem mely ágazathoz tartozik – biztonsági eseménykezelő szervezetként jár el. A Központot az Országos Katasztrófavédelmi Főigazgatóság működteti és a katasztrófák elleni védekezésért felelős miniszter irányítja.[172] A Központ feladata, hogy más szervezetekkel együttműködve védje a létfontosságú rendszerek és létesítmények szolgáltatásait a globális kibertéren keresztül érkező támadások ellen. Felelős a hálózatbiztonság fenntartásának elősegítéséért, fokozásáért, a létfontosságú rendszerelem hálózatbiztonságát érintő eseménnyel összefüggésben az érintett üzemeltető riasztásáért, az elhárítás koordinációjáért. Folyamatos rendelkezésre állást biztosítva ellátja a kibertérből érkező beavatkozások elhárításának koordinálását, rendszeres tájékoztatást ad a felismert és publikált sérülékenységekről. A Központ tevékenysége során együttműködik a GovCert-tel, az Országos Informatikai és Hírközlési Főügyelettel, az Alkotmányvédelmi Hivatallal, a Terrorelhárítási Központtal, az általános rendőrségi feladatok ellátására létrehozott szervvel.[173]

4.2.4. Nemzeti Közszolgálati Egyetem[174]

Az Ibtv. alapján a Nemzeti Közszolgálati Egyetem (a továbbiakban: NKE) felel a kötelező információbiztonsági képzésért. Tevékenységének ellátása során felelős:

a) az elektronikus információs rendszerek védelméért felelős vezetők, az elektronikus információs rendszer biztonságáért felelős személyek, valamint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek képzési, továbbképzési követelményeinek, oktatási programjának kidolgozásáért;
b) az elektronikus információs rendszer biztonságáért felelős személy részére előírt szakképzettség képzettségi követelményeinek meghatározásáért.

[172] CERT vhr. 7. § (1) bekezdés
[173] CERT vhr. 7. § és 8. §
[174] Ibtv. 23. §

A képzés, a továbbképzés és az éves továbbképzés tartalmát miniszteri rendelet[175] határozza meg, amely rögzíti az NKE felelősségét, feladatait és a képzések részletszabályait. A miniszteri rendeletben előírt szakirányú képesítés megszerzését az Ibtv. hatálybalépését követő 5 éven belül (2018. július 1-ig) kell megszereznie az elektronikus információs rendszer biztonságáért felelős személyeknek. Mentesül a szakirányú képesítés megszerzése alól az, aki rendelkezik a miniszteri rendeletben meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.[176] A miniszteri rendelet a mentességek[177] körét az ISACA[178] által kiadott CISA[179], CISM[180], CRISC[181], és az ISSCC[182] által kiadott CISSP[183] érvényes oklevelek esetében állapítja meg, szakmai gyakorlatnak:

a) az információbiztonsági irányítási rendszer tervezése, kialakítása, működtetése során,
b) az információbiztonsági ellenőrzés vagy felügyeleti tevékenység területén,
c) az információbiztonsági kockázatelemzés területén,
d) az elektronikus információs rendszerek információbiztonsági tanúsítási tevékenysége során, vagy
e) az elektronikus információs rendszerek információbiztonsági tesztelésében (etikus hacker tevékenységben)

szerzett szakmai tapasztalatot ismeri el.

[175] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmát a 26/2013. (X. 21.) KIM rendelet (a továbbiakban: Miniszteri rendelet).
[176] Ibtv. 13. § (8) és (10) bekezdés
[177] Miniszteri rendelet 7. §
[178] Information Systems Audit and Control Association
[179] Certified Information System Auditor
[180] Certified Information Security Manager
[181] Certified in Risk and Information Systems Control
[182] International Information Systems Security Certification Consortium, Inc.
[183] Certified Information Systems Security Professional

FOGALOMKATALÓGUS

1. melléklet

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. §-a szerinti értelmező rendelkezések:

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. *adatfeldolgozás:* az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

3. *adatfeldolgozó:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

4. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

5. *adatkezelő:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

6. *adminisztratív védelem:* a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

7. *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

8. *bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

9. *biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

10. *biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

11. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

12. *biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

13. *biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

14. *biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

15. *elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

16. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

17. *észlelés:* a biztonsági esemény bekövetkezésének felismerése;

18. *felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre;

19. *fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

20. *fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

21. *folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

22. *globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

23. *informatikai biztonságpolitika:* a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

24. *informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

25. *információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

26. *kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez;

27. *kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

28. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

29. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

30. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

31. *kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

32. *korai figyelmeztetés:* valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

33. *létfontosságú információs rendszerelem:* az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek

azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

34. *logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

35. *magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

36. *megelőzés:* a fenyegetés hatása bekövetkezésének elkerülése;

37. *reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

38. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

39. *sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

40. *sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

41. *sérülékenységvizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

42. *számítógépes incidenskezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

43. *szervezet:* az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint egyéni vállalkozó;

44. *teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

45. *üzemeltető:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

46. *védelmi feladatok:* megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

47. *zárt célú elektronikus információs rendszer:* jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

48. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1. §-a szerinti értelmező rendelkezések:

1. *ágazati kritérium:* azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése (a továbbiakban együtt: kiesés) által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy mely ágazatba tartozik;

2. *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam;

3. *európai létfontosságú rendszerelem:* e törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne - az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve - legalább két EGT-államra;

4. *horizontális kritérium:* azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének kiesése által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén - figyelemmel a bekövetkező emberiélet-veszteségekre, az egészségre gyakorolt hatásra, a gazdasági és társadalmi hatásokra, a természetre és az épített környezetre gyakorolt hatásra - az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki attól függetlenül, hogy mely ágazatba tartozik;

5. *létfontosságú rendszerelem védelme:* a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység;

6. *létfontosságú rendszerelem:* az 1-3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához -, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna;

7. *nemzeti létfontosságú rendszerelem:* e törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatása lenne Magyarországon;

8. *üzemeltető:* az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős.

A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet 1. §-a szerinti értelmező rendelkezések:

1. *adminisztrátori jogosultsággal rendelkező vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján a teljes informatikai rendszer állapota ellenőrzésre kerüljön;

2. *automatizált vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének a sérülékenységei célszoftverek segítségével kerülnek feltérképezésre;

3. *átlagostól jelentősen eltérő elektronikus információs rendszer:* a biztonsági vizsgálattal érintett szervezet (a továbbiakban: érintett szervezet) elektronikus információs rendszere az átlagostól jelentősen eltér, ha:

a) a rendszer

aa) a külső internetes tartományban több mint 20 IP címen elérhető eszközzel,

ab) több mint 10 webes szolgáltatással,

ac) a belső hálózat tekintetében több mint 50 szerverrel,

ad) több mint 500 munkaállomással,

ae) több mint 5 vezeték nélküli hálózattal, vagy

af) több mint 500 fős felhasználói létszámmal

rendelkezik, vagy

b) az érintett szervezet több mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel;

4. *belső vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik;

5. *célszoftverek:* a biztonsági vizsgálati eljárás során a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett szoftverek;

6. *emberi tényezőkön alapuló vizsgálat:* a dolgozók általános informatikai felkészültségének, és a szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata;

7. *felhő alapú számítástechnikai szolgáltatás:* olyan szolgáltatás, amelyet a szolgáltató a felhasználó számára nem egy erre a célra rendelt hardvereszközön, hanem a saját eszközein elosztva, az üzemeltetés részleteit elrejtve üzemelteti, és amelyet a felhasználók interneten keresztül érhetnek el;

8. *hálózati végpont:* adott informatikai rendszer hálózatához való csatlakozási pont;

9. *kézi vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;

10. *kritikus ügyviteli folyamat:* olyan speciális tevékenységsor, amely az adott szervezet működését alapvetően befolyásoló folyamatokat tartalmaz, vagy kiesése az állampolgári jogok gyakorlását és kötelezettségek teljesítését ellehetetlenítheti;

11. *külső vizsgálat:* az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;

12. *regisztrált felhasználói jogosultság nélküli vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik a szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez;

13. *regisztrált felhasználói jogosultsággal rendelkező vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;

14. *súlyos biztonsági esemény:* olyan esemény, amely az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervek elektronikus információs rendszerei, vagy a kibertér tekintetében jogszabályban meghatározott mértékű, nagy kárt okoz;

15. *titkosítási eljárás:* olyan eljárás, amely az adat megismerhetőségét azáltal korlátozza, hogy az adat egy algoritmus segítségével átalakításra kerül olyan jelsorozattá, ami olvashatatlan azon személy számára, aki nem rendelkezik a visszaalakításhoz szükséges egyedi jelsorozatból álló kulccsal;

16. *titkosítási kulcs:* titkosítási eljárás során alkalmazott olyan jelsorozat, amelynek ismeretében a titkosított állomány megismerhető;

17. *webes vizsgálat:* olyan biztonsági vizsgálati eljárás, amely során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei;

18. *vezeték nélküli hálózat vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

19. *3G/GPRS vizsgálat:* 3G/GPRS szolgáltatások sérülékenységvizsgálata, amelynek során a hálózatok és az elérhető szolgáltatások automatizált és kézi vizsgálati módszerrel történő feltárására kerül sor.

2. melléklet

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény személyi hatálya alá tartozó szervek

1. Az Ibtv. személyi hatálya kiterjed[184]:

a) a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvényben rögzítettek figyelembevételével a központi államigazgatási szervekre[185], ezen belül:

- a Miniszterelnökségre és a minisztériumokra,
- az autonóm államigazgatási szervekre (Közbeszerzési Hatóság, Egyenlő Bánásmód Hatóság, a Gazdasági Versenyhivatal, Nemzeti Adatvédelmi és Információszabadság Hatóság, Nemzeti Választási Iroda),
- a kormányhivatalra, mint törvény által létrehozott, a Kormány irányítása alatt működő szervre (Központi Statisztikai Hivatal, Országos Atomenergia Hivatal, Szellemi Tulajdon Nemzeti Hivatala, Nemzeti Adó- és Vámhivatal),
- a központi hivatalokra, mint a kormányrendelet által létrehozott, miniszter irányítása alatt működő szervekre (pl.: Magyar Államkincstár, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, Bevándorlási és Állampolgársági Hivatal, Országos Meteorológiai Szolgálat, Oktatási Hivatal, Klebelsberg Intézményfenntartó Központ, Szociális és Gyermekvédelmi Főigazgatóság),
- a rendvédelmi szervekre (rendőrség, büntetés-végrehajtási szervezet, hivatásos katasztrófavédelmi szerv, polgári nemzetbiztonsági szolgálatok[186] – Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat) és a Katonai Nemzetbiztonsági Szolgálatra,
- az önálló szabályozó szervekre (Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal).

A jogszabály szerint a Kormány és a kormánybizottságok is központi államigazgatási szerveknek minősülnek, azonban az Ibtv. hatálya nem terjed ki ezekre a szervekre, mivel önálló szervezetrendszerrel nem rendelkező testületként gyakorolják feladataikat és önálló elektronikus információs rendszerekkel nem rendelkeznek.

[184] Ibtv. 2. §
[185] A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2)-(6) bekezdései.
[186] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. §-a.

b) a Köztársasági Elnöki Hivatalra[187], az Országgyűlés Hivatalára[188];
c) az Alkotmánybíróság Hivatalára[189];
d) a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény rendelkezései figyelembevételével az Országos Bírósági Hivatalra és a bíróságokra (Kúria, ítélőtábla, törvényszék, járásbíróság és a kerületi bíróság, közigazgatási és munkaügyi bíróság[190]);
e) az ügyészségről szóló 2011. évi CLXIII. törvény figyelembevételével az ügyészségekre (Legfőbb Ügyészség, fellebbviteli főügyészségek, főügyészségek, járási ügyészségek[191]);
f) az Alapvető Jogok Biztosának Hivatalára[192];
g) az Állami Számvevőszékre[193];
h) a Magyar Nemzeti Bankra[194];
i) a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény figyelembevételével a fővárosi és megyei kormányhivatalokra (ideértve a fővárosi és megyei kormányhivatal szervezeti egységeit – törzshivatal, szakigazgatási szervek, járási és fővárosi kerületi hivatalok[195]);
j) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira (polgármesteri hivatal, megyei önkormányzati hivatal, közös önkormányzati hivatal[196]), a hatósági igazgatási társulásokra[197]; Az Ibtv. hatálya nem terjed ki az önkormányzatok képviselő-testületeire, azok bizottságaira, és a közgyűlésre.
k) a Magyar Honvédségre[198].

2. Az Ibtv. hatálya kiterjed továbbá az a)-j) pontokban felsorolt szervek és a számukra adatkezelést végző szervek elektronikus információs rendszereinek védelmére.

3. Az Ibtv. személyi hatálya kiterjed[199]:

a) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói elektronikus információs rendszereinek védelmére[200], így többek között:

[187] A köztársasági elnök jogállásáról és javadalmazásáról szóló 2011. évi CX. törvény 15. §-a.
[188] Az Országgyűlésről szóló 2012. évi XXXVI. törvény 123. §-a.
[189] Az Alkotmánybíróságról szóló 2011. évi CLI. törvény 22. §-a.
[190] A bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 16. §-a.
[191] Az ügyészségről szóló 2011. évi CLXIII. törvény 8. §-a.
[192] Az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 41. §-a.
[193] Az Állami Számvevőszékről szóló 2011. évi LXVI. törvény 1-2. §-ai.
[194] A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 5. §-a.
[195] A fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény 3. §-a.
[196] Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 85. §-a.
[197] Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 87. §-a.
[198] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 35. §-a és 38. §-a.
[199] Ibtv. 2. §

- a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala esetében:
  - a polgárok személyi adatainak és lakcímének nyilvántartására;
  - a központi idegenrendészeti nyilvántartására;
  - az egyéni vállalkozók nyilvántartására;
  - a központi útiokmány-nyilvántartásra;
  - a közúti közlekedési nyilvántartásra;
  - a Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartására;
  - a szabálysértési nyilvántartási rendszerre;
  - a bűnügyi nyilvántartási rendszerre;
- a Nemzeti Rehabilitációs és Szociális Hivatalnak az egységes szociális nyilvántartására és az egységes örökbefogadási nyilvántartásra;
- a Földmérési és Távérzékelési Intézetre és a földhivatalokra, mint az ingatlan-nyilvántartás, a földhasználati nyilvántartás és egyéb földmérési és térképészeti, a rendeletben meghatározott nyilvántartás adatfeldolgozóira;
- az Országos Nyugdíjbiztosítási Főigazgatóságra[201], mint a nyugdíjbiztosítási nyilvántartás adatkezelőjére;
- az Országos Egészségbiztosítási Pénztárra[202], mint az egészségbiztosítási nyilvántartás adatkezelőjére;
- az MH Geoinformációs Szolgálat és HM Térképészeti Közhasznú Nonprofit Kft.-re, a közepes és kisméretarányú állami topográfiai térképek adatfeldolgozása tekintetében;
- a Pillér Pénzügyi és Számítástechnikai Kft.-re, a Nemzeti Adó- és Vámhivatal által kezelt adó- és vámhatósági adatok nyilvántartásának adatfeldolgozása tekintetében;
- a Nemzeti Infokommunikációs Szolgáltató Zrt.-re, a Foglalkoztatási és Szociális Adatbázis, a kulturális örökségvédelmi nyilvántartás elektronikus adatfeldolgozása tekintetében;

b) az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemekre (pl.: pénzintézetek, erőművek, távközlési rendszerek).

---

[200] A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III.22.) Korm. rendelet melléklete alapján.

[201] A társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 40. § a) pont.

[202] A társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 40. § b) pont.

3. melléklet

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerinti alap szervezeti biztonsági szintek[203]

2. biztonsági szint: Köztársasági Elnöki Hivatal, Országgyűlés Hivatala, Alkotmánybíróság Hivatala, Alapvető Jogok Biztosának Hivatala, helyi és nemzetiségi önkormányzatok képviselő-testületének hivatalai és a hatósági igazgatási társulások.

3. biztonsági szint:

A) központi államigazgatási szervek:

a) Miniszterelnökség és a minisztériumok,

b) autonóm államigazgatási szervek (Közbeszerzési Hatóság, Egyenlő Bánásmód Hatóság, a Gazdasági Versenyhivatal, Nemzeti Adatvédelmi és Információszabadság Hatóság, Nemzeti Választási Iroda),

c) kormányhivatal, mint törvény által létrehozott, a Kormány irányítása alatt működő szerv (Központi Statisztikai Hivatal, Országos Atomenergia Hivatal, Szellemi Tulajdon Nemzeti Hivatala, Nemzeti Adó- és Vámhivatal),

d) központi hivatalok, mint kormányrendelet által létrehozott, miniszter irányítása alatt működő szervek (pl.: Magyar Államkincstár, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, Bevándorlási és Állampolgársági Hivatal, Országos Meteorológiai Szolgálat, Oktatási Hivatal, Klebelsberg Intézményfenntartó Központ, Szociális és Gyermekvédelmi Főigazgatóság),

e) rendvédelmi szervek (rendőrség, büntetés-végrehajtási szervezet, hivatásos katasztrófavédelmi szerv, polgári nemzetbiztonsági szolgálatok – Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat) és a Katonai Nemzetbiztonsági Szolgálatra,

f) önálló szabályozó szervek (Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal),

B) bírósági szervezetrendszer (Országos Bírósági Hivatal, Kúria, ítélőtábla, törvényszék, járásbíróság és kerületi bíróság, közigazgatási és munkaügyi bíróság),

C) ügyészségi szervezetrendszer (Legfőbb Ügyészség, fellebbviteli főügyészség, főügyészségek, járási ügyészségek),

[203] Ibtv. 9. § (1) és (2) bekezdés

D) Állami Számvevőszék,

E) Magyar Nemzeti Bank,

F) fővárosi és megyei kormányhivatalok.

4. biztonsági szint: Magyar Honvédség

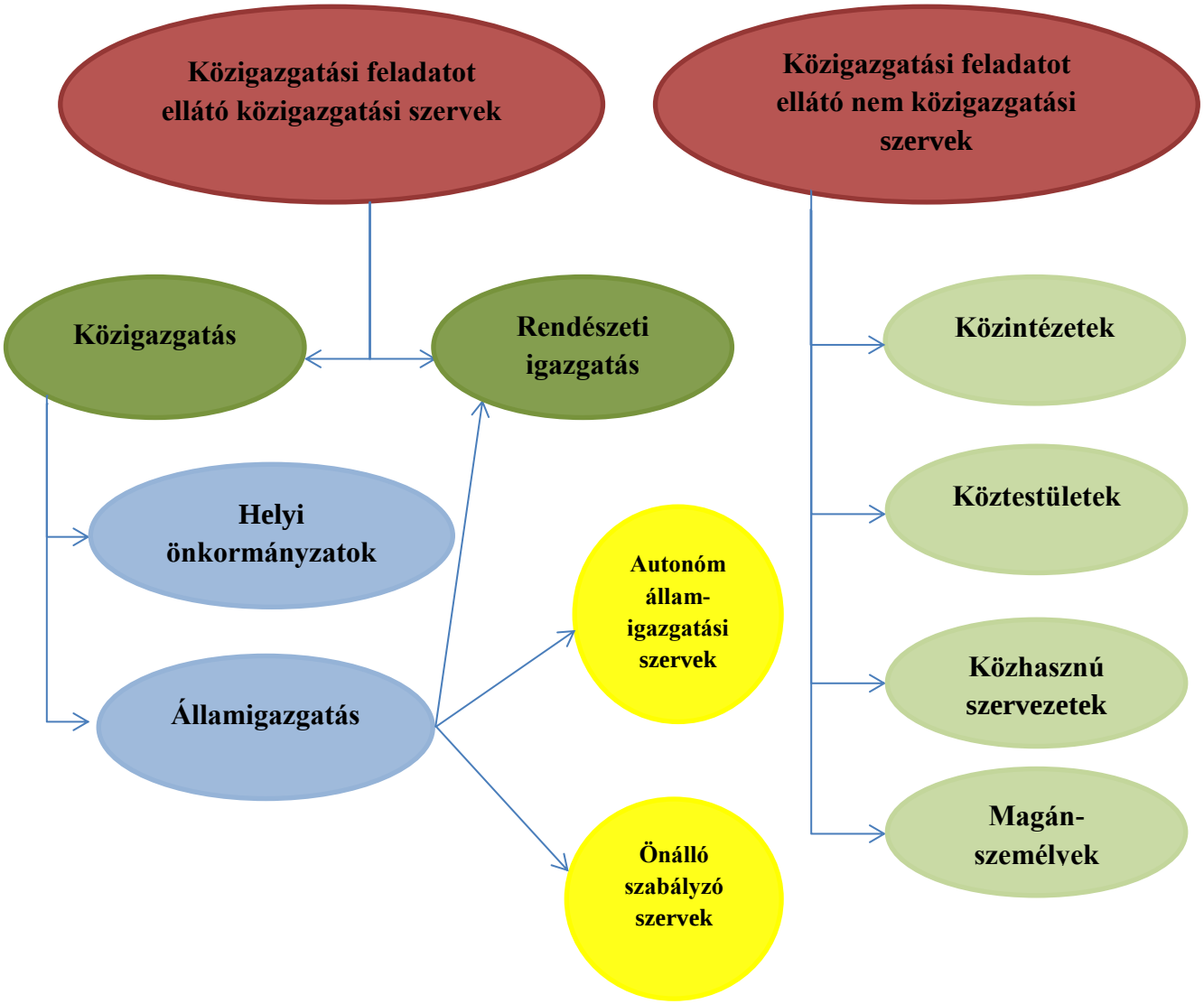
5. biztonsági szint:

A) nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,

B) európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek

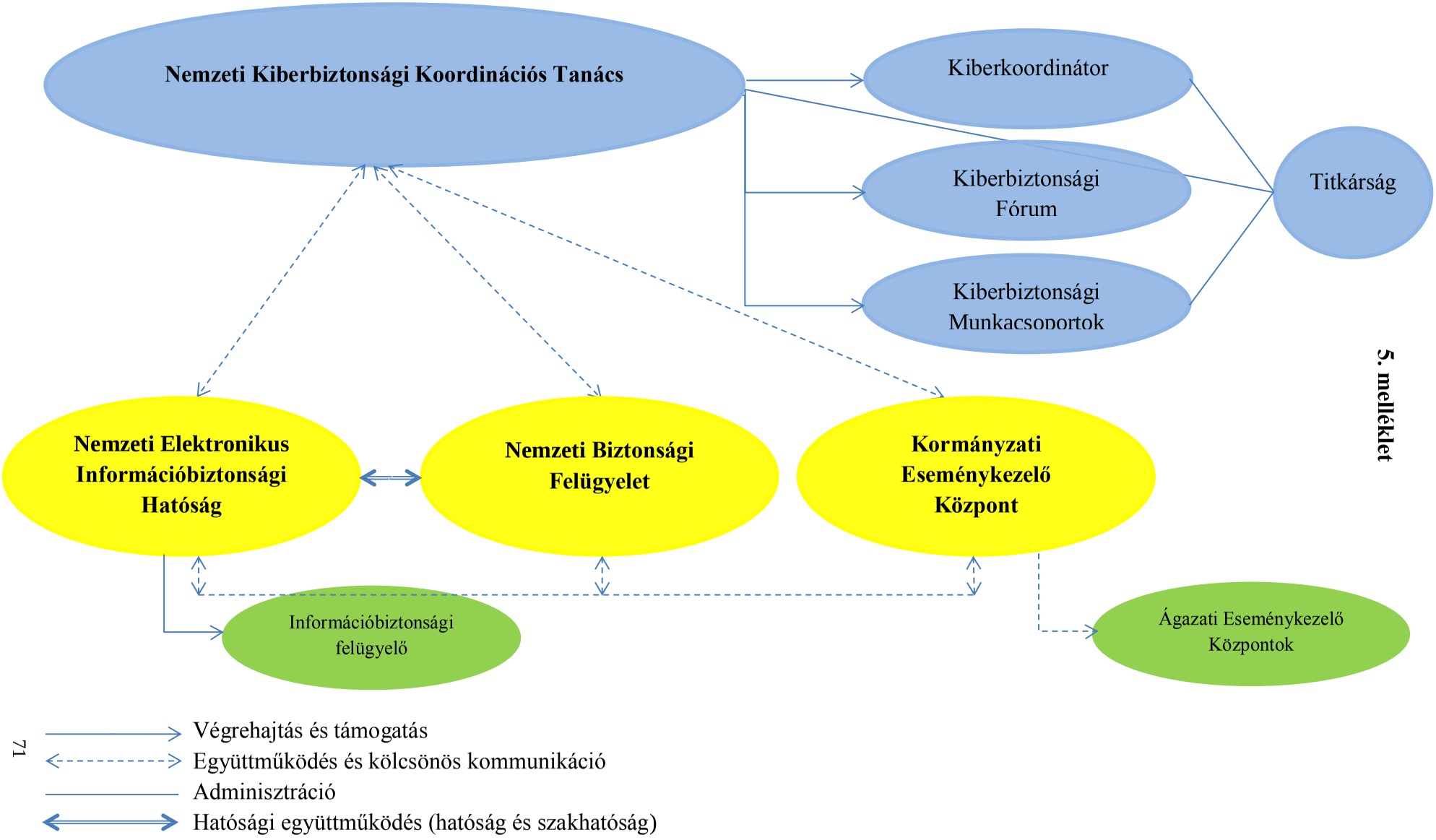
4. melléklet

A MAGYAR KÖZIGAZGATÁS INTÉZMÉNYRENDSZERE



5. melléklet

AZ ÁLLAMI ÉS ÖNKORMÁNYZATI SZERVEK ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGÁRÓL SZÓLÓ 2013. ÉVI L. TÖRVÉNY SZERVEZETRENDSZERE



Felhasznált irodalom

1. Szilágyi Péter: Jogi alaptan (Osiris Kiadó, 2003. Budapest)
2. Fazekas Marianna – Ficzere Lajos: Magyar közigazgatási jog – Általános rész (Osiris Kiadó, 2002. Budapest)

Felhasznált és kapcsolódó főbb jogszabályok jegyzéke

1. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (Magyar Közlöny 2013. évi 47. szám)

   a) A kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet (Magyar Közlöny 2012. évi 29. szám)

   b) Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat (Magyar Közlöny 2012. évi 19. szám)

2. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Magyar Közlöny 2013. évi 69. szám)

   a) Az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelet (Magyar Közlöny 2013. évi 111. szám)

   b) A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet (Magyar Közlöny 2013. évi 129. szám)

   c) A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet (Magyar Közlöny 2013. évi 211. szám)

d) A zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet (Magyar Közlöny 2013. évi 123. szám)

e) A Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet (Magyar Közlöny 2013. évi 143. szám)

f) A Nemzeti Adó- és Vámhivatal elektronikus információs rendszerei biztonságának felügyeletéről és ellenőrzéséről szóló 34/2013. (VIII. 30.) NGM rendelet (Magyar Közlöny 2013. évi 143. szám)

g) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (Magyar Közlöny 2013. évi 173. szám)

h) Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet (Magyar Közlöny 2013. évi 201. szám)

i) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és a biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet (Magyar Közlöny 2013. évi 214. szám)

j) A diplomáciai információs célokra használt zárt célú elektronikus információs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 3/2014. (II.26.) KüM rendelet (Magyar Közlöny 2014. évi 29. szám)

3. A létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Magyar Közlöny 2012. évi 154. szám)

a) A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (Magyar Közlöny 2013. évi 40. szám)

4. A minősített adat védelméről szóló 2009. évi CLV. törvény (Magyar Közlöny 2009. évi 194. szám)

   a) A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet (Magyar Közlöny 2010. évi 44. szám)

   b) Az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet (Magyar Közlöny 2010. évi 47. szám)

   c) A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet (Magyar Közlöny 2010. évi 69. szám)

5. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Magyar Közlöny 2011. évi 88. szám)

6. A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény (Magyar Közlöny 2010. évi 196. szám)

7. A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Magyar Közlöny 2012. évi 92. szám)

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.