Nemzeti
Közszolgálati Egyetem
Vezető- és Továbbképzési Intézet

DR. BODÓ ATTILA PÁL (szerk.)

Információbiztonsági jogi ismeretek vezetőknek

Budapest, 2014

A tananyag az ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel című projekt keretében készült el.

Kiadja:
© NKE, 2014

Felelős kiadó:
Patyi András
rektor

Budapest, 2014

Hatályosítva: 2015. április 30.

ISBN 978-615-5491-67-2

Tartalom

1. Gondolatok az elektronikus információbiztonságról 5

2. Stratégiaalkotás 6
2.1. Nemzeti jövőkép és szabályozás 6
2.2. Nemzeti cselekvési területek 7
2.3. Kormányzati intézkedések 8
2.4. Stratégiaalkotás az Európai Unióban 9

3. Törvényi szabályozás 11
3.1. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11
3.1.1. Az Ibtv. alapelvei és fogalmi rendszere 11
3.1.2. Az Ibtv. hatálya 13
3.1.3. Az elektronikus információs rendszerek biztonsági osztályba sorolása és a szervezetek biztonsági szintjének meghatározása 16
3.2. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 19
3.3. Kapcsolódó törvényi rendelkezések 22
3.3.1. A minősített adat védelméről szóló 2009. évi CLV. törvény 22
3.3.2. A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 23
3.3.3. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 23
3.3.4. Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény 23

4. Az elektronikus információbiztonság szervezetrendszere 25
4.1. Kormányzati koordináció 25
4.2. Hatóság és szakhatóság 26
4.3. Eseménykezelő központok 27
4.3.1. A kormányzati eseménykezelő központ és az ágazati eseménykezelő központok 27
4.3.2. A Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja 28
4.4. A Nemzeti Közszolgálati Egyetem központi szerepe 29

5. Végrehajtási szabályok 31
5.1. A hatóság és a szakhatóság eljárása 31
5.1.1. A hatósági eljárás lefolytatása 31
5.1.1.1. A hatósági eljárás általános szabályai 31
5.1.1.2. Az egyes hatósági eljárások lefolytatása 32
5.1.2. A szakhatósági eljárás lefolytatása 33
5.1.2.1. A sérülékenységvizsgálat 33
5.1.2.2. A biztonsági események adatainak műszaki vizsgálata 34
5.1.3. A hatósági, szakhatósági eljárás jogkövetkezményei 34
5.2. Bejelentési és nyilvántartási rendszer 34
5.2.1. A szervezet hatósági nyilvántartásba vétele 35
5.2.2. A biztonsági események bejelentése, közzététele 36
5.3. Technológiai követelmények meghatározása 36
5.3.1. Az elektronikus információs rendszerek biztonsági osztályba sorolása 36
5.3.2. Az elektronikus információs rendszereket működtető szervezetek biztonsági szintbe sorolása 37
5.3.3. Az elektronikus információs rendszerek védelmével, a biztonsági szintek kialakításával összefüggő intézkedések köre 39

5.4. Elektronikus információbiztonság az oktatásban 40
5.5. Ágazati speciális szabályok 41

6. Felelősségi szabályok 43
6.1. Az elektronikus információs rendszerek védelmét biztosító kötelezettségek 43
6.1.1. A szervezet vezetőjének feladatai, kötelezettségei 43
6.1.2. Az elektronikus információs rendszer biztonságáért felelős személy feladatai, kötelezettségei 44
6.1.3. .Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy feladatai 45
6.2. Az információs rendszerekkel kapcsolatos bűncselekmények 45
6.3. Polgári jogi és munkajogi szabályok 47

7. Felhasznált és kapcsolódó főbb jogszabályok jegyzéke: 49

8. Felhasznált internetes források jegyzéke: 51

1. Gondolatok az elektronikus információbiztonságról

A digitalizáció hatására a társadalmi és gazdasági folyamatok egyre nagyobb részben információs hálózatokon keresztül mennek végbe, amely „virtualizálódás" 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 információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.[1] A kibertérben megjelenő veszélyek – kül- és belbiztonsági tevékenységek, gazdasági-, társadalmi-, állami működés megzavarás**ára**, megszakítás**ár**a, illetve megakadályozás**ára irányuló**, továbbá egyes károkozó tevékenységek – egyre nagyobb biztonsági kockázattal járnak az államok és a társadalom tagjai, a gazdaság szereplői számára. Az elmúlt években megszaporodtak és egyre összetettebbé váltak az információs infrastruktúrák elleni, a kibertérből érkező támadások (pl.: Stuxnet, Duqu, Red October, MiniDuke, Teamspy), melyek fizikai megjelenésük **útján** kihatnak a kibertérhez kapcsolódó elektronikus információs rendszerekre is. Ezzel összefüggően a **közigazgatás és a társadalom működését lehetővé tevő informatikai infrastruktúrák** és a nemzeti adatvagyon védelme, a biztonság megerősítése és fenntartása kormányzati és társadalmi igénnyé és ebből következően kiemelt feladattá vált.

2011-ben kezdődött az az előkészítő munka, amely jogalkotási feladatként tűzte ki célul az elektronikus információbiztonság szabályozási környezetének kialakítását. A Kormány 2011. második félévétől kezdve szerepeltette munkatervében[2] az elektronikus információbiztonság szabályairól szóló törvényre vonatkozó előterjesztés elkészítését és a szabályozási környezet kialakítását. Jelen tananyag az újonnan kialakított szabályozási környezet középpontba helyezésével és kapcsolódó egyéb szabályozások felhívásával – a rendszertani megközelítésre fókuszálva – mutatja be az elektronikus információbiztonság hatályos jogi környezetét. A tananyag célja, hogy rávilágítson a terület főbb szabályaira és sajátosságaira, a részletszabályok megismeréséhez szükséges hivatkozások megadása mellett.

1 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 1. § (1) bekezdés 22. pontja.

2 1236/2011. (VII. 7.) Korm. határozat, 1429/2011. (XII. 7.) Korm. határozat, 1226/2012. (VII. 6.) Korm. határozat, 1636/2012. (XII. 19.) Korm. határozat.

2. Stratégiaalkotás

A hatékony és hosszútávra tervezhető feladatellátás egyik alapvető eszköze, hogy az egyes szakterületeket érintően megfogalmazott célok és azok elérésének lehetséges módjai meghatározásra kerüljenek, azaz a stratégiai tervdokumentumok kidolgozása megtörténjen. A Magyary Zoltán Közigazgatás-fejlesztési Program (továbbiakban: Magyary Program) ezt felismerve 2011-ben célul tűzte ki a közigazgatási stratégiaalkotás megújítását annak érdekében, hogy rögzítésre kerüljenek az alkalmazandó stratégiai dokumentumok egyes típusai, valamint kötelező formátumuk, tartalmuk és rangsorrendszerük. Ezen célkitűzés alapján született meg *a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet* (továbbiakban: Stratégiai R.), mely meghatározza azokat az egységes szempontokat és elveket, amelyek szerint sor kerül a kormányzati stratégiai dokumentumok kidolgozására, nyomon követésére, értékelésére és felülvizsgálatára.

A Magyary Programban és fent jelzett kormányrendeletben megfogalmazott elvek figyelembevételével került kidolgozásra a *Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat* (továbbiakban: Nemzeti Biztonsági Stratégia), amely 1. mellékletének 31. pontja Magyarországot érintő biztonsági kihívásként azonosítja a kiberbiztonság[3] megteremtését és az ehhez kapcsolódó feladatokat. Ezek között rögzíti a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását és a nemzetközi együttműködésben való részvételt.[4]

Az elektronikus információbiztonság szabályozási környezete kialakításának egyik első állomásaként – párhuzamosan a kapcsolódó törvény előkészítésével – 2013 márciusában elfogadásra került Magyarország Nemzeti Kiberbiztonsági Stratégiája[5] (továbbiakban: Kiberstratégia), mely a Nemzeti Biztonsági Stratégiában foglaltakat részletezve – összhangban a Stratégiai R.-ben foglaltakkal – elemzi Magyarország jelenlegi kiberbiztonsági helyzetét, jövőképét, továbbá megnevezi az elérendő célokat és az alkalmazandó eszközöket.

2.1. Nemzeti jövőkép és szabályozás

A Kiberstratégia célja, hogy *„…meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is,"*[6] melynek szabad, demokratikus jogállami és biztonságos működését Magyarország alapvető értéknek és érdeknek tekinti.

A magyar kibertér fogalmát *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* (továbbiakban: Ibtv.) adja meg, mely szerint a 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.[7]

A Kiberstratégiában rögzített célok és cselekvési területek a magyar kibertérre terjednek ki, és ezen feladatok hatékony megvalósításával járulhat hozzá Magyarország a globális kibertér védelméhez. Annak érdekében, hogy a magyar kibertér megfeleljen a jövő kihívásainak, biztonságos és megbízható környezetet kell biztosítania:

a.) az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,
b.) a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,
c.) a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,
d.) az állami szolgáltatások innovatív és előremutató fejlesztéséhez hozzájárulva az elektronikus közigazgatás számára.[8]

3 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.
4 Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat 31. pont a) és b) alpont.
5 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról (továbbiakban: Kiberstratégia).
6 Kiberstratégia 1. pont.
7 Ibtv. 1. § (1) bekezdés 35. pont
8 Kiberstratégia 8. pont

A Kiberstratégia hangsúlyozza, hogy a kibertér szabadságának és biztonságának fenntartása több szinten megvalósítandó feladat. Nemzeti szinten elengedhetetlen a kormányzati tevékenységben a tudományos, a gazdasági és a civil szféra szereplőinek hatékony közreműködése is. Mivel az elektronikus információs rendszerek egy világszintű hálózatot alkotnak, a nemzetközi szintű – más államokkal és nemzetközi szervezetekkel (EU, NATO, EBESZ, ENSZ, Európa Tanács) történő –, kölcsönös bizalmon alapuló együttműködés kialakítása ugyanolyan jelentőséggel bír. Magyarországnak – geopolitikai helyzetéből adódóan – figyelemmel kell lennie a közép- és kelet-európai régióra, melynek kiberbiztonsága regionális együttműködések keretében tovább erősíthető.

A nemzetbiztonsági, a hatékony válságkezelési és felhasználóvédelmi szempontok szem előtt tartásával a Kiberstratégia meghatározza a szabad és biztonságos kibertér használat érdekében elérendő nemzeti célokat, úgy mint

a.) hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek kiépítését a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen,

b.) a nemzeti adatvagyon megfelelő szintű védelmét, a létfontosságú rendszerek és létesítmények üzembiztos működését, megfelelően gyors, hatékony és a veszteséget minimalizáló, különleges jogrend idején is alkalmazható helyreállítási képességet,

c.) a legjobb nemzetközi gyakorlatoknak, hazai és nemzetközi biztonsági tanúsítási szabványoknak megfelelő színvonalú informatikai, hírközlési termékek és szolgáltatások kialakítását a magyar kibertérben,

d.) a legjobb nemzetközi gyakorlatoknak megfelelő kiberbiztonsági oktatás, képzés, kutatás és fejlesztés, továbbá hazai tudásbázis kialakítását,

e.) a legjobb nemzetközi gyakorlatoknak megfelelően kialakított biztonságos kiberteret a gyermekek és a jövő nemzedékek számára.

2.2. Nemzeti cselekvési területek

A Kiberstratégia kilenc cselekvési területet, azaz intézkedési vagy beavatkozási irányt azonosít, amelyek kezelése a kiberbiztonság megfelelő szinten tartásához, folyamatos fejlesztéséhez és a kitűzött célok eléréséhez szükséges:

1. *Kormányzati koordináció:* a kormányon belüli, továbbá az állami, gazdasági, tudományos és civil szereplők közötti együttműködés koordinációjának elősegítése és a végrehajtás figyelemmel kísérése a Miniszterelnökség keretein belül létrehozott testület révén.
2. *Együttműködés:* olyan operatív együttműködési fórumok működtetése, amely a civil, a gazdasági és a tudományos területek képviselőinek részvételét biztosítja a kormányzati döntés-előkészítési folyamat során és lehetőséget nyújt arra, hogy ezen fórumok tagjai ajánlásokat és véleményt fogalmazzanak meg a kiberbiztonsági tevékenység fejlesztésére, folyamatos újítására.
3. *Szakosított intézmények:* egymással, valamint az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködő, speciális szakértelemmel és hatáskörrel rendelkező szervezetek általi feladatellátás a kibervédelem terén [pl. az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által akkreditált tagszervezetként működő kormányzati eseménykezelő központ és az egyes szakágazatok területén működtetett ágazati eseménykezelő központok].
4. *Szabályozás:* többszintű (törvényi, kormányrendeleti és miniszteri rendeleti szintű) jogalkotási tevékenység és együttműködési megállapodások a civil, a gazdasági és a tudományos terület szereplőivel.
5. *Nemzetközi együttműködések:* Magyarország aktív szerepének további erősítése az EU és a NATO keretein belül folyó kibervédelmi kezdeményezésekben, együttműködésben és kibervédelmi gyakorlatokban, valamint az ENSZ és az EBESZ kiberbiztonsági együttműködéseiben. Szerepvállalás a nemzeti/kormányzati és ágazati incidenskezelő központok európai, atlanti és globális szervezeteiben, az Európai Hálózati és Információ Biztonsági Ügynökségben, valamint az Európai Elektronikus Hírközlési Hatóságok Testületében.
6. *Tudatosság:* a kiberbiztonsággal összefüggő hazai és nemzetközi szakmai fórumok szervezése; a kibertér biztonságos használatát célzó és figyelemfelhívó tevékenységek, a kiberbiztonsági gyakorlati tudást elősegítő kezdeményezések, valamint a civil és gazdasági szféra tudatosságnövelésének támogatása.
7. *Oktatás, kutatás-fejlesztés:* a kiberbiztonság szakterület beépítése az általános, a közép- és felsőoktatás, továbbá a kormányzati tisztviselők képzésének és a szakmai továbbképzések informatikai oktatásába; stratégiai együttműködési megállapodások kidolgozása az állam és azon egyetemi és tudományos kutatóhelyek között, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.
8. *Gyermekvédelem:* a Gyermekbarát Internet Európai Stratégiája célkitűzéseinek figyelembevételével a gyermekeknek és fiataloknak szóló minőségi online tartalmak előállításának ösztönzésére, a tudatosságnövelő és felkészítő intézkedések támogatására, a gyermekek zaklatása és kizsákmányolása elleni küzdelemre és a biztonságos

online környezet megteremtésére irányuló intézkedések bevezetése, együttműködve az online gyermekvédelem terén eredményeket elért magyar civil szervezetekkel.

9. *Gazdasági szereplők motivációja:* olyan intézkedések kidolgozása a gazdasági szereplők számára, amelyek a kiberbiztonság fokozását célozzák, így különösen az informatikai és hírközlési közbeszerzések kapcsán olyan kiberbiztonsági követelmények meghatározása, amelyek során a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönzik a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat.

2.3. Kormányzati intézkedések

A Kiberstratégiában kifejtett célok eléréséhez Magyarország már rendelkezik a szükséges kompetenciák és potenciális erőforrások jelentős részével. Ezek közé tartozik:

1. *A magyar kibertér biztonságáért felelős kormányzati szervek számbavétele, koordinációja és együttműködése.* A Kiberstratégia, az Ibtv., valamint *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény* rendelkezései figyelembevételével felállításra került a Nemzeti Kiberbiztonsági Koordinációs Tanács és szervezete (Kiberbiztonsági Fórum és Kiberbiztonsági Munkacsoportok), a Nemzeti Elektronikus Információbiztonsági Hatóság, valamint a kormányzati eseménykezelő központ (ezen szervek feladat- és hatáskörét lásd részletesen a 4. és 5. fejezetben).
2. *A magyar kibertér biztonságáért felelős civil, gazdasági és tudományos szervezetek számbavétele és intézményes keretek között folyó együttműködés kialakítása.* A Kiberbiztonsági Munkacsoportokon keresztül megtörténik a nem kormányzati szakértők bevonása a magyar kibertér biztonságát érintő döntéshozatalba (lásd részletesen 4.1. pont).
3. *A létfontosságú információs infrastruktúrák és vagyonelemek, illetve a nemzeti adatvagyon számbavétele és védelmének biztosítása.* A vonatkozó jogszabályok (lásd: 3.2. és 4.3. pontok) alapján megtörténik a nemzeti és európai létfontosságú rendszerelemek kijelölése, és megkezdte működését a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja, amely a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet látja el. Megalkotásra kerültek a nemzeti adatvagyont érintő alapvető jogszabályok, *a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény* és *a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet*.
4. *A szakosított kormányzati intézmények működtetése.* Az elektronikus információs rendszerek biztonságának felügyeletét a Nemzeti Elektronikus Információbiztonsági Hatóság látja el, melynek tevékenységét egyes feladatok esetén szakhatóságként a Nemzeti Biztonsági Felügyelet segíti. A biztonsági események kezelése a kormányzati és ágazati eseménykezelő központok, és a nemzeti létfontosságú rendszerek és létesítmények ágazati eseménykezelő központjának a feladata (az intézményrendszer részleteit a 4. fejezet tartalmazza).
5. *A szabályozási környezet biztosítása.* A Kiberstratégia és a kapcsolódó jogszabályi rendelkezések megteremtették a kibervédelem általános jogi alapjait Magyarországon. Az Ibtv. felhatalmazást ad számos végrehajtási rendelet megalkotására a részletszabályok kidolgozása érdekében, melyek már hatályba léptek, így az abban rögzített szabályok a gyakorlatban alkalmazhatóak és alkalmazandóak (a hatályba lépett jogszabályokat lásd a Felhasznált és kapcsolódó jogszabályok jegyzékében).
6. *Nemzetközi és regionális együttműködésekben történő részvétel, politikai, operatív és szabályozási szinten egyaránt.* Az Európai Unió tagállamaként Magyarország részese az EU kibervédelmi törekvéseinek (lásd 2.4. pont és 4.5. pont), rendszeresen részt vesz a NATO által szervezett kibervédelmi gyakorlatokban. Szorosabb együttműködést alakított ki a szomszédos országokkal, köztük a Visegrádi Négyek tagállamaival.
7. *Támogatási keretrendszer kialakítása a kutatás és fejlesztés, valamint az oktatás és tudatosítás terén.* Az illetékes minisztérium már több egyetemmel is kötött együttműködési megállapodást annak érdekében, hogy az információbiztonság és az adatvédelem iránt érdeklődő hallgatók tanulmányaik során megismerkedjenek a közigazgatás e területén működő intézmények munkájával.
8. *Gazdasági motivációs rendszerek megteremtése.* A Nemzeti Kiberbiztonsági Koordinációs Tanács mellett működő Kiberbiztonsági Munkacsoportok munkájában a nem kormányzati szereplők is részt vesznek (vö. 2. pont), ezáltal a gazdasági élet képviselői is részt vállalhatnak a kibervédelem nemzeti irányvonalainak és célkitűzéseinek meghatározásában, melyek az egyes fejlesztési projektekhez kapcsolódó közbeszerzési eljárások során érvényesülnek.
9. *A kiberbiztonsági szempontok érvényesítése az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során.* A Nemzeti Elektronikus

Információbiztonsági Hatóság az elektronikus információs rendszerek és az azokban kezelt adatok biztonsága érdekében jogosult a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását.

Ezen eszközök megerősítését és a kiberbiztonság céljait szolgáló hatékony felhasználását hivatott elősegíteni a Nemzeti Kiberbiztonsági Koordinációs Tanács és az irányításával kialakítás alatt álló együttműködési rendszer a kormányon belüli és nem-kormányzati szereplők között.

2.4. Stratégiaalkotás az Európai Unióban

Az Európai Bizottság, mint az Európai Unió döntés-előkészítő, végrehajtó, döntéshozó, ellenőrző és képviseleti szerve (az Európai Parlament és az Európai Unió Tanácsa mellett a három fő uniós kormányzati intézmény egyike) először 2001-ben, *„Hálózat- és információbiztonság: javaslat egy európai politikai megközelítésre" című közleményében* hívta fel a figyelmet a hálózat- és információbiztonság növekvő jelentőségére. Ezt 2006-ban követte a biztonságos információs társadalomra irányuló stratégia elfogadása, amelynek célja az európai hálózat- és információbiztonsági kultúra kialakítása volt. 2009-ben jelent *meg a kritikus informatikai infrastruktúrák védelméről (CIIP) szóló bizottsági közlemény*, amely Európa hálózati zavarokkal szembeni védelmével foglalkozott. Az Európai Bizottság mellett az Európai Unió Tanácsa – mely az Európai Parlamenttel együtt az Európai Unió törvényhozó szerve – is foglalkozott az információbiztonság kérdésével, amikor 2009-ben állásfoglalást fogadott el *„a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről"*. Érzékelhető, hogy az Európai Unió bár felismerte az információbiztonság tárgykörének fontosságát, korábban csupán közlemények, állásfoglalások szintjén foglalkozott a témával, a megelőzés, észlelés és elhárítás terén megvalósítandó feladatokat általános és kötelező jelleggel előíró jogszabályok elfogadására uniós szinten nem került sor.

Az Európai Unió először az információs rendszerek elleni támadások szankcionálása tárgyában alkotott konkrét szabályokat. *Az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat*[9] célja a tagállami büntetőjogszabályok harmonizálása a tagállamok igazságügyi és egyéb hatóságai – így a rendőrség és egyéb bűnüldözési szakszolgálatok – közötti együttműködésének javítása érdekében. A kerethatározat alapvetően büntetőjogi megközelítést alkalmaz, rögzíti, hogy melyek azok a cselekmények, amelyek megvalósítását a tagállamoknak legalább jelentősebb bűncselekménynek kell minősíteniük, milyen szempontok mentén kell meghatározni a szankciókat, melyek a súlyosbító körülmények és miként alakul a jogi személyek felelőssége és szankcionálása. *A Büntető Törvénykönyvről szóló 2012. évi C. törvény* (továbbiakban: Btk.) 375. §-a és XLIII. fejezete – melyet a 6. fejezet részletesen tárgyal – ezen kerethatározatban foglaltakkal összhangban került megalkotásra.

További, az információbiztonság témaköréhez kapcsolódó szektorális szabályok megalkotására került sor az elektronikus hírközlés *(2009/136/EK irányelv)*, a személyes adatok védelme *(95/46/EK irányelv)*, az általános adatvédelem (a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló rendelet tervezete) és a létfontosságú rendszerelemek védelme *(2008/114/EK irányelv)* terén. Ezek az irányelvek olyan európai uniós jogi aktusok, amelyek az elérendő célok tekintetében kötelezik a tagállamokat, de az általános cél megvalósításának konkrét formáját, a megfelelő eljárásokat és eszközöket a tagállamok maguk választják meg. A tagállamoknak kötelességük, hogy az irányelvben foglaltak meghatározott időn belül nemzeti jogszabályaikban meghatározásra kerüljenek, azaz jogszabályi szinten rögzíteni kell az előírásokat.

Az Európai Bizottság 2010 májusában mutatta be az *Európai Digitális Menetrend* című akciótervét, melynek célja a gazdasági fellendülés felgyorsítása és a fenntartható digitális jövő alapjainak megteremtése. A cselekvési terv hét kiemelt intézkedési területet határozott meg, melyek közül az egyik az internet iránti bizalom és a biztonság erősítése, figyelemmel arra, hogy a fent említett kerethatározatban foglaltak ellenére az információs rendszerek elleni támadások száma továbbra is nőtt. A Bizalom és biztonság intézkedési területen célként került meghatározásra:

a.) a javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;

b.) a számítógépes támadások elleni gyorsreagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepének megerősítése;

c.) a javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;

9 A kerethatározat egy olyan uniós jogi eszköz, amely a tagállami jogi és a közigazgatási előírások harmonizálását szolgálja. A kerethatározatban megfogalmazott cél megvalósítása a tagállam számára kötelező feladat, de a végrehajtási formáját és eszközét a tagállamok szabadon választhatják meg (pl. a meglévő jogszabályaikat módosítják, vagy új jogszabályt alkotnak). Nem közvetlen hatályú, tehát a magánszemélyek a nemzeti vagy az európai bíróságok előtt közvetlenül nem hivatkozhatnak a kerethatározatban foglaltakra.

d.) a tudatosságnövelés, így többek között az internetes védelem iskolai oktatása;
e.) egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;
f.) a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

A célok közül kiemelendő, hogy az a) pontban foglalt intézkedés végrehajtását szolgálja az *Európai Parlament és a Tanács 2013. augusztus 12-i, 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról*. Az irányelv – mely hatályon kívül helyezte a 2005/222/IB tanácsi kerethatározatot – meghatározza azokat a minimumszabályokat, amelyek mentén a tagállamoknak 2015. szeptember 4-ig harmonizálniuk kell a vonatkozó nemzeti büntetőjogi szabályaikat. A b) pontban foglalt intézkedések eredményeként az Európai Unió intézményei 2013-ban létrehozták a CERT-EU-t, megszületett az *Európai Parlament és a Tanács 2013. május 21-i, 526/2013/EU rendelete az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről*, valamint felállításra került a Számítástechnikai Bűnözés Elleni Európai Központ (az Európai Unió információbiztonsággal foglalkozó szervezeteit részletesebben a 4.5. pont mutatja be).

Az Európai Bizottság felismerte, hogy a Digitális Menetrendben foglaltak érvényesítése érdekében a büntetőjogi aspektus vizsgálata és kiteljesítése mellett uniós érdek a kiberbiztonság **kérdéskörének átfogó, stratégiai szintű áttekintése. Erre figyelemmel az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és** a Régiók Bizottsága 2013 februárjában közzétette közös közleményét *„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”* **című** uniós stratégiáról (továbbiakban: uniós stratégia). Az uniós stratégia az alábbi prioritásokat vázolja fel:

a.) az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtése;
b.) a számítástechnikai bűnözés drasztikus visszaszorítása;
c.) a kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát érintő képességek fejlesztése;
d.) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
e.) az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f.) a számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

Az uniós stratégiában foglaltak teljesítését célozza *a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvjavaslat* (továbbiakban: irányelvjavaslat). Az irányelvjavaslat előírja, hogy:

a.) a tagállamok a hálózat- és információbiztonság területén illetékes hatóságok létrehozásával, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) felállításával és nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek elfogadásával nemzeti szinten biztosítsák a képességek minimális szintjét;
b.) az illetékes nemzeti hatóságoknak hálózatot kell alkotniuk, amelyben együttműködnek az összehangolt információcsere, valamint az uniós szinten történő felderítés és reagálás biztosítása érdekében; a tagállamok e hálózaton keresztül az európai hálózat- és információbiztonsági együttműködési terv alapján bonyolítják a hálózat- és információbiztonsági fenyegetések és események elleni küzdelemhez szükséges információcserét és együttműködést;
c.) kialakuljon egy kockázatkezelési kultúra, és gyakorlattá váljon a magán- és a közszféra közötti információmegosztás a hálózatokat és információs rendszereket komolyan veszélyeztető, valamint a kritikus szolgáltatások folyamatosságát és az áruellátást jelentősen befolyásolni képes biztonsági eseményekről;
d.) a tagállamok nemzeti hálózat- és információbiztonsági stratégiát és együttműködési tervet készítsenek, hálózat- és információbiztonságért felelős nemzeti hatóságot jelöljenek ki, illetve ún. számítógépes vészhelyzeteket elhárító csoportot állítsanak fel a biztonsági események és kockázatok kezelésére;
e.) az érintett vállalkozások és a közszféra számára bizonyos biztonsági követelmények kerüljenek meghatározásra és ezen szereplők számára esemény bejelentési kötelezettség álljon fenn.

Az Európai Unió intézményei kiemelt figyelmet fordítanak az uniós stratégia és az irányelvjavaslat mielőbbi véglegesítésére, valamennyi soros elnökség prioritásként kezeli a kérdést.

A fentiekben és a további fejezetekben kifejtettek alapján elmondható, hogy a kiberbiztonságot érintő hazai törvényi szabályozás, melyet az Európai Unió és tagállamai tekintetében Magyarország elsőként alkotott meg és léptetett hatályba, összhangban van az uniós elvekkel és elvárásokkal.

3. Törvényi szabályozás

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

A magyar kibertér biztonságos szabályozásának első jogalkotási lépése az Országgyűlés 2013. április 15-ei ülésnapján elfogadott, Ibtv. Az Ibtv. már címében meghatározza, hogy alapvetően mely szervezeti körre kíván szabályozni és tudatosan használja az információbiztonság kifejezés előtt az „elektronikus" jelzőt, mivel az állami és önkormányzati szervek esetében az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza. Olyan szabályozási környezet alapjait teremti meg, amely a prevenciót, a fenyegetéseket számba vevő, az elektronikus információs rendszer minden elemére kiterjedő védelmet, illetve az elektronikus információbiztonság tudatosságnövelését tekinti alapvetésnek. Ezeknek az alapelveknek a felhasználásával a biztonsági problémák kialakulásának a megelőzését és minimalizálását, a biztonsági események bekövetkezése esetén a felmerült problémák tudatos kezelését célozza meg.

3.1.1. Az Ibtv. alapelvei és fogalmi rendszere

A megelőzés, a biztonság, a védelem és a tudatosságnövelés, mint alapelvek és mint általános társadalmi igény már az Ibtv. preambulumában megjelennek: *„A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."* Az Ibtv. fogalmi rendszere fenyegetés alatt olyan lehetséges műveletet, eseményt vagy mulasztásos cselekményt rögzít, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát [Ibtv. 1. § (1) bekezdés 19. pont]. A preambulum további szövegezése szerint *„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."*

Ezek az alapelvek az értelmező rendelkezések között is helyet kapnak, mivel az Ibtv.-ben önálló fogalomként jelenik meg – többek között – a *bizalmasság,*[10] a *sértetlenség,*[11] a *rendelkezésre állás*[12] és a védelem különböző formáinak a meghatározása. Az Ibtv. fogalom meghatározása szerint:

a.) Bizalmasságnak az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.

b.) Sértetlenség alatt az adat azon tulajdonságát kell érteni, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

c.) Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.

Az új szabályozási környezet kialakítása és az egységes jogértelmezés biztosítása érdekében az Ibtv. széles kört felölelve, közel ötven pontban rögzíti az értelmező rendelkezéseket (1. § (1) bekezdés). Ezek jelentős része nem ismeretlen a magyar szakirodalomban, mivel azok tartalmukat tekintve a Közigazgatási Informatikai Bizottság[13] által kiadott ajánlásokban már megjelennek. A kifejezések igazodnak a szakterület nemzetközi dokumentumaiban foglaltakhoz, az információ biztonság területén nemzetközileg is elfogadott és elismert ISO/IEC 27000-es sorozathoz és a Common Criteria (CC – Közös Követelmények) elveihez.

Az Ibtv. preambulumában megjelenő alapelvek és az értelmező rendelkezések közötti összefüggésre visszautalva hangsúlyozni szükséges azt, hogy a védelem biztosítása kiemelt jelentőséggel bír e területen. Ennek megfelelően az Ibtv. magát a védelmi feladatokat is meghatározza [Ibtv. 1. § (1) bekezdés 46. pont] és rögzíti, hogy védelmi

10 Ibtv. 1. § (1) bekezdés 8. pont
11 Ibtv. 1. § (1) bekezdés 39. pont
12 Ibtv. 1. § (1) bekezdés 38. pont
13 Létrehozva a közigazgatási informatikai feladatok kormányzati koordinációjáról szóló 1026/2007. (IV. 11.) Korm. határozat 3. pontja alapján.

feladatok alatt a *megelőzést*, a *korai figyelmeztetést*, az észlelést, a *reagálást*, és magát az *eseménykezelést* kell érteni. Ez a meghatározás az igen széles körben elfogadott és a gyakorlatban is használt védelemi módszert, az ún. PreDeCo (Preventive-Detective-Corrective) elvet veszi alapul. A módszertan a védelmet három egymásra épülő és egymást kiegészítő részre, a megelőző (preventív), a felismerő (detektív) és az elhárító (korrektív) intézkedésekre helyezi, azzal, hogy ezek együttes alkalmazása éri el a kívánt védelmi hatást. A fogalmak meghatározásánál az Ibtv. rögzíti, hogy:

a.) megelőzés a fenyegetés által okozható hatás bekövetkezésének elkerülése [Ibtv. 1. § (1) bekezdés 36. pont]*;*

b.) korai figyelmeztetés olyan aktív szervezeti cselekvés, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni [Ibtv. 1. § (1) bekezdés 32. pont];

c.) észlelés a biztonsági esemény bekövetkezésének felismerése [Ibtv. 1. § (1) bekezdés 17. pont];

d.) reagálás a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés [Ibtv. 1. § (1) bekezdés 37. pont].

A védelmi intézkedések során kiemelt jelentősége van annak, hogy azoknak ún. *kockázatokkal arányos védelem* útján szükséges megvalósulniuk, azaz a védelmi intézkedésekre fordított **költsége**knek arányosnak kell lenni a fenyegetések által okozható károk értékével [Ibtv. 1. § (1) bekezdés 31. pont]. A védelem kérdését tekintve az Ibtv. már a fogalmi meghatározások között kiemelten kezeli a védelem különböző formáit és meghatározza azokat az alábbiak szerint:

a.) adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás [Ibtv. 1. § (1) bekezdés 6. pont];

b.) 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 [Ibtv. 1. § (1) bekezdés 20. pont];

c.) logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem [Ibtv. 1. § (1) bekezdés 34. pont];

d.) folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem [Ibtv. 1. § (1) bekezdés 21. pont];

e.) teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem [Ibtv. 1. § (1) bekezdés 44. pont];

f.) zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem [Ibtv. 1. § (1) bekezdés 48. pont].

A védelem különböző módozatara figyelemmel az Ibtv. általános biztonsági követelményként rögzíti az elektronikus információs rendszereknek azt az állapotát, amely során az elektronikus információs rendszerek teljes életciklusában meg kell valósítani azt, hogy az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmére kerüljön sor.[14]

A gyakorlatban fontos szerepe van annak, hogy a felsorolt védelmi intézkedések által lehetőleg elkerülhető legyen a biztonsági események bekövetkezése. Biztonsági eseménynek azt a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot tekintjük, 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.[15] Ha mégis sor kerül a biztonsági esemény bekövetkezésére, annak azonnali észlelése és kezelése kiemelt jelentőséggel bír, ezért kulcsfontosságú a hiteles dokumentálás, a kiváltó okok azonosítása, az esetlegesen bekövetkezett károk felmérése, és a felelősség megállapítása.[16] A folyamat eredményeként a védelmi intézkedések kiegészítésével vagy megerősítésével, a szabályozás javításával és az érintettek oktatásával kell gondoskodni arról, hogy a biztonsági események bekövetkezésének a valószínűsége és az ezáltal okozott kár minimalizálható legyen. Az elektronikus információs rendszerek védelmének körében az Ibtv. hatálya alá tartozó szervezeteknek a külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatározniuk, úgy, hogy az intézkedéseknek támogatniuk kell a *megelőzés*t

14 Ibtv. 5. § és Ibtv. 1. § (1) bekezdés 15. pont

15 Ibtv. 1. § (1) bekezdés 9. pont

16 *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 (Ibtv. 1. § (1) bekezdés 10. pont)

és a *korai figyelmeztetés*t, az észlelést, a *reagálás*t és a *biztonsági események kezelését*.[17] Biztonság alatt az elektronikus információs rendszer olyan állapotát kell tehát érteni, amely során az összes számításba vehető fenyegetést figyelembe kell venni, és amely az elektronikus információs rendszer valamennyi elemére kiterjed, folyamatában megvalósul, illetve költségei arányosak a fenyegetések által okozható károkkal.

Az értelmező rendelkezések széles köre a jogalkalmazást hívatott segíteni. Egyes, további fogalmak ismertetésére az Ibtv. és végrehajtási rendeleteinek felépítéséhez igazodva, önállóan a kapcsolódó tananyagrésznél kerül sor.

3.1.2. Az Ibtv. hatálya

Az Ibtv. már az értelmező rendelkezések között rögzíti a tárgyi hatály megállapításához azt, hogy alkalmazásában mit tekint elektronikus információs rendszernek. E szerint elektronikus információs rendszernek[18] 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.

Eszközök alatt a környezeti infrastruktúr**át**, a hardvert, a hálózatot, és az adathordozókat, eljárások alatt a szabályozást, a szoftvert és a kapcsolódó folyamatokat kell érteni.

Az Ibtv. személyi hatályának rögzítése során alapelvként az alkotmányos rend és a közigazgatás hatékony működésének fenntartása szempontjából kiemelt jelentőséggel rendelkező, valamint a nemzeti adatvagyon kezelését ellátó szervezetek kerültek meghatározásra.

1. Ezen alapelvhez igazodva az Ibtv. hatálya[19]:
   a.) a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvényben rögzítettek figyelembevételével kiterjed a központi államigazgatási szervekre[20], ezen belül:
   - 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, Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal),
   - 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 szolgálatok21 – 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.

17 Ibtv. 6. §
18 Ibtv.1. § (2) és (3) bekezdés
19 Ibtv. 2. §
20 A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2)-(6) bekezdései.
21 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. §-a.

b.) kiterjed a Köztársasági Elnöki Hivatalra,[22] az Országgyűlés Hivatalára;[23]
c.) kiterjed az Alkotmánybíróság Hivatalára;[24]
d.) a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény rendelkezései figyelembevételével kiterjed az Országos Bírósági Hivatalra és a bíróságokra (Kúria, ítélőtábla, törvényszék, járásbíróság és a kerületi bíróság, közigazgatási és munkaügyi bíróság[25]);
e.) az ügyészségről szóló 2011. évi CLXIII. törvény figyelembevételével kiterjed az ügyészségekre (Legfőbb Ügyészség, fellebbviteli főügyészségek, főügyészségek, járási ügyészségek[26]);
f.) az Alapvető Jogok Biztosának Hivatalára;[27]
g.) az Állami Számvevőszékre;[28]
h.) a Magyar Nemzeti Bankra;[29]
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 kiterjed a fővárosi és megyei kormányhivatalokra (ideértve a fővárosi és megyei kormányhivatal szervezeti egységeit a járási és fővárosi kerületi hivatalokat[30]);
j.) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira (polgármesteri hivatal, megyei önkormányzati hivatal, közös önkormányzati hivatal[31]), a hatósági igazgatási társulásokra;[32]
Az Ibtv. hatálya nem terjed ki az önkormányzatok képviselő-testületeire, azok bizottságaira, és a közgyűlésre.
k.) a Magyar Honvédségre[33].

Az Ibtv. hatálya kiterjed továbbá az a)-k) pontokban felsorolt szervek és a számukra adatkezelést végző szervek[34] elektronikus információs rendszereinek védelmére.

2. Az Ibtv. szervi hatálya kiterjed:[35]
a.) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói elektronikus információs rendszereinek védelmére,[36] így többek között:
- a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala esetében:
  - a Foglalkoztatási és Közfoglalkoztatási Adatbázisra;
  - az állami foglalkoztatási szerv feladatainak ellátásához szükséges adatbázisra (pl.: a közfoglalkoztatásért felelős miniszter, mint első fokon eljáró állami foglalkoztatási szerv a kormányhivatalok bevonásával működteti a munkavédelmi és a munkaügyi feladatok ellátásához, az adatok nyilvántartásához szükséges egységes informatikai rendszert[37] – ilyen rendszer az Integrált Rendszer (IR), mely az ügyfelek nyilvántartási adatait tartalmazza;
  - a polgárok személyi adatainak és lakcímének nyilvántartására;
  - elektronikus anyakönyvi nyilvántartásra;
  - a központi idegenrendészeti nyilvántartására;
  - a Schengeni Információs Rendszer nemzeti rendszerére;
  - a kötvénynyilvántartásra;
  - az egyéni vállalkozók nyilvántartására;
  - a központi útiokmány-nyilvántartásra;
  - a közúti közlekedési nyilvántartásra;

22 A köztársasági elnök jogállásáról és javadalmazásáról szóló 2011. évi CX. törvény 15. §-a.
23 Az Országgyűlésről szóló 2012. évi XXXVI. törvény 123. §-a.
24 Az Alkotmánybíróságról szóló 2011. évi CLI. törvény 22. §-a.
25 A bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 16. §-a.
26 Az ügyészségről szóló 2011. évi CLXIII. törvény 8. §-a.
27 Az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 41. §-a.
28 Az Állami Számvevőszékről szóló 2011. évi LXVI. törvény 1-2. §-ai.
29 A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 5. §-a.
30 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.
31 Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 85. §-a.
32 Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 87. §-a.
33 A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 35. §-a és 38. §-a.
34 Ibtv. 1. § (1) bekezdés 4. és 5. pontja
35 Ibtv. 2. §
36 A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III.22.) Korm. rendelet melléklete alapján.
37 Az állami foglalkoztatási szerv, a munkavédelmi és munkaügyi hatóság kijelöléséről, valamint e szervek hatósági és más feladatainak ellátásáról szóló 320/2014. (XII. 13.) Korm. rendelet 5. § f) pontja.

  - 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 járási hivatalokra, mint az ingatlan-nyilvántartás, a földhasználati nyilvántartás és egyéb földmérési és térképészeti, a rendeletben meghatározott nyilvántartás adatfeldolgozóira;
- az Országos Nyugdíjbiztosítási Főigazgatóságra,[38], mint a nyugdíjbiztosítási nyilvántartás adatkezelőjére;az Országos Egészségbiztosítási Pénztárra,[39] 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 Mezőgazdasági és Vidékfejlesztési Hivatal a mezőgazdasági és vidékfejlesztési támogatási szerv által kezelt nyilvántartási rendszerek adatfeldolgozása tekintetében;
- a reForster Gyula Nemzeti Örökségvédelmi és Vagyongazdálkodási Központra[40] 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). A kapcsolódó törvény[41] főbb rendelkezéseinek bemutatását a 3.2. pont tartalmazza.

Ez a széles körben meghatározott személyi és tárgyi hatály hívatott biztosítani, hogy a szabályozás minden, az állam működése szempontjából lényeges elektronikus információs rendszer védelmére kitérjen. Bizonyos védelmi szempontok – kül- és belbiztonság, adat- és információvédelem – alapján szükséges azonban, hogy az Ibtv. rendelkezései korlátok között érvényesüljenek. Ennek érdekében az Ibtv. rendelkezéseit a minősített adatokat kezelő elektronikus információs rendszereket érintően *a minősített adat védelméről szóló 2009. évi CLV. törvényben* meghatározott eltérésekkel kell alkalmazni.

Az Ibtv. a tárgyi hatály meghatározásánál rögzíti, hogy a hatósági és a szakhatósági feladatok ellátása tekintetében bizonyos 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 esetében az irányítási feladatokat gyakorló miniszter rendeletben szabályozza ezen feladatok ellátását.[42]

Az Ibtv. az elektronikus információs rendszerekben kezelt adatok esetében korlátozza a Magyarország területén kívüli kezelést és előírja, hogy a személyi hatály alá tartozó szervek – lásd fent 1. pont a)-j) alpontjai – és a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói – lásd fent 2. pont a) alpont – esetében az általuk kezelt, a nemzeti adatvagyon részét képező adatok csak Magyarország területén üzemeltetett elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek.[43] Ez a tiltó rendelkezés nem terjed ki a Magyar Honvédségre – lásd fent 1. pont k) alpontja –, mert a Magyar Honvédség feladatellátásából adódóan külföldön is dolgozik az adataival, elektronikus információs rendszereivel (pl.: NATO tagságból eredő kötelezettségek).

Az európai létfontosságú rendszerelem és a nemzeti létfontosságú rendszerelem[44] esetében az Ibtv. megengedő szabályozást tartalmaz arra az esetre, ha az elektronikus információs rendszerben kezelt adat nem a nemzeti adatvagyon részét képező adat. Ez esetben az elektronikus információs rendszer az Európai Unió tagállamai területén is üzemeltethető,[45] mivel a kizárólag Magyarország területén belül engedélyezett adatkezelés biztonsági és gazdasági szempontból sem indokolt. Az adatok Európai Unión belüli kezelésének kényszere elégséges korlátozás, az uniós és

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

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

40 A Forster Gyula Nemzeti Örökségvédelmi és Vagyongazdálkodási Központról szóló 199/2014. (VIII. 1.) Korm. rendelet 5. §-a.

41 A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (továbbiakban: Lrtv.).

42 Ibtv. 2. § (4) és (5) bekezdés

43 Ibtv. 3. § (1) bekezdés

44 Lrtv. 1. § c) és g) pont

45 Ibtv. 3. § (2) bekezdés

az uniós országok nemzeti szabályozása megfelelő védelmet és ellenőrizhetőséget biztosít. Abban az esetben, ha az európai létfontosságú rendszerelem és a nemzeti létfontosságú rendszerelem a nemzeti adatvagyon része, az adatkezelés csak Magyarországon történhet.

Az Ibtv. a személyi hatálya alá tartozó szervek – lásd fent 1. pont a)-j) alpontjai – 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.[46] 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 nem a Nemzeti Elektronikus Információvédelmi Hatóság, hanem a miniszter rendelet**é**ben meghatározott és hatósági feladatot ellátó szervezeti egység engedélyezi az Európai Unión belüli adatkezelést.

3.1.3. Az elektronikus információs rendszerek biztonsági osztályba sorolása és a szervezetek biztonsági szintjének meghatározása

Ahhoz, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszer vagy rendszerelem, és az ezekben kezelt adatok esetében a biztonsági kockázatokat meghatározni és értékelni, továbbá ehhez igazodva a kockázatokkal arányos védelmet meghatározni és biztosítani lehessen, a szervezetnek el kell végezni az elektronikus információs rendszer biztonsági osztályba sorolását.[47] Ennek elvégzése a szervezet vezetőjének a felelőssége. A biztonsági osztályba sorolást[48] a már említett rendszertulajdonságok, a bizalmasság és a sértetlenség, valamint a rendelkezésre állás alapján – minden egyes elektronikus információs rendszerre vonatkozóan – kell elvégezni, azzal a céllal, hogy a felmért kockázatok alapján az elektronikus információs rendszer védelmének elvárt erőssége meghatározásra kerüljön. Annak meghatározásához, hogy a biztonsági osztályba sorolás alkalmával mit kell kockázatnak tekintetni, az Ibtv. értelmező rendelkezései nyújtanak támpontot, ahol rögzítésre került: kockázat alatt a fenyegetettség mérték**ét kell azonosítani**, amely mérték egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.[49]

Az elvárt védelmi erősségnek mind a kockázatokkal (a kármértékkel), mind a ráfordított költségekkel arányosnak kell lennie, ezért szükséges annak megállapítása, hogy az adott elektronikus információs rendszer, illetve az abban kezelt adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának elvesztése egyenként milyen nagyságrendű károkat okozhat. A nagyságrend ismerete elégséges ahhoz, hogy a védelmi intézkedésekhez szükséges erőforrások költséghatékonyan meghatározhatóak legyenek, ugyanis a tételes költség meghatározás aránytalanul idő- és erőforrás igényes lenne.

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 azokat a külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket, melyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást és a biztonsági események kezelését.[50] Az arányosság elve alapján – és a költséghatékonyságot figyelembe véve – nem a szervezet egészénél egységesen, azonos biztonsági osztályba sorolva kell az elektronikus információs rendszerek védelmét megvalósítani, hanem a védelem rendszerenként eltérő lehet.

Az Ibtv. hatálya alá tartozó szervezetnek a biztonsági osztályba sorolást a bizalmasság, a sértetlenség vagy rendelkezésre állás kockázata alapján, minden egyes elektronikus információs rendszer esetében önbesorolás útján, 1-től 5-ig terjedő számozással ellátott skálán kell elvégezni azzal, hogy a számozás emelkedésével a védelmi előírások fokozatosan szigorodnak.[51] A biztonsági osztályokhoz és a védelmi intézkedésekhez tartozó technikai szabályokat az 5.3. pont („Technológia követelmények meghatározása") tartalmazza.

Az elektronikus információs rendszerek kezdő, alapállapotának rögzítéséhez a már működő elektronikus információs rendszerek biztonsági osztályba sorolását első alkalommal az Ibtv. hatálybalépését követő egy éven belül, 2014

46 Ibtv. 3. § (3) bekezdés
47 Ibtv. 1. § (1) bekezdés 11. pont és 7. § (1) bekezdés
48 Ibtv. 1. § (1) bekezdés 12. pont
49 Ibtv. 1. § (1) bekezdés 28. pont
50 Ibtv. 7. § (4) bekezdés
51 Ibtv. 7. § (2) bekezdés

július 1-ig kellett elvégezniük a szervezeteknek.[52] Az alapállapot és a kezdő intézkedések megtételéhez az egy éves átmeneti időszak – figyelemmel a kockázatértékelésre – megfelelő felkészülési időt biztosít.

2015. január 1-jétől lépett hatályba az a módosító rendelkezés, amely szerint az egy éves átmeneti időszak leteltével, 2014. július 1-jét követően az Ibtv. 2. § (1) bekezdésének hatálya alá tartozó szervek részére adatkezelést végző szervezetek esetében az adatkezelési tevékenység megkezdésének feltétele, hogy az adatkezelő a biztonsági osztályba sorolást elvégezze és az 5.2.1 pontban részletezett bejelentési kötelezettségét teljesítse.[53]

Ha a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóinak köre (lásd: 3.1.2 pont) jogszabály szerint kiegészül, a biztonsági osztályba sorolást az adatfeldolgozónak az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépését követő három hónapon belül kell elvégeznie azzal, hogy az 5.2.1 pont szerinti adatszolgáltatás határidejét az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől kell számítani.[54]

Ha jogerős kijelölő határozat alapján a létfontosságú rendszerelemek köre (lásd: 3.2 pont) kiegészül, a biztonsági osztályba sorolást a kijelölő határozat jogerőre emelkedését számított egy éven belül kell elvégezni azzal, hogy az 5.2.1 pont szerinti adatszolgáltatás határidejét a kijelölő határozat jogerőre emelkedésétől kell számítani.[55]

Fenti átmeneti szabályoktól függetlenűl fő szabályként érvényesül, hogy az alapállapot rögzítését követően a biztonsági osztályba sorolást legalább háromévenként kell elvégezni, azonban az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése, továbbá a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás esetén, soron kívüli felülvizsgálatot kell elvégezni.[56]

Alapvető elvárás, hogy az elektronikus információs rendszerek védelme ne egy statikus, adott időpillanatban rögzített állapot legyen, hanem a szervezet meghatározott időszakonként és keretek között, folyamatában figyelemmel kísérje a felmerült kockázatokat, ezért a biztonsági osztályba sorolás időszakosságának indoka a kockázatok folyamatos változása és az elektronikus információs rendszerek állapotváltozása, amely alapesetben feltételezhető. hogy folyamatos fejlődéssel jár. A fokozatosság elvét alapul véve az Ibtv. biztosítja a szervezetek számára, hogy az elvárt védelem erősségének eléréséhez szükséges biztonsági intézkedéseket az első vizsgálatkor megállapított biztonsági osztályt alapul véve lépésről lépésre érjék el, minden egyes következő, magasabb biztonsági osztályhoz rendelt biztonsági intézkedés kivitelezésére két év áll rendelkezésre a szervezetek számára.[57] Ha például egy szervezet az önbesorolás alapján elektronikus információs rendszerét 3. biztonsági osztályba sorolja 2015 májusában, azonban a reá irányadó érték az 5-ös, akkor a 4-es biztonsági osztály elérésére 2 év – 2017 májusáig –, az 5-ös szint és osztály elérésére további 2 év áll rendelkezésére – 2019 májusáig –, összesen tehát 4 év alatt kell a megfelelő biztonsági osztályt elérnie.

A biztonsági osztályba sorolás alkalmával fontos tényező, hogy az adott biztonsági osztály meghatározására és elérésére az elektronikus információs rendszer jelentőségével, állapotával arányosan kerüljön sor. Előfordulhatnak olyan esetek, amikor szükség van arra, hogy a védelmet magasabb – adott esetben alacsonyabb – szinten valósítsa meg a szervezet. Az Ibtv. lehetőséget biztosít a szervezet vezetőjének arra, hogy az irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthasson az elektronikus információs rendszerre vonatkozóan.[58] Ezen egyedi esetek körét – jellegüknél fogva – jogszabályi szinten nem indokolt rögzíteni, azonban megalapozottságukat ellenőrzés keretében az arra jogosult hatóság (Nemzeti Elektronikus Információbiztonsági Hatóság) ellenőrzi. A hatóság a szervezet által megállapított biztonsági osztályt felülbírálhatja és magasabb – indokolt esetben alacsonyabb – szintű biztonsági osztályba sorolást is megállapíthat.[59] Ez a felülbírálati jogosítvány nem vonatkozik a minősített adatokat kezelő elektronikus információs rendszerekre és bizonyos 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 elektronikus információs rendszerekre.[60]

A biztonsági osztályba sorolást dokumentált módon kell elvégezni, melyet a szervezet vezetője hagy jóvá, eredményét – azt, hogy az elektronikus információs rendszer melyik biztonsági osztályba kell, hogy tartozzon – a szervezet informatikai biztonsági szabályzatában kell rögzíteni.[61] Ha a biztonsági osztályba sorolás alkalmával a szervezet az adott elektronikus információs rendszerére vonatkozóan hiányosságot állapít meg, akkor a vizsgálatot követő 90

52 Ibtv. 26. §
53 Ibtv. 26. § (6) bekezdés a) pont
54 Ibtv. 26. § (6) bekezdés b) pont
55 Ibtv. 26. § (6) bekezdés c) pont
56 Ibtv. 8. § (1) és (2) bekezdés
57 Ibtv. 8. § (3) bekezdés
58 Ibtv. 7. § (5) bekezdés
59 Ibtv. 8. § (6) bekezdés
60 Ibtv. 2. § (3) és (4) bekezdés
61 Ibtv. 7. § (4) bekezdés és 8. § (1) és (4) bekezdés

napon belül cselekvési tervet kell készítenie, amely a hiányosságok megszüntetésére vonatkozó intézkedéseket tartalmazza.[62] (A szervezet vezetőjének felelősségére vonatkozó szabályokat a 6.1. pont tartalmazza.)

Az elektronikus információs rendszerek biztonsági osztályba sorolásával párhuzamosan, annak szabályrendszeréhez igazodva kell elvégezni a szervezet biztonsági szintjének a meghatározását is, amely a szervezet vezetőjének a felelőssége. Az Ibtv. hatálya alá tartozó szervezet biztonsági szintje alatt a szervezetnek azt a felkészültségét kell meghatározni, amely az Ibtv.-ben és végrehajtási rendeleteiben meghatározott biztonsági feladatok kezelésére vonatkozik,[63] azaz a szervezet elektronikus információs rendszereinek védelmét a bizalmasság és a sértetlenség, valamint a rendelkezésre állás alapján hogyan, a kockázatokkal mennyire arányosan és költséghatékonyan biztosítja.

A szervezet az elektronikus információs rendszerek védelmére való felkészültsége alapján – a biztonsági osztályba soroláshoz hasonlóan – önértékelés útján úgy köteles biztonsági szintjét megállapítani, hogy az a kockázatokkal arányos, költséghatékony védelem kialakítását szolgálja. Ennek érdekében az Ibtv. a hatálya alá tartozó szervek esetében rögzíti azt a minimum biztonsági szintet, amelyet a szervezetnek el kell érnie. Alapelvként egy adott szervezet biztonsági szintje azonos a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával, de az Ibtv. alapbiztonsági szintként:

a.) a Köztársasági Elnöki Hivatal, az Országgyűlés Hivatala, az Alkotmánybíróság Hivatala, az Alapvető Jogok Biztosának Hivatala, a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai és a hatósági igazgatási társulások esetén legalább a 2. biztonsági szintet,

b.) a központi államigazgatási szervek, a bírósági szervezetrendszer (Országos Bírósági Hivatal, Kúria, ítélőtábla, törvényszék, járásbíróság és kerületi bíróság, közigazgatási és munkaügyi bíróság), az ügyészségi szervezetrendszer (Legfőbb Ügyészség, fellebbviteli főügyészség, főügyészségek, járási ügyészségek), az Állami Számvevőszék, a Magyar Nemzeti Bank, a fővárosi és megyei kormányhivatalok esetén legalább a 3. biztonsági szintet,

c.) a Magyar Honvédség esetén legalább a 4. biztonsági szintet,

d.) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek esetén legalább az 5. biztonsági szintet határozza meg[64] (a biztonsági szintekhez tartozó szabályokat az 5.3. pont tartalmazza).

A szervezet biztonság szintjének azt a biztonsági szintet kell elérnie, amely megegyezik az általa kezelt elektronikus információs rendszerek közül a legmagasabb biztonsági osztállyal, de minimum az Ibtv.-ben előírt alap biztonsági szinttel.

Ha egy központi államigazgatási szerv olyan elektronikus információs rendszert kezel, melyben az információk bizalmassági besorolása 2., sértetlenségi besorolása 3., rendelkezésre állási besorolása 1., akkor a szervezeti biztonsági szintjét az alap biztonsági szint meghatározását figyelembe véve 3. szinten kell meghatároznia. Ha ennél a szervezetnél minden osztályba sorolási érték 2., a szervezeti biztonsági szintje akkor is 3., mivel ez 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 4. szinten kell meghatározni.

A szervezet biztonsági szintjének elérése a garancia arra, hogy a védelem elvárt erőssége és az információbiztonság a legmagasabb kockázatok alapján legyen meghatározva. A szervezet kezdő, alap biztonsági szintjének meghatározását első alkalommal az Ibtv. hatálybalépését követő egy éven belül kell megtenni.[65]

2015. január 1-jétől lépett hatályba az a módosító rendelkezés, amely az Ibtv. hatálybalépését követő egy éves, átmeneti időszak leteltéhez igazította az újonnan, jogelőd nélkül létrejött szervezetek biztonsági szintbe sorolásának kötelezettségét. E szabály szerint az Ibtv. 2. § (1) bekezdésében meghatározott, 2014. július 1-ét követően létrejött és jogelőddel nem rendelkező szervezeteknek a biztonsági szintbe sorolást a létesítést megalapozó döntés hatálybalépésétől számított egy éven belül kell elvégezni. Ez esetben az 5.2.1 pont szerinti adatszolgáltatás is a létesítést megalapozó döntés hatálybalépésétől számított határidők szerint kell teljesíteni.[66] Ilyen kötelezettségek teljesítése alá tartozó szervezet például a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal (vö.: 3.1.2. pontnál leírtak).

Az alapállapot rögzítését követően fő szabály szerint a biztonsági szint meghatározását – a biztonsági osztályba sorolással analóg módon – a meghatározott alap biztonsági szint elérését követően legalább háromévenként kell elvégezni, azonban az elektronikus információs rendszer biztonságát érintő változás esetén vagy új elektronikus információs rendszer bevezetésekor, soron kívüli felülvizsgálatot kell elvégezni.[67]

A szervezetek biztonsági szintbe sorolásánál is – hasonlóan a biztonsági osztályba soroláshoz – érvényesül a fokozatosság elve. Az adott szint elérése a szervezet feladat- és hatáskörének függvénye, ez biztosítja, hogy a biztonsági szint a szervezet feladatellátásával, az államigazgatási szervezetrendszerben elfoglalt helyével arányosan kerüljön kialakításra.

62 Ibtv. 8. § (5) bekezdés
63 Ibtv. 1. § (1) bekezdés 13. pont
64 Ibtv. 9. § (1) és (2) bekezdés
65 Ibtv. 26. §
66 Ibtv. 26. § (5) bekezdés a) pont
67 Ibtv. 10. § (5) és (6) bekezdés

Az alap biztonsági szint teljesítése során a szervezetnek lehetősége van arra, hogy az előírt alap biztonsági szintet lépésről lépésre érje el, minden egyes következő, magasabb biztonsági szint elérésére két év áll rendelkezésre.[68] Ha egy szervezet az önbesorolás alapján önmagát 2. biztonsági szintre sorolja 2015 májusában, azonban a reá irányadó alap biztonsági szint értéke a 4-es szint, akkor a 3-as szint elérésére 2 év – 2017 májusáig –, a 4-es szint elérésére további 2 év áll rendelkezésére – 2019 májusáig –, összesen tehát 4 év alatt kell a megfelelő biztonsági szintet elérnie. 2015. január 1-től változott az a korábbi kiegészítő szabály, hogy ha a szervezet biztonsági szintje az önbesorolás alapján az 1. biztonsági szintet nem éri el, az 1. biztonsági szint eléréséhez szükséges intézkedéseket a vizsgálatot követő egy éven belül meg kell tennie. 2015. január 1-től ez a határidő is az alapszabályhoz lett igazítva, így az 1. biztonsági szint eléréséhez – az önbesorolás elvégzését követően – két év áll a szervezet rendelkezésére.[69] Ez esetben egy 2015 májusában elvégzett felülvizsgálat esetén 2017 májusáig kell az 1. biztonsági szint eléréséhez szükséges intézkedéseket megtenni.

A szervezet jogállását és feladatkörének változásait figyelembe véve az Ibtv. lehetőséget biztosít a szervezet vezetőjének arra, hogy az irányadó biztonsági szintnél magasabb biztonsági szintet is megállapíthasson[70]. A hatóság a szervezet által megállapított biztonsági szintet felülbírálhatja és magasabb – indokolt esetben alacsonyabb – szintű biztonsági szintű besorolást is megállapíthat[71]. A minősített adatokat kezelő elektronikus információs rendszerek és bizonyos 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 elektronikus információs rendszerek esetében ez a felülbírálati jogosítvány az elektronikus információs rendszerek biztonságának felügyeletét és ellenőrzését ellátó ágazati szerv hatáskörében van.[72]

A biztonsági szint meghatározását – hasonlóan a biztonsági osztályba soroláshoz – dokumentált módon kell elvégezni, melyet a szervezet vezetője hagy jóvá, eredményét – azt, hogy a vizsgálat elvégzésekor a szervezet milyen biztonsági szintnek felel meg – a szervezet informatikai biztonsági szabályzatában kell rögzíteni.[73] Ha a biztonsági szint meghatározása alkalmával megállapításra kerül, hogy a szervezet biztonsági szintje alacsonyabb az előírt alap biztonsági szintnél, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie, amely az előírt alap biztonsági szint eléréséhez szükséges intézkedéseket tartalmazza. 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.[74]

Érzékelhető, hogy az elektronikus információs rendszerek biztonsági osztályba sorolása és a szervezet biztonsági szintjének meghatározása együtt mozog, a biztonsági osztály kihatással van a biztonsági szint meghatározására.

3.2. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

Az Ibtv. rendelkezéseihez szorosan kapcsolódó törvényi szabályozást *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény* (továbbiakban: Lrtv.) tartalmaz, mivel az Ibtv. tárgyi hatálya kiterjed az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé (a továbbiakban: létfontosságú rendszerelem) törvény alapján kijelölt rendszerelemekre is. Magyarországon is vannak olyan infrastruktúrák, amelyek megzavarása vagy megsemmisítése befolyásolná az állam, a gazdaság és a társadalom mindennapi működését, akár úgy, hogy annak határokon átnyúló hatása is lesz.

Az Lrtv. alapvető célja a veszélyeztetett létfontosságú rendszerek és létesítmények azonosítására és kijelölésükre vonatkozó alapszabályok rögzítése. A *2008/114/EK irányelv*[75] által használt terminológiához igazodva az Lrtv. szerint létfontosságú rendszerelem:

a.) az energetikai,
b.) a közlekedési,
c.) az agrárgazdasági,
d.) az egészségügyi,
e.) a pénzügyi,

68 Ibtv. 10. § (4) bekezdés
69 Ibtv. 10. § (3) bekezdés
70 Ibtv. 9. § (3) bekezdés
71 Ibtv. 9. § (4) bekezdés
72 Ibtv. 9. § (4) bekezdés
73 Ibtv. 10. § (1) bekezdés és 10. § (8) bekezdés
74 Ibtv. 10. § (2) és (7) bekezdés
75 Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK tanácsi irányelv.

f.) az ipari,
g.) az infokommunikációs,
h.) a vízügyi,
i.) a kormányzati (ideértve a jogrendet is),
j.) a közbiztonsági

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.[76]

Az Lrtv. az értelmező rendelkezések között a létfontosságú társadalmi feladatok ellátását példálózó jelleggel határozza meg, ide tartozónak tekinti különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához tartozó rendszerelemeket. Alapvetően létfontosságúnak kell tekinteni minden olyan rendszert, rendszerelemet vagy létesítményt, amely kiemelkedő fontosságú a lakosság ellátása és a társadalom zavartalan működésének fenntarthatósága szempontjából, ugyanakkor sebezhetősége okán nem áll rendelkezésre olyan helyettesítő eszköz, amely kiesése esetén pótolhatja annak működését. Az ágazatokon belüli, ún. alágazatokra vonatkozó felosztást az Lrtv. 1-3. melléklete tartalmazza.

A létfontosságú rendszerelem fogalmához igazodóan, az egyértelmű elhatárolás és a gyakorlati alkalmazhatóság szempontjából az Lrtv. rögzíti, hogy mit kell európai és nemzeti létfontosságú rendszerelemnek tekinteni. E szerint a törvényben előírtak alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése:

a.) jelentős hatással lenne legalább két EGT-államra – ez esetben az egyes ágazatokon átnyúló kölcsönös függőségből következő hatásokat is figyelembe kell venni – európai létfontosságú rendszerelemnek,
b.) a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatása lenne Magyarországon nemzeti létfontosságú rendszerelemnek minősül[77].

A nemzeti létfontosságú rendszerelemmé történő kijelölés tagállami (nemzeti) hatáskör, amely alapján az egyes ágazatok esetében nemzeti létfontosságú rendszerelemmé történő kijelölést (vagy annak visszavonását) – az azonosítási eljárás lefolytatása után – az üzemeltető vagy a javaslattevő hatóság azonosítási jelentés benyújtásával kezdeményezheti az ágazati kijelölő hatóságnál.[78] Az ágazati kijelölő hatóság eljárása *a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény* (továbbiakban: Ket.) rendelkezései szerinti hatósági eljárásnak minősül, amely során az ágazati kijelölő hatóság az ún. ágazati és horizontális kritériumok alapján határozathozatallal dönt a nemzeti létfontosságú rendszerelem kijelöléséről vagy annak visszavonásáról.

Ágazati kritériumok azok a szempontok és az ezekhez tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek alapján egy eszköz, létesítmény rendszereleme megzavarásának, vagy megsemmisítésének hatása meghatározható, a hatások ismeretében az eszköz, a létesítmény, a rendszer vagy azok része létfontosságú rendszerelemmé jelölhető és ágazati besorolása meghatározható. Az ágazati kritériumok meghatározásáról az egyes ágazati jogszabályok rendelkeznek (pl.: *az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet*).

Horizontális kritériumok esetén az eszköz, létesítmény rendszerelemének azon tulajdonságai és azok a szempontok kerülnek meghatározásra, amelyek figyelemmel vannak a bekövetkező emberiélet-veszteségekre, a gazdasági és társadalmi hatásokra, az egészségre, a természetre, az épített környezetre gyakorolt hatásokra és létfontosságú rendszerelemmé történő kijelölésük független az ágazati besorolástól. A horizontális kritériumok meghatározásáról külön jogszabály rendelkezik.[79]

A hatósági döntés során meghatározásra kerül az a határidő, amely időpontig az üzemeltetőnek biztonsági tervet kell kidolgoznia és rögzítésre kerülnek a létfontosságú rendszerelem védelmével[80] összefüggő, a rendszerelem egyedi sajátosságaihoz, környezetéhez, a veszély mértékéhez igazodó feltételek.[81]

A nemzeti létfontosságú rendszerelemmé történő kijelölés tagállami hatáskörével ellentétben az európai létfontosságú rendszerelemek kijelölése (a kijelölés visszavonása) nem nemzeti hatáskör, a kijelölési folyamat vagy Magyarországon belül, az üzemeltető vagy a javaslattevő hatóság kérelmére, vagy pedig valamely EGT-állam kezdeményezésére

76 Lrtv. 1. § f) pont és 1-3. mellékletei
77 Lrtv. 1. § c) és g) pont
78 Lrtv. 2. § (1) bekezdés
79 A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. vhr.).
80 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; - Lrtv. 1. § e) pont.
81 Lrtv. 1. § a) és d) pontok, 2. § (3) bekezdés

indulhat meg. A kijelölés nem hatósági eljárás, legalább kettő tagállam együttműködését, megállapodását és nemzetközi szerződés megkötését igényli. A nemzetközi szerződés hatálybalépésétől számított 30 napon belül az ágazati kijelölő hatóság az európai létfontosságú rendszerelemmé történő kijelölésről határozatot hoz, amely határozatban a nemzetközi szerződésben foglaltak alapján rögzíteni kell az üzemeltető számon kérhető kötelezettségeit, azok végrehajtásának határidejét és ellenőrzését.[82] Az európai létfontosságú rendszerelemek esetében az Lrtv. a Kormány részére – kötelező adattartalommal – éves jelentéstételi kötelezettséget ír elő az Európai Bizottság irányába.[83]

A kijelölő hatóság határozata alapján – mind a nemzeti és mind az európai létfontosságú rendszerelemek esetében – az üzemeltetőnek – a felmerülő költségek viselésével egyetemben – kötelezettsége van arra nézve,[84] hogy:

a.) a határozatban meghatározott, de minimum annak közlésétől számított 60 napon belül kidolgozza az üzemeltetői biztonsági tervet (továbbiakban: biztonsági terv) és megküldje a nyilvántartó hatóságnak és az ágazati kijelölő hatóságnak;

b.) a rendszerelem védelmét és folyamatos működését a biztonsági tervvel összhangban szervezze meg.

A kijelölő határozatban rögzített tartalmi és formai követelmények szerint a biztonsági tervben tételesen fel kell sorolnia az üzemeltetőnek a létfontosságú rendszerelemeket. Az egyes rendszerelemekhez igazodva rögzíteni[85] kell:

a.) a szervezeti és eszközrendszert és azokat a biztonsági intézkedéseket, amelyek a rendszerelemek védelmét biztosítják,

b.) a különböző kockázati és veszélyszinteknek megfelelően meg kell határozni azokat az ideiglenes intézkedéseket is, amelyek megtétele szükséges a védelem biztosításához,

c.) a védelmet szolgáló meglévő vagy kialakítás alatt álló biztonsági megoldásokkal kapcsolatos eljárásokat.

A biztonsági terv helyettesíthető az üzemeltető által korábban elkészített biztonsági dokumentummal, ha az az a)–c) pont szerinti tartalmi elemeket magában foglalja és a helyettesítésről a kijelölő határozatban az ágazati kijelölő hatóság rendelkezett.[86]

Az üzemeltető további kötelezettsége, hogy a kijelölési eljárásban részt vevő hatóságokkal, szakhatóságokkal való kapcsolattartás céljából kijelölje az adott ágazatnak megfelelő szakirányú végzettséggel rendelkező biztonsági összekötő személyt, gondoskodjon foglalkoztatásáról és folyamatosan biztosítsa a tevékenysége ellátásához szükséges feltételeket.[87]

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatósága[88] (továbbiakban: BM OKF), mint ellenőrzést koordináló szerv köteles az európai létfontosságú rendszerelemet vagy a nemzeti létfontosságú rendszerelemet rendszeresen ellenőrizni. További feladata a hatósági ellenőrzések koordinálása. A BM OKF e feladatkörében eljárva ellátja a védelemmel kapcsolatos hálózatbiztonsági intézkedések koordinációját, a hálózatbiztonsággal kapcsolatos események elemzését, értékelését is. A helyszíni ellenőrzést lefolytató szervként **külön jogszabályban** kijelölt szerv[89] számára az Lrtv. kötelezettségként írja elő, hogy az európai létfontosságú rendszerelemet vagy a nemzeti létfontosságú rendszerelemet legalább kétévenként helyszíni ellenőrzéssel – a nemzetbiztonsági szempontok figyelembevételével – kell vizsgálni. Az időszakos ellenőrzések alapvető célja, hogy a biztonsági terv avulását megelőzve a védelmi képességek fenntarthatóságát az ellenőrző szerv nyomon kövesse.

Az ágazati kijelölő hatóság az üzemeltető kötelezettségszegése esetén – a fokozatosság elvét szem előtt tartva – határozatban:

a.) felszólítja az üzemeltetőt a kötelezettségek betartására,

b.) kötelezi az üzemeltetőt a biztonsági terv módosítására vagy új biztonsági terv készítésére,

c.) 100 ezer forinttól 3 millió forintig terjedő bírságot szab ki.[90]

Az Lrtv. az energetika, mint speciális ágazati sajátosságokkal rendelkező szektor esetében különleges szabályokat állapít meg a villamosenergia-rendszer, a kőolajipar és a földgázipar tekintetében azzal, hogy az energetikai létesítmény alkotórészének kell tekinteni a létesítmény működését alapvetően befolyásoló technológiai hírközlési és informatikai rendszert is, továbbá az ágazati és horizontális kritériumokat a kijelölés során azzal az eltéréssel kell alkalmazni, hogy

82 Lrtv. 3. §
83 Lrtv. 13. §
84 Lrtv. 6. § (1) és (3) bekezdés, valamint 7. §-a
85 Lrtv. 6. § (2) és (3) bekezdés, valamint Lrtv. vhr. 6. §-a.
86 Lrtv. 6. § (4) bekezdés
87 Lrtv. 6. § (7) bekezdés
88 A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet 2. § (1) bekezdés és az Lrtv. 8. §-a.
89 Vízügyi ágazat tekintetében a vízügyi igazgatóság (541/2013. (XII.30.) Korm. rendelet), agrárgazdasági ágazat tekintetében a Nemzeti Élelmiszerlánc-biztonsági Hivatal (540/2013. (XII.30.) Korm. rendelet).
90 Lrtv. 9. §-a és a Lrtv. vhr. 9. §-a

a létfontosságú rendszer, létesítmény vagy eszköz alatt kizárólag a rendszerelemet kell érteni. További eltérés, hogy az üzemeltető feladata, hogy a kijelölést követő 5 évente az azonosítási eljárást lefolytassa, és azonosítási jelentést nyújtson be az ágazati kijelölő hatóságnak. Mulasztás esetén az ágazati kijelölő hatóság bírságolhat, vagy a kijelölést kezdeményezheti. Az azonosítási jelentés alapján az ágazati kijelölő hatóság az üzemeltető döntését jóváhagyja és az azonosított rendszerelemeket nemzeti létfontosságú rendszerelemnek minősíti, vagy elfogadja, hogy az üzemeltető egyetlen rendszerelemet sem azonosított nemzeti létfontosságú rendszerelemként, illetve új azonosítási jelentés benyújtását írja elő. E szabály szerint európai létfontosságú rendszerelemnek történő kijelölési eljárás csak akkor indul meg, ha az azonosítási jelentés erre is kiterjed, vagy ha azt EGT-állam kezdeményezte.[91]

3.3. Kapcsolódó törvényi rendelkezések

Az Lrtv. mellett szükséges további, kapcsolódó törvényi rendelkezések ismertetése is, annak érdekében, hogy az Ibtv. speciális szabályozási környezetét komplex módon értelmezni lehessen. A következőkben a főbb törvényi szabályozások kerülnek bemutatásra.

3.3.1. A minősített adat védelméről szóló 2009. évi CLV. törvény

Az állam sajátos szerepvállalásából adódóan (honvédelmi, rendvédelmi feladatok ellátása, igazságszolgáltatás, közigazgatás megszervezése stb.), kiemelt figyelmet kell fordítani az állam működése során keletkezett adatok kezelésére, megőrzésére, jogosultság szerinti megismerésére. A *minősített adat védelméről szóló 2009. évi CLV. törvény* (továbbiakban: Mavtv.) szabályozza:

a.) a minősített adatok jelölését („Korlátozott terjesztésű!," „Bizalmas!," „Titkos!," „Szigorúan titkos!" minősítés), a minősített adatok kezelésének, védelmének, a minősítési eljárásnak a rendjét,
b.) az adat minősítésének fokától függően az adminisztratív és fizikai intézkedéseket (melyek kármértékhez igazodnak),
c.) a minősített adat megismerésére, kezelésére vonatkozó jogosultságokat és feltételeket,
d.) a minősített adatok 5 évenkénti felülvizsgálatát,
e.) a minősítés időtartamát, azt 10, 20, 30 évben állapítja meg (pl. a „Szigorúan titkos!" és „Titkos!" minősítési szintű adat esetén legfeljebb 30 év), amely meghatározott esetekben[92] hosszabbítható,
f.) a minősítésre jogosultak körét[93] (pl.: a köztársasági elnök, az Országgyűlés elnöke, a Kormány tagja, a Miniszterelnökséget vezető államtitkár, a kormánybiztos, a miniszterelnöki biztos, a Nemzeti Biztonsági Felügyelet vezetője stb.), és a minősítési jogkör delegálásának jogát,
g.) a minősített adat elektronikus információs rendszerben történő kezelésének feltételeit (előzetes engedélyhez köti), rögzíti továbbá a kezeléshez igénybe vett technikai eszközökkel szemben támasztott követelményeket, és ezek érvényesülése érdekében kijelöli az ellenőrzésére jogosult hatóságot (Nemzeti Biztonsági Felügyelet).

Az Ibtv.-t a minősített adatokat kezelő elektronikus információs rendszereket érintően a Mavtv.-ben meghatározott eltérésekkel kell alkalmazni, amelynek gyakorlati kezeléséhez az Ibtv. a módosító rendelkezések között 2013. július 1-jével módosította a Mavtv.-t. (10. § (4) bekezdés). A módosítás eredményeképpen minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges és az adat minősítési szintjének megfelelő biztonsági feltételeket az alábbiak szerint:

a.) a minősített adat védelméhez szükséges és a minősítési szintnek megfelelő Mavtv. és végrehajtási rendeletei szerinti személyi, fizikai és adminisztratív védelmet, illetve
b.) ha a minősített adat elektronikus információs rendszeren van kezelve, akkor 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 védelm**et.

91 Lrtv. 10-12. §-ok
92 Mavtv. 5. §
93 Mavtv. 4. §

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

Az adatok védelme terén kiemelt jelentőségű szabályozás a *nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény* (továbbiakban: Adatvagyon tv.), melynek célja:

a.) a közigazgatás működésének folyamatos biztosítása,

b.) a nemzeti adatvagyon[94] körébe tartozó nyilvántartások biztonságának megteremtése, ezen nyilvántartások jogszerű felhasználását akadályozó cselekmények bűncselekménnyé nyilvánításával azok megelőzése (lásd bővebben a 6.2. pont alatt).

Az Adatvagyon tv. alapján *„a nemzeti adatvagyon részét képező adatállomány tekintetében törvény az adatfeldolgozással megbízható személyek és szervezetek körét korlátozhatja, az vagy az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja."*[95] Az Adatvagyon tv. végrehajtási rendelete[96] (lásd bővebben a 3.1.2. pont alatt) rögzíti a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóinak körét, az adatfeldolgozó igénybevételének jellegét (kötelező vagy az adatkezelő döntésétől függ).

3.3.3. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

Az adatbiztonság és az adatok védelmére vonatkozó kötelezettség alapelvként jelenik meg *az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben* (továbbiakban: Infotv.). Az Infotv. az alapjogszabály, amely az adatot tekinti védett jogi tárgynak. Ehhez igazodva rendelkezései biztosítják a személyes adatok védelmét, a közérdekű adatok nyilvánosságát, rögzítik az adatkezelés során az adatbiztonsági előírásokat, és a célhoz kötöttség elvének alapul vételével az adatok kezelésének jogszerűségét és az állampolgári jogok érvényesülését. Az Infotv. alapelveihez igazodóan az elektronikus információs rendszerben kezelt adatok védelmének speciális szabályait az Ibtv. tartalmazza.

3.3.4. Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény

Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény (továbbiakban: Interop. tv.) 2015. január 1-jén lépett volna hatályba, azonban a központi címregiszter létrehozásával összefüggő, valamint egyes igazgatási tárgyú törvények módosításáról szóló 2014. évi XCIII. törvény[97] lépcsőzetes hatálybaléptetést vezetett be. Az Interop. tv megalkotásának célja azon jogszabályi környezet kialakítása, amely által az eltérő állami adatbázisokban kezelt adatok felhasználása egycsatornássá válhat, a hatósági eljárások és az adatigénylések egyszerűsíthetőek. Az Interop. tv. rögzíti, hogy alkalmazásakor a személyes adatok kezelésére vonatkozó jogszabályi előírásokat betartva kell eljárni, és rendelkezéseit egyes állami és önkormányzati nyilvántartások esetében nem kell alkalmazni (pl.: nemzetbiztonsági szolgálatok, a közfeladatot ellátó szervek belső nyilvántartásai stb.)[98].

A nyilvántartások, az abban kezelt adatok védelme érdekében a nyilvántartónak az Ibtv. szerinti elektronikus információs rendszerben kell vezetnie a nyilvántartást, és automatikus adatátvétel, vagy automatikus adatelérési felület útján lehetővé kell tennie a nyilvántartások közötti adatkapcsolat-szolgáltatást.[99] Ehhez kapcsolódóan az Interop. tv. végrehajtási rendelete fogja kijelölni azokat a nyilvántartásokat, amelyek esetében kötelező biztosítani az automatikus adatelérési felületen történő adatátadást.[100]

Az Interop. tv. alapján a nyilvántartónak[101]:

94 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 (a továbbiakban. Adatvagyon tv.) 1. § 1. pont.

95 Adatvagyon tv. 2. § (1) bekezdés

96 A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet.

97 A központi címregiszter létrehozásával összefüggő, valamint egyes igazgatási tárgyú törvények módosításáról szóló 2014. évi XCIII. törvény 53. § (2) bekezdése.

98 Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény(a továbbiakban: Interop. tv.) 1. §-a

99 Adatkapcsolat-szolgáltatás: olyan szolgáltatás, amelynek keretében a nyilvántartó adatokat ad át egy másik nyilvántartónak, ami az adatokat e törvényben meghatározott egyszerű adatátvétel vagy automatikus adatátvétel útján veszi át. Interop. tv. 2. § 3. pont és 3 §

100 Interop. tv. 16. § (1) bekezdés 6. pont

101 Interop. tv. 7. §

a.) adatkapcsolat-szolgáltatási szabályzatot (továbbiakban: szabályzat) kell kiadnia, azt folyamatosan kell aktualizálnia, és be kell jelentenie a nyilvántartások felügyeletéért felelős szervnek, ezen felül
b.) az adatkapcsolat-szolgáltatások igénybevételére vonatkozóan adatkapcsolat-szolgáltatási megállapodást kell kötnie, melyet a Nemzeti Elektronikus Információbiztonsági Hatóság hagy jóvá, és az adatkapcsolat-szolgáltatás csak a jóváhagyást követően nyújtható a szolgáltatást igénybevevők részére.

A nyilvántartások felügyeletéért felelős szerv információbiztonságot érintő kérdésekben feladatainak végrehajtásába a Nemzeti Elektronikus Információbiztonsági Hatóságot köteles bevonni.[102]

102 Interop. tv. 8. § (6) bekezdés

4. Az elektronikus információbiztonság szervezetrendszere

Az Ibtv. az elektronikus információbiztonság szervezetrendszerének kialakítására vonatkozó főbb rendelkezéseket tartalmazza, azzal, hogy a szervezetek működtetésére vonatkozó részletszabályok megalkotását a felhatalmazó rendelkezésekkel végrehajtási (rendeleti) szintre utalja. Az Ibtv. 24. §-a felhatalmazást ad a Kormánynak arra, hogy rendeletben jelölje ki az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságot, valamint rendelet útján határozza meg:

a.) az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság:
  – feladatának részletes szabályait,
  – hatósági ellenőrzése lefolytatásának részletes eljárási szabályait,
  – által kiszabható bírság mértékét, a bírság kiszabásának és befizetésének részletes eljárási szabályait,
b.) az információbiztonsági felügyelő kirendelésének szabályait, feladatkörét és eljárásának rendjét,
c.) a Nemzeti Biztonsági Felügyelet szakhatósági feladat- és hatáskörét,
d.) a kormányzati eseménykezelő központ és az ágazati eseménykezelő központok feladat- és hatáskörét,
e.) a Nemzeti Kiberbiztonsági Koordinációs Tanács, a Nemzeti Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokat, feladat- és hatáskörüket.

Az Ibtv. hatályának kiterjesztése során elkülönített, rendészeti, honvédelmi, nemzetbiztonsági, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerek[103] és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró, vagy törvényi felhatalmazás alapján speciális feladatokat ellátó információs rendszerek esetében felhatalmazást kap az irányítási feladatokat gyakorló miniszter, hogy rendeletben szabályozza a hatósági (szakhatósági) feladatok ellátását [Ibtv. 24. § (3) bekezdés]. Ennek megfelelően:

a.) a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat, továbbá a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a honvédelemért felelős miniszter,
b.) a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek esetében a rendvédelmi szervet irányító miniszter,
c.) a diplomáciai információs célokra használt rendszer esetében a külpolitikáért felelős miniszter,
d.) a Nemzeti Adó- és Vámhivatal esetében az adópolitikáért felelős miniszter,
e.) az Információs Hivatal esetében a Kormány polgári hírszerzési tevékenység irányításáért felelős tagja,
f.) a médiaszolgáltatási és az elektronikus hírközlési tevékenység esetében a Nemzeti Média- és Hírközlési Hatóság elnöke,
g.) a minősített adatokat kezelő elektronikus információs rendszerek esetében a minősített adatok védelmének szakmai felügyeletéért felelős miniszter,

hogy az irányítása alatt álló szervezet által működtetett elektronikus információs rendszer biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokat rendeletben határozza meg. Ezek további szabályait az 5. fejezet tartalmazza.

A következőkben az egyes szervezetek jogállását, irányítását és a szervezetrendszerben betöltött szerepét és főbb feladataikat tárgyaljuk.

4.1. Kormányzati koordináció[104]

A Kiberstratégia és az Ibtv. rendelkezései alapján a Kormány javaslattevő, véleményező szerveként, a kiberbiztonság kormányzati koordinációja érdekében a kormányzati tevékenység összehangolásáért felelős miniszter elnökletével létrehozásra került a Nemzeti Kiberbiztonsági Koordinációs Tanács (továbbiakban: Tanács). A Tanácson belül folytatja tevékenységét a kormányzati tevékenység összehangolásáért felelős miniszter által delegált kiberkoordinátor is, aki egyben az elnök általános helyettese.

103 Ibtv. 1. § (1) bekezdés 47. pont

104 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.

A Tanács feladata, hogy a kiberbiztonság[105] területén:

a.) összehangolja az Ibtv. hatálya alá tartozó szervezetek együttműködését;
b.) elősegítse a szabályozást, valamint az ágazati munkacsoportok munkáját;
c.) támogassa a Nemzeti Kiberbiztonsági Fórum munkáját;
d.) támogassa a források hatékony felhasználását;
e.) a Kiberstratégiában meghatározott cselekvési területeken a kormányzati tevékenység koordinációját elősegítse és figyelemmel kísérje a végrehajtást, erről jelentést tegyen a Nemzetbiztonsági Kabinetnek;
f.) a Kiberstartégia cselekvési területeihez társított kormányzati intézkedéseket, ún. Nemzeti Kiberbiztonsági Akciótervet – melynek elfogadásáról a Kormány dönt – készítsen – a Fórum javaslatainak és véleményének figyelembevételével – és azt évente felülvizsgálja;
g.) elősegítse az egységes magyar kormányzati álláspont kialakítását és hozzájáruljon Magyarország nemzetközi politikai képviseletéhez.[106]

A Tanács tagja a miniszterek által delegált 1 fő állami vezető, és a kiberkoordinátor. Az elnök felkérésére 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 munkájában.

A Tanács feladatai ellátásához igazodva, de legalább félévente ülésezik. Tevékenységéről az elnök – legalább félévente – a miniszterelnöknek tartozik beszámolási kötelezettséggel. A Tanács a kibertámadások kezelése és az elektronikus információbiztonság területén rendelkezik azzal a jogosítvánnyal, hogy az e területen alkalmazandó legjobb gyakorlatokról a munkacsoportok javaslatára ajánlásokat adjon ki, melyek jellegükből adódóan azonban jogi kötelező erővel nem rendelkeznek.

A Tanács munkáját javaslattételi joggal és véleményezési lehetőséggel az általa felkért szakmai, illetve nem kormányzati gazdasági vezetőkből álló Nemzeti Kiberbiztonsági Fórum segíti, amelynek vezetését az elnök, munkájának szakmai koordinálását a kiberkoordinátor látja el. A Fórum feladatai ellátásához igazodva, de legalább félévente ülésezik.

A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik. A munkacsoportok egyes szakterületekhez igazodva kerültek létrehozásra, kötelező jelleggel az eseménykezelés, a belbiztonság, az e-közigazgatás, az energetika, és a gyermekvédelem területén, de a Tanács felkérésére további munkacsoportok is létrehozhatóak. Ezen munkacsoportok tagja a kiberkoordinátor, és az általa felkért állami szervek által delegált közszolgálati tisztviselők, valamint a kiberkoordinátor által felkért nem kormányzati szakértő. A munkacsoportok a feladataik ellátásához igazodva, de legalább félévente tartanak ülést.

A Tanács felépítéséből adódóan, különböző szinteken más-más szempontok figyelembevételével képes áttekinteni az elektronikus információs rendszerek biztonságával, a létfontosságú rendszerelemek védelmével, és a kibervédelemmel kapcsolatos feladatokat.

4.2. Hatóság és szakhatóság

h.) Az Ibtv. rendelkezik arról, hogy a hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét a Kormány által kijelölt hatósága (továbbiakban: Hatóság) látja el[107]. A Hatóság feladata:

a.) az elektronikus információs rendszerek biztonsági osztályba sorolásának és a szervezet biztonsági szintje meghatározásának hatósági ellenőrzése és szükség esetén a megállapított biztonsági osztály és biztonsági szint felülbírálata;
b.) az elektronikus információs rendszert veszélyeztető informatikai állapot észlelése esetén szankcionálás, ennek keretében információbiztonsági felügyelő kirendelése vagy bírságolás;
c.) az információbiztonsággal kapcsolatos nyilvántartások vezetése;
d.) az elektronikus információs rendszer Európai Unió tagállamaiban történő üzemeltetésének engedélyezése és az Európai Unión kívüli üzemeltetés ellenőrzése;

105 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. - Ibtv. 1. § (1) bekezdés 26. pont.

106 Ibtv. 21. § (2) bekezdés

107 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 2. §-a

e.) információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülésének ellenőrzése;
f.) az azonnali reagálás érdekében incidenskezelési munkacsoport működtetése;
g.) tevékenységéről éves jelentés keretében beszámolni a Tanács részére;
h.) a jelentős kihatással bíró kiberbiztonsági eseményről eseti jelentést készíteni a Tanács részére;
i.) együttműködés az elektronikus információbiztonság területén működő szervekkel (GovCert, ágazati CERT-ek, szakhatóság).

A Hatóság közigazgatási szervek esetében – határozott időtartamra s – a belügyminiszternél, mint az e-közigazgatásért felelős miniszternél kezdeményezheti információbiztonsági felügyelő kirendelését az adott szervezethez. Az információbiztonsági felügyelő jogosult a szervezet által meghozott védelmi intézkedéseket véleményezni, adott esetben az intézkedéssel szemben kifogással élhet, pénzügyi kötelezettségvállalásra azonban nem jogosult. A fenyegetés elhárítása érdekében intézkedéseket, eljárásokat javasolhat a szervezet részére, és feladatellátásával összefüggésben tájékoztatást, adatszolgáltatást kérhet, dokumentumokba betekinthet. A kirendelés indokolt esetben legfeljebb egy alkalommal a folyamatban lévő intézkedések lezárásáig meghosszabbítható.

A Hatóság által működtetett kormányzati információtechnológiai és hálózatbiztonsági információ-megosztási incidens-kezelési munkacsoport (továbbiakban: incidens-kezelési munkacsoport) 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 Nemzeti Biztonsági Felügyelet (továbbiakban: NBF), mint szakhatóság a Ket. szerint – igazgatási szolgáltatási díj ellenében – közreműködik a biztonsági osztályba sorolás és a biztonsági szint meghatározására, a Hatósághoz érkező bejelentések kivizsgálására vonatkozó hatósági eljárásban, valamint a Hatóság éves ellenőrzési terv alapján végzett ellenőrző tevékenységében. Az NBF látja el az Ibtv. hatálya alá tartozó szervezetek esetében az elektronikus információs rendszerek, rendszerelemek sérülékenység-vizsgálatát, amely vizsgálatot a szervezet felkérésére a Hatóság eljárásától függetlenül is elvégezheti. A vizsgálat alapvető célja, hogy már a biztonsági esemény bekövetkezését megelőzően feltárja az elektronikus információs rendszer esetleges sérülékenységeit, a védelem hiányosságait. Az NBF ellátja továbbá a biztonsági események adatainak műszaki vizsgálatát is, melyet a Hatóság megkeresése vagy egyedi esetben felkérésre végez el.

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.

4.3. Eseménykezelő központok

4.3.1. A kormányzati eseménykezelő központ és az ágazati eseménykezelő központok[108]

Az Ibtv. szerinti kormányzati eseménykezelő központ feladatait ellátó szervezet *az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet* alapján már korábban is létezett. A hatályos rendelkezések szerint az Ibtv.-ben rögzített biztonsági események kezelését a belügyminiszter irányítása alá tartozó Nemzetbiztonsági Szakszolgálat keretén belül működő kormányzati eseménykezelő központ [Számítógépes Vészhelyzeti Reagáló Egység – Computer Emergency Response Team, (a továbbiakban: GovCert)] látja el. A GovCert az eseménykezelési feladatokat az Ibtv. szervi hatálya alá tartozó szervek esetében (lásd. 3.1.2. pont) látja el.

Az eseménykezelő központok feladatai:
a.) folyamatosan elérhető 24 órás ügyelet működtetése;
b.) a bejelentett biztonsági események fogadása, kivizsgálása és kezelése, műszaki vizsgálatok elvégzése, és ennek keretében a biztonsági események elhárításának koordinálása;
c.) napi rendszerességgel hálózatbiztonsági helyzetértékelések elvégzése;
d.) biztonsági események adatainak gyűjtése, melyhez hozzátartozik az is, hogy az adatgyűjtés eredményeként a tudomására jutott sérülékenységekről, a biztonsági esemény bekövetkezésének veszélyéről vagy annak fennállásáról, valamint a javasolt intézkedésekről – személyes adatokat nem tartalmazó – nyilvántartást vezetnek;
e.) a biztonsági eseményekről negyedévente jelentés készítése a Tanács részére;
f.) a hazai és nemzetközi információbiztonsági irányokról elemzések és jelentések készítése a Tanács részére;

108 Ibtv. 19.-20. §-ok

g.) a nemzetközileg publikált sérülékenységek és a kritikus hálózatbiztonsági eseményekről magyar nyelvű azonnali figyelmeztetések közzététele a honlapon, és emellett tájékoztatás a tudomásukra jutott sérülékenységekről;
h.) együttműködés az informatikai és hálózatbiztonsági védelemben érintett magyar nemzetbiztonsági szolgálatokkal és bűnüldöző szervekkel, iparági szereplőkkel,
i.) részvétel az infokommunikációs biztonságra vonatkozó stratégiák és ágazati szabályozások előkészítésében,
j.) 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. Az eseménykezelő központok együttműködnek a Hatósággal és az NBF-fel.

Az Ibtv. rendelkezései szerint több ágazati eseménykezelő központ is létrehozható, melynek indoka, hogy egyes speciális szakterületi sajátosságokhoz igazodóan kerüljenek létrehozásra azok a reagáló egységek, melyek az ágazatok egyedi jellemzői alapján képesek a biztonsági események kezelésére. 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 esetében (lásd. Ibtv. 2. § (4) bekezdés), valamint a Nemzeti Média- és Hírközlési Hatóság **és** a Magyar Energetikai és Közműszabályozási Hivatal, mint önálló szabályozó szervek esetében kerülhet sor, azzal hogy részükre előírásra került, hogy a biztonsági események adatait kötelesek haladéktalanul a GovCert részére továbbítani.

Magyarországot nemzetközi színtéren, a kormányzati eseménykezelő központok nemzetközi együttműködésében az európai kormányzati eseménykezelő csoport által akkreditált CERT képviseli. Ez jelenleg a GovCert. Az ágazati eseménykezelő központok részére lehetőség van arra, hogy a fenntartó döntése alapján akkreditáltassák magukat és ezáltal a nemzetközi együttműködésben részt vegyenek.

Az eseménykezelő központok hatáskörébe tartozó fent rögzített feladatokon 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.

4.3.2. A Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja

Az eseménykezelési feladatok ellátása körében nemzeti szinten működik a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (továbbiakban: központ), amelyet az Országos Katasztrófavédelmi Főigazgatóság működtet, és amelyet a katasztrófák elleni védekezésért felelős miniszter irányít. A központ jellegzetességét az adja, hogy bár egyfajta sajátos ágazati eseménykezelő központként értelmezhető, mégis 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.

Ennek megfelelően 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.

4.4. A Nemzeti Közszolgálati Egyetem központi szerepe[109]

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

a.) a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeinek, oktatási programjának kidolgozásáért;
b.) az elektronikus információs rendszer biztonságáért felelős személy részére előírt szakképzettség képzettségi követelményeinek meghatározásáért.

Gondoskodik továbbá a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről, valamint közreműködik az információbiztonsági, kibervédelmi, létfontosságú információs rendszer védelmi gyakorlatokon.

Nemzetközi kitekintés

A hazai intézményrendszer bemutatása akkor lehet teljes, ha annak nemzetközi kapcsolatait, együttműködési területeit is tárgyaljuk. Az Európai Unió tagállamaként először a kiberbiztonsággal foglalkozó uniós szervezeteket mutatjuk be.

Az Európai Közösség 2004-ben a *460/2004/EK rendelettel* hozta létre az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA) abból a célból, hogy létrejöjjön egy olyan uniós szintű szakértői központ, amely a hálózat- és információbiztonság területén iránymutatással, tanácsadással és segítségnyújtással szolgál, és amelyre az uniós intézmények és a tagállamok támaszkodhatnak. Az *Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről szóló 2013. május 21-i, 526/2013/EU európai parlamenti és tanácsi rendelet*, mely egy általános hatályú, valamennyi tagállamra kötelező és a nemzeti törvényekkel egyenértékű uniós jogszabály, amely meghatározza az ENISA feladatait. Főbb feladatait tekintve az ENISA:

a.) összegyűjti az elektronikus hírközlés, az elektronikus infrastruktúra és az elektronikus szolgáltatások biztonságát és ellenálló képességét fenyegető veszélyforrások elemzéséhez szükséges információkat és adatokat, és ezek alapján felméri az uniós hálózat- és információbiztonság állapotát, melyben a tagállamok, az Európai Bizottság és szükség esetén az érintett érdekeltek is közreműködnek;
b.) gondoskodik az uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel, valamint a tagállamokkal való együttműködésről;
c.) javítja az európai érdekeltek közötti közös munkát, ennek érdekében tevékenységébe bevonja a vonatkozó területen működő illetékes nemzeti és uniós szerveket és a civil szféra szakembereit, különösen az elektronikus hírközlő hálózatok szolgáltatóit és az elektronikus hírközlési szolgáltatásnyújtókat, a hálózati berendezések gyártóit és a szoftverek forgalmazóit.

A *Digitális Menetrend* további célkitűzése volt egy hálózatbiztonsági vészhelyzeteket elhárító, állandó csoport felállítása is. Az Európai Unió intézményei 2013-ban hozták létre a CERT-EU-t, mely együttműködik az egyes uniós intézmények számítástechnikai biztonsági csoportjaival, kapcsolatot tart fenn a tagállamokban, így a Magyarországon és az unión kívül működő CERT-ekkel és számítástechnikai biztonsági cégekkel. A kapcsolattartás fő célja, hogy biztosítható legyen a fenyegetésekre és az ezek kezelésére vonatkozó információcsere.

Az információbiztonság uniós intézményrendszerében szükséges még megemlíteni a szintén 2013-ban létrehozott Számítástechnikai Bűnözés Elleni Európai Központot, mely az Európai Rendőrségi Hivatal (Europol) részét képezi. A központ fő feladata a súlyos és szervezett számítástechnikai bűncselekményeket elkövető bűnözői hálózatok tevékenységének meghiúsítása, a számítástechnikai bűnözés terén elérhető európai szakértelem összefogása, operatív támogatás nyújtása az uniós tagállamok és az Unión kívüli együttműködő partnerek bűnüldöző szervei számára. A központ első egy éves tevékenysége során számos számítástechnikai bűnözés elleni műveletet koordinált[110] és részt vett több, a gyermekek internetes szexuális kizsákmányolása ellen irányuló Unión belüli rendőrségi műveletben.

A központ a komplex vizsgálódás és a stratégiai gondolkodás jegyében első éves jelentésében megvizsgálta a számítástechnikai bűnözés jövőbeni fenyegetéseit és tendenciáit. A jelentés rámutat arra, hogy egyre nő a számítástechnikai bűncselekményt elkövetők köre, és ezzel együtt növekedik a számítástechnikai bűnözők szolgáltatásai iránti kereslet és azok igénybevétele is. Számítani lehet arra, hogy kifinomultabb, agresszívabb és ellenállóbb rosszindulatú számító-

109 Ibtv. 23. §

110 Ilyen volt pl. a Police Ransomware nevű, rosszindulatú számítógépes programmal kapcsolatos nyomozás, mely program azzal vádolja az áldozatot, hogy gyermekkel való szexuális visszaélésről készült felvételt vagy más illegális tevékenységet tartalmazó illegális weboldalakat látogatott meg. A bűnözők „bírság" megfizetését követelik az áldozat megbénított számítógépének felszabadításáért, a Ransomware pedig olyan formában jelenik meg, mintha törvényes bűnüldöző szervet képviselne. A számítástechnikai bűnözők meggyőzik az áldozatot, hogy fizessen mintegy 100 eurós „bírságot" két típusú – virtuális és névtelen – fizetési átjárón keresztül.

gépes programok kifejlesztésére kerül sor, melyek új csatornákon, mobil eszközökön és azok szoftverein is terjednek majd. Az internetkapcsolat gyors terjedésének köszönhetően növekedni fog a délkelet-ázsiai, afrikai és dél-amerikai eredetű számítástechnikai bűncselekmények száma. Várhatóan növekedik majd a pénzmosás iránti igény, amelyhez elektronikus fizetőeszközöket és más névtelen fizetési rendszereket használnak a bűnözők. Arra lehet számítani, hogy a bűnözők egyre többször próbálnak majd feltörni felhőalapú informatikai szolgáltatásokat kémkedés, fizetési azonosítók letöltése és zsarolás céljából.

A *szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség létrehozásáról szóló 2011. október 25-i 1077/2011/EU parlamenti és tanácsi rendelet* hozta létre azt az európai ügynökséget (eu-LISA), melynek feladata a három uniós belügyi IT-rendszer [második generációs Schengeni Információs Rendszer (SIS II); Vízuminformációs Rendszer (VIS); Eurodac (az ujjlenyomatok összehasonlítására alkalmas számítógépes központi adatbázis, valamint a tagállamok és az adatbázis közötti elektronikus adatátvitelt biztosító rendszer)] üzemeltetési igazgatása. Ezek a rendszerek Magyarország számára is nagy jelentőséggel bírnak a bennük tárolt adatok okán. Az ügynökség biztosítja:

a.) a rendszerek biztonságos és folyamatos működését, pénzügyileg elszámoltatható igazgatását, a hatékony fejlesztést szolgáló, megfelelő projektirányítási struktúra alkalmazását;
b.) a felhasználók számára megfelelően magas színvonalú szolgáltatásnyújtást;
c.) a szolgáltatás folyamatosságát és zavartalanságát;
d.) a magas szintű adatvédelmet;
e.) az adat- és a fizikai biztonság megfelelő szintjét;
f.) a rendszerek technikai használatára vonatkozó képzéssel kapcsolatos feladatokat.

A kiberbiztonság előmozdításában közreműködő nemzetközi fórumok bemutatása során az Európai Unió által létrehozott intézményeken kívül meg kell említeni az ISACA (Information Systems Audit and Control Association) non-profit szakmai szervezetet is. Az ISACA tagjai az ipari-, a pénzügyi- és a szolgáltató vállalatok IT vezetői, üzemeltetői, biztonsági szakemberei és ellenőrei, illetve a téma iránt érdeklődő szakemberek, valamint magánemberek, világszerte mintegy 95.000 fő. 160 országban, 193 tagszervezettel rendelkezik, többek között Magyarországon is, ahol több mint 420 tagja van. Az ISACA egyik elsődleges célja a legjobb gyakorlatra alapozott módszerek felkutatása, oktatása és elterjesztése, melyhez egyfajta szakmai fórumot biztosít tagjai számára a tapasztalatcsere és a tapasztalatok hasznosítás céljából. Az ISACA kidolgozott egy minősítési rendszert, mely minősítések (CISA, CISM, CGEIT, CRISC) megszerzésével a pályázó szakemberek világszerte bizonyíthatják széleskörű és alapos információbiztonsági ismereteiket. Tevékenysége továbbá szakmai ajánlások kidolgozása, etikai szabályok meghonosítása, a tudatosságnövelésben való részvétel, a megfelelő jogszabályi háttér kidolgozásának elősegítése. A képzés során szakmai oktatások tananyagának, tematikájának kidolgozásában való részvétellel járul hozzá a tudatosságnöveléshez. A számítógépes és azzal támogatott bűnözés visszaszorításának elősegítése céljából együttműködik a jogalkotó és felügyeleti szervekkel, hatóságokkal és egyéb közintézményekkel.

5. Végrehajtási szabályok

Az Ibtv. felhatalmazó rendelkezése alapján kiadásra kerültek azok a végrehajtási rendeletek, amelyek meghatározzák az elektronikus információbiztonság szervezetrendszerét és szerveinek feladatellátását, a hatósági, szakhatósági eljárás lefolytatásának speciális szabályait, a biztonsági események bejelentésének, kezelésének rendjét, a nyilvántartások vezetésére vonatkozó szabályokat és részletesen tartalmazzák a szervek számára előírt feladatok, kötelezettségek végrehajtását támogató rendelkezéseket és a tudatosságnövelést segítő intézkedéseket.

5.1. A hatóság és a szakhatóság eljárása

Az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét – a törvényben meghatározott kivétellel – az e-közigazgatásért felelős miniszter látja el. A hatósági és a szakhatósági feladatok 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* (továbbiakban: Korm. rendelet) tartalmazza.

5.1.1. A hatósági eljárás lefolytatása

5.1.1.1. A hatósági eljárás általános szabályai[111]

A Hatóságnak az Ibtv.-ben meghatározott és a 4.2. pontban ismertetett valamennyi feladatához kapcsolódó eljárása során érvényesülnek az alábbi általános szabályok:

a.) az ügyintézési határidő 60 nap, amely egy alkalommal további 30 nappal meghosszabbítható;
b.) a Hatóság az eljárást lezáró döntésének meghozatala előtt egyeztetést folytat le az eljárással érintett szervezettel;
c.) a Hatóság helyszíni ellenőrzést folytat le,
d.) Hatóság bármely hatásköre szerinti eljárási cselekményt haladéktalanul lefolytathat, ha az a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és polgárai számára kiemelten fontos információs rendszereket súlyosan veszélyeztető fenyegetés elhárítását szolgálja;
e.) a Hatóság az érintett szervezetek bejelentése, valamint a kormányzati eseménykezelő központ értesítése alapján tudomására jutott biztonsági eseményeket haladéktalanul megvizsgálja, és megteszi azok elhárítása érdekében szükséges intézkedéseket;
f.) a Hatóság határozatai ellen rendkívüli jogorvoslatként újrafelvételi eljárásnak nincs helye, továbbá a határozatok felügyeleti jogkörben való visszavonására, módosítására sincs lehetőség.

A Hatóság helyszíni ellenőrzésének lefolytatása során a helyszíni ellenőrzést ellátó munkatársai – a Hatóság vezetője által kiállított megbízólevél alapján – az alábbiak szerint járnak el:

a.) az ellenőrzés során beléphetnek az érintett szervezet információtechnológiai tevékenységével összefüggő helyiségeibe,
b.) ezen helyiségekben ellenőrzést tarthatnak, a kapcsolódó dokumentációt, információs rendszert, biztonsági intézkedést megismerhetik, ellenőrizhetik,
c.) információtechnológiai műszaki vizsgálatot végezhetnek, kivéve a szakhatóság hatáskörébe tartozó biztonsági események műszaki vizsgálatát.
d.) A helyszíni ellenőrzésről az érintett szervezet vezetőjét előzetesen írásban, az információs rendszer biztonságáért felelős személyt a helyszíni vizsgálat megkezdése előtt elektronikusan értesítenie kell a Hatóságnak, amely értesítés mellőzhető, ha:
e.) súlyos fenyegetés áll fenn vagy ennek bekövetkezése valószínűsíthető,
f.) súlyos biztonsági esemény történt vagy ennek bekövetkezte valószínűsíthető,
g.) az érintett szervezet a helyszíni ellenőrzés eredményes lefolytatását feltehetően meghiúsítaná.

A helyszíni ellenőrzés során az érintett szervezet vezetőjét, munkatársait és az elektronikus információs rendszer biztonságáért felelős személyt együttműködési kötelezettség terheli.

111 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) 2. - 5. §-ok és 20. § alapján

A helyszíni ellenőrzésről a Hatóság 8 napon belül jegyzőkönyvet köteles készíteni, melyet az érintett szervezet 8 napos határidővel véleményezhet és kezdeményezésére az esetleges észrevételekről a Hatósággal egyeztetést folytathat le.

5.1.1.2. Az egyes hatósági eljárások lefolytatása

1. A Hatóság az érintett szervezetnek az Európai Unió tagállamaiban történő elektronikus információs rendszere üzemeltetésének engedélyezése során vizsgálja[112]:

h.) az adatkezelés indokát,
i.) a kezelt adatok és az adatbázisok leírását,
j.) az adatkezelő üzemeltetőjének és az adatkezelés jogszabályi megfeleléséért felelős személy kilétét,
k.) az adatkezelő rendszer technikai és technológia leírását,
l.) ha a kérelem benyújtásakor az érintett szervezetnek nincs érvényes biztonsági tanúsítványa:
- az adatkezelő rendszer információbiztonságának ismertetését,
- a rendszerhez kapcsolódó és az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- a biztonsági rendszer felülvizsgálatának eredményét,
- a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot, és
- az üzemeltetés helyszínén illetékes hatóságoknak a kezelt adatokba történő betekintésre való jogosultságát.

Az engedélyezési eljárás kérelemre indul, melyet 90 nappal az Európai Unió területén történő adatkezelés megkezdése előtt kell benyújtani a Hatósághoz. Engedély hiányában az elektronikus információs rendszer Európai Unió területén történő üzemeltetése nem kezdhető meg. Ez alól kivételt jelent az az eset, ha az adatkezelésre vagy rendszerüzemeltetésre olyan nemzetközi szerződés alapján kerül sor, amelyben a magyar állam az egyik szerződő fél. Ennek tényéről a Hatóságot tájékoztatni kell, amely tájékoztatást a Hatóság eljárás lefolytatása nélkül tudomásul vesz.

2. A Hatóság jogosult a központi, valamint uniós forrásból megvalósuló fejlesztési projektek információbiztonsági követelményei teljesítésének ellenőrzésére is, melynek során a szakhatóság véleményét is köteles beszerezni. Az ellenőrzés lefolytatása érdekében az adott projektszakasz zárását megelőző legalább 30 nappal – 60 napnál rövidebb időtartamú projekt esetében a projekt befejezésekor – a projekt vezetője véleményezés céljából átadja a Hatóságnak a biztonsági osztályba sorolásra, a biztonsági szint meghatározására vonatkozó dokumentációt, továbbá valamennyi olyan iratot, amelyek alapján elvégezhető az ellenőrzés.[113]

3. Az elektronikus információs rendszer biztonsági osztályba sorolásának ellenőrzését a Hatóság az érintett szervezet által részére megküldött információk alapján *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 biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendeletben* (továbbiakban: technológiai rendelet) meghatározott szempontok szerint végzi el.

Ha a Hatóság felülbírálja az érintett szervezet önbesorolását és magasabb biztonsági osztályt állapít meg az elektronikus információs rendszer vonatkozásában, akkor a Hatóság döntésének megfelelő biztonsági osztályhoz igazodva, a 3.1.3. pontban meghatározott időtartam alapján – a fokozatosság elvének betartásával – kell az érintett szervezetnek meghatároznia, hogy az elvárt biztonsági intézkedések megtételére milyen ütemezéssel kerül sor.

Ha a Hatóság arra a következtetésre jut, hogy a bejelentett biztonsági osztálynál alacsonyabb biztonsági osztályt is alkalmazhat az érintett szervezet, akkor erre az érintett szervezetnek javaslatot tesz. Abban az esetben, ha az érintett szervezet álláspontja szerint az elektronikus információs rendszerére irányadó biztonsági osztály helyett alacsonyabb biztonsági osztály megállapítására kerülhet sor, az érintett szervezetet indokolási kötelezettség terheli, amelyet a Hatóság felülbírálhat.

4. A biztonsági osztályba sorolásra vonatkozó fenti eljárási szabályok érvényesülnek az érintett szervezet biztonsági szintje megállapításának Hatóság általi vizsgálata során is.[114]

112 Korm. rendelet 8. §
113 Ibtv. 1. § (1) bekezdés 40. pont
114 Korm. rendelet 9. §

5.1.2. A szakhatósági eljárás lefolytatása

5.1.2.1. A sérülékenységvizsgálat[115]

A *„sérülékenység az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat”*[116], erre tekintettel különösen fontos annak folyamatos vizsgálata, az azzal összefüggésben felmerülő kockázatok feltárása.

Az NBF mint szakhatóság által lefolytatott sérülékenységvizsgálat célja:
a.) a szervezet elektronikus információs rendszere, rendszerelemei gyenge pontjainak feltárása,
b.) az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása.

A sérülékenységvizsgálat tárgya:
a.) az adatok, információk kezelésére használt elektronikus információs rendszereknek, rendszerelemeinek, eszközöknek, eljárásoknak, és kapcsolódó folyamatoknak, valamint
b.) az ezeket kezelő személyek általános informatikai felkészültségének, és a szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.

A sérülékenységvizsgálat során az előzetesen elkészített szakhatósági dokumentáció szolgál kiindulási pontként az egyes vizsgálatok elvégzéséhez, amelyben rögzítésre kerülnek az elvégezendő feladatok és célok, a technikai és személyi feltételek, az alkalmazott módszertan, a vizsgálat befejezésének várható időpontja. A szakhatósági dokumentációt – a sérülékenységvizsgálat megfelelő előkészítése érdekében – az érintett szervezet 3 munkanapos határidővel véleményezheti.

A sérülékenységvizsgálat több különböző vizsgálatból is állhat, melyek elvégzésére a Korm. rendelet eltérő határidőket állapít meg az alapos és átfogó vizsgálati eljárás lefolytatása érdekében. A külső vizsgálat[117] (15 nap), a webes vizsgálat[118] (50 nap), a belső vizsgálat[119] (75 nap), a vezeték nélküli hálózat vizsgálat[120] (15 nap), a 3G/GPRS vizsgálat[121] (30 nap) és az emberi tényezőkön alapuló vizsgálat[122] (30 nap) egyaránt azt szolgálják, hogy az érintett szervezet elektronikus információs rendszerét érintő belső és külső kapcsolódások, behatások áttekintésére és a veszélyforrások feltárására sor kerülhessen. 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.[123]

A sérülékenységvizsgálat eredményes lefolytatásához az érintett szervezet együttműködése is szükséges, így ha az érintett szervezet a hiánypótlási felhívásban megjelölt adatokat, dokumentumokat, eszközöket és egyéb információkat nem adja át a szakhatóságnak, illetve a tényállás tisztázása során a kért nyilatkozatot nem teszi meg, a szakhatóság a rendelkezésére álló adatok alapján dönt.

A szakhatósági eljárás eredménye a sérülékenységvizsgálati szakhatósági állásfoglalás (a továbbiakban: állásfoglalás). Az 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.

115 Korm. rendelet 12. – 14. §-ai
116 Ibtv. 1. § (1) bekezdés 40. pont
117 Korm. rendelet) 1.§ 11. pont.
118 Korm. rendelet 1.§ 17. pont
119 Korm. rendelet 1.§ 4. pont
120 Korm. rendelet 1.§ 18. pont
121 Korm. rendelet 1.§ 19. pont
122 Korm. rendelet 1.§ 6. pont
123 Korm. rendelet 1.§ 1., 12., 13. pont, 13. § (4) bekezdés

5.1.2.2. A biztonsági események adatainak műszaki vizsgálata[124]

A biztonsági események adatainak műszaki vizsgálatára irányuló szakhatósági eljárás – melynek ügyintézési határideje 60 nap, és egy alkalommal legfeljebb 30 nappal meghosszabbítható – lefolytatásának célja:

a.) a biztonsági esemény bekövetkezte esetén azok okainak, körülményeinek megismerése,
b.) a biztonsági eseménnyel érintett elektronikus információs rendszerek, rendszerelemek meghatározása,
c.) a biztonsági esemény következtében keletkezett kár elhárítása, és
d.) az érintett szervezetek, a Hatóság, a GovCert tájékoztatása a biztonsági események megelőzése érdekében.

5.1.3. A hatósági, szakhatósági eljárás jogkövetkezményei

Az eljárás eredményétől függően a Hatóság különböző jogkövetkezményeket[125] alkalmazhat.

a.) Írásbeli felszólítás, amely az érintett szervezet vezetőjének felszólítása a mulasztás, a biztonsági követelmény megsértésének megszüntetésére, a kötelezettség teljesítésére.[126]
b.) A felügyeleti szerv közreműködésre történő felkérése: csak költségvetési szerv esetében alkalmazható abban az esetben, ha a szervezet az írásbeli felszólításnak nem tesz eleget.[127]
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.[128]
d.) Bírságolás: 50 ezer forinttól 5 millió forintig terjedő bírság kiszabása, amely jogkövetkezmény költségvetési szerv esetében nem alkalmazható.[129]
e.) Információbiztonsági felügyelő kirendelése, amelyre csak költségvetési szerv esetében kerülhet sor, ha a szerv a jogszabályokban foglalt biztonsági követelményeket és az ezekhez kapcsolódó eljárási szabályokat nem teljesíti.[130]
f.) A rövid-, közép- és hosszú távú intézkedési terv végrehajtása, amely a sérülékenységvizsgálati szakhatósági állásfoglalásban kerül meghatározásra.[131]
g.) Hatósági eljárás lefolytatásának kezdeményezése, melyet az NBF, mint szakhatóság a sérülékenységvizsgálati, illetve biztonsági események adatainak műszaki vizsgálatára vonatkozó 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.[132]

Az elektronikus információbiztonsági szabályokban előírtak érvényesülése érdekében a 4. pontban felsorolt szervek kölcsönösen tájékoztatják egymást az Ibtv. személyi hatálya alá tartozó szervek és a létfontosságú rendszerelemek kapcsán feltárt, az elektronikus információbiztonságot érintő megállapításaikról.

5.2. Bejelentési és nyilvántartási rendszer

Az elektronikus információs rendszerek védelmével kapcsolatos kötelezettségek teljesítése, a hatósági, szakhatósági feladatok ellátása, a biztonsági események kezelése érdekében szükséges a vonatkozó adatoknak a Hatósághoz történő bejelentése, azok Hatóság általi nyilvántartása. A szervezetek hatósági nyilvántartásba vételére, a biztonsági események jelentésének és közzétételének rendjére az Ibtv. és *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* (továbbiakban: NFM rendelet) előírásai alapján kerül sor.

A létfontossági rendszerelemek nyilvántartását érintő szabályokat az Lrtv. állapítja meg, amely szerint a Korm. rendeletben kijelölt ágazati nyilvántartó hatóság nyilvántartja és kezeli:[133]

a.) az üzemeltetőre, a biztonsági összekötő személyre vonatkozó adatokat,

124 Korm. rendelet 15. §
125 Korm. rendelet 17. §
126 Ibtv. 16. § (2) bekezdés a) pont, (3) bekezdés a) pont, Korm. rendelet 17. § (1) bekezdés
127 Ibtv. 16. § (3) bekezdés b) pont
128 Korm. rendelet 17. § (2) bekezdés
129 Ibtv. 16. § (2) bekezdés b) pont, Korm. rendelet 17. § (3) bekezdés
130 Ibtv. 16. § (3) bekezdés c) pont
131 Korm. rendelet 14. § (7) bekezdés
132 Korm. rendelet 13. § (2) bekezdés, 15. § (2) bekezdés
133 Lrtv. 5. §

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.

Az adatkezelés célja az Lrtv. szerinti azonosítási, kijelölési, kijelölés visszavonására vonatkozó eljárás lefolytatása és a hatósági ellenőrzés biztosítása.

5.2.1. A szervezet hatósági nyilvántartásba vétele

A szervezetnek a hatósági nyilvántartásba[134] vétel érdekében meg kell küldenie a Hatósághoz:
a.) az azonosításához szükséges adatokat,
b.) azt elektronikus információs rendszereire (megnevezés, biztonsági osztály, technikai adatok), a szervezet biztonsági szintjére vonatkozó adatokat,
c.) az elektronikus információs rendszere biztonságáért felelős személynek a személyazonosító adatait, elérhetőségeit, a feladatellátásához szükséges felsőfokú végzettségére és szakképzettségére vonatkozó adatokat,
d.) az informatikai biztonsági szabályzatát és
e.) a biztonsági eseményekkel kapcsolatos bejelentéseket.

A hatósági nyilvántartásba vételre vonatkozó bejelentési kötelezettséget[135]:
a) az a)-c) pontok tekintetében:
a. alapesetben az Ibtv. hatálybalépésétől,
b. az Ibtv hatálya alá tartozó (lásd: 3.1.2. pont) 2014. július 1-jét követően jogelőd nélkül létrejött szervezet esetében a létesítést megalapozó döntés hatálybalépésétől,
c. az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől,
d. a létfontosságú rendszerelemmé kijelölő határozat jogerőre emelkedésétől számított 60 napon belül, illetve az adatkezelési tevékenység megkezdéséig,
b) a d) pont esetében:
a. alapesetben az Ibtv. hatálybalépésétől,
b. az Ibtv hatálya alá tartozó (lásd: 3.1.2. pont) 2014. július 1-jét követően jogelőd nélkül létrejött szervezet esetében a létesítést megalapozó döntés hatálybalépésétől,
c. az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől,
d. a létfontosságú rendszerelemmé kijelölő határozat jogerőre emelkedésétől számított 90 napon belül, illetve az adatkezelési tevékenység megkezdéséig, kell a szervezetnek teljesítenie.

Az NFM rendelet szerint az Ibtv. hatálya alá tartozó szervezetnek a tevékenysége megkezdését megelőző nyolc napon belül kell eleget tennie a Hatóság részére történő adatközlési kötelezettségének.[136] Az adatközlés 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 nyilvántartásba veszi és 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.

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

134 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) 1. § 4. pont.
135 Ibtv. 26. § (5) bekezdés
136 Ibtv. 15. § (1) bekezdés a)-c) pontjai szerinti adatok.

5.2.2. A biztonsági események bejelentése, közzététele[137]

Az elektronikus információs rendszerek védelmének egyik fontos eleme a biztonsági események[138] megelőzése, bekövetkezésük esetén az azokra történő gyors reagálás, az események szakszerű kezelése. A biztonsági eseményekről a Hatóság az Ibtv. hatálya alá tartozó szervek bejelentése alapján szerez tudomást, amely bejelentéseket a közigazgatási hatósági eljárásról és szolgáltatásról szóló törvény szerint írásbelinek minősülő elektronikus úton[139] köteles megtenni. E szabály alól kivételt képez a minősített adatot tartalmazó bejelentés, amelyet papír alapon kell megtenni.

A biztonsági események bejelentését követően a Hatóság:

a.) jogosult – személlyel, szervezettel nem azonosítható módon – az elektronikus tájékoztatásra vonatkozó szabályok szerint közzétenni azokat a megismert biztonsági eseményeket, amelyek általános fenyegetést jelentenek a kiberbiztonságra,

b.) közzéteheti továbbá a fenyegetés elhárítására szolgáló információkat,

c.) tájékoztathatja – személlyel, szervezettel nem azonosítható módon – az incidens-kezelési munkacsoportot azon biztonsági eseményekről és azok értékeléséről, amelyek a munkacsoport tagjainak védelmi felkészültségét növelik,

d.) a bejelentésről értesíti a Nemzeti Adatvédelmi és Információszabadság Hatóságot, ha a bejelentett, vagy a tudomására jutott biztonsági eseményről egyértelműen megállapítható, hogy az személyes adatokat, vagy azok bizalmasságát sértette.

5.3. Technológiai követelmények meghatározása

Az elektronikus információs rendszerek teljes életciklusában megvalósuló zárt, teljes körű, folytonos és kockázatokkal és költségekkel arányos védelmének megteremtését szolgáló alapeljárás a 3.1.3. pontban ismertetett biztonsági osztályba sorolás és az ehhez kapcsolódó szervezeti biztonsági szint meghatározás. A biztonsági osztályba sorolásra és a biztonsági szint meghatározására vonatkozó részletszabályokat a technológiai rendelet tartalmazza. A szervezet elektronikus információs rendszereit a technológiai rendelet 1. mellékletében foglaltak figyelembevételével sorolja be biztonsági osztályokba. A szervezet biztonsági szintjének megállapítására a technológiai rendelet 2. melléklete alapján kerül sor.

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. Figyelemmel arra, hogy egy adott elektronikus információs rendszer nem minden eleme, funkciója kerül használatba vételre, a szervezetnek az előírt követelményeket az elektronikus információs rendszer csak azon elemei, funkciói tekintetében kell megvalósítani, amelyek üzemeltetésére, használatára sor kerül.

A technológiai rendelet – az elektronikus információs rendszerek üzemeltetési gyakorlatára figyelemmel – külön rendelkezést tartalmaz továbbá arra az esetre, ha az adott elektronikus információs rendszert több szervezet használja. Ez esetben az üzemeltetőnek kell gondoskodnia a követelmények érvényesítéséről, azzal, hogy a követelmények, feltételek, elvárások az érintett szervezet elektronikus információbiztonsággal kapcsolatos eljárásrendjébe beépüljenek.

5.3.1. Az elektronikus információs rendszerek biztonsági osztályba sorolása

Az elektronikus információs rendszerek biztonsági osztályba sorolásakor (lásd: 3.1.3. pont) a bizalmasság, a sértetlenség, a rendelkezésre állás alapkövetelményének az elektronikus információs rendszer funkciójára tekintettel, ahhoz igazodó súllyal általánosságban kell érvényesülnie. A technológiai rendelet szerint létfontosságú információs rendszerelem vonatkozásában a rendelkezésre állás biztosítása az elsődleges követelmény, más esetben ez a sértetlenség (pl. a nemzeti adatvagyont kezelő rendszerek esetében), vagy a bizalmasság fenntartása (pl. a különleges személyes adatokat kezelő rendszerek esetében) tekintetében jelenik meg.

A biztonsági osztályba sorolás a szervezet feladatainak, elektronikus információs rendszereinek folyamatos felülvizsgálatát igénylő feladat, amely során a biztonsági osztály fokához igazodva szigorodnak a követelmények és ezzel

137 NFM rendelet 8.-9. §-ok

138 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. - Ibtv. 1. § (1) bekezdés 9. pont.

139 Ket. 28/A. § (1) bekezdés a) pont ab) alpont.

arányos az elvégezendő feladat nagysága, ezért kiemelten fontos a biztonsági osztályba sorolást megelőzően elvégezni a kockázatelemzést. A kockázatelemzés alapját:

a.) az adatnál, rendszerelemnél jelentkező sérülés,
b.) az adatvesztés,
c.) a bekövetkezett kár, vagy a káros hatás terjedelme, nagysága,
d.) a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszélynek a mértéke, becsült valószínűsége képezi.

A technológiai rendelet[140] alapján az elektronikus információs rendszereket:

1. biztonsági osztályba kell sorolni akkor, ha csak jelentéktelen káresemény következhet be, mivel nem kerül sor jogszabály által védett adat kezelésére és bizalomvesztésre, továbbá a bekövetkezett anyagi kár jelentéktelennek minősül az érintett szervezet költségvetése, szellemi és anyagi erőforrásaihoz képest.
2. biztonsági osztályba kell sorolni akkor, ha csekély káresemény következhet be, mivel személyes adatok és az üzlet- vagy ügymenet szempontjából csekély értékű, belső intézményi szabályzóval védett adat vagy elektronikus információs rendszer sérülhet, továbbá az anyagi kár a szervezetet tekintve csekélynek mondható, és ezzel összefüggésben a lehetséges társadalmi-politikai hatások még az érintett szervezeten belül kezelhetőek.
3. biztonsági osztályba kell sorolni akkor, ha közepes káresemény következhet be, mivel:
   a.) nagy tömegű személyes adat vagy különleges személyes adat sérülhet,
   b.) az üzlet- vagy ügymenet szempontjából közepes értékű, vagy az érintett szervezet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal védett adat sérülhet;
   c.) az anyagi kár az érintett szervezet költségvetése, szellemi és anyagi erőforrásait illetően közepesnek tekinthető,
   d.) lehetséges társadalmi-politikai hatásként bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek.
4. biztonsági osztályba kell sorolni akkor, ha nagy káresemény következhet be, mivel:
   a.) különleges személyes adat nagy tömege sérülhet;
   b.) az üzlet- vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy az érintett szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet,
   c.) megnőhet a személyi sérülés esélye;
   d.) az anyagi kár a szervezetet tekintve jelentős,
   e.) a káresemény lehetséges társadalmi-politikai hatásaként a szervezet jogszabálynak megfelelő működése sérülhet, a szervezeten belül bizalomvesztés állhat elő, melynek következményeként az érintett szervezetnél személyi változással járó intézkedéseket kell alkalmazni.
5. biztonsági osztályba kell sorolni akkor, ha kiemelkedően nagy káresemény következhet be, mivel:
   a.) különleges személyes adat kiemelten nagy tömege sérül,
   b.) helyreállíthatatlanul megsérülhet a nemzeti adatvagyon,
   c.) meghatározott létfontosságú információs rendszer rendelkezésre állása nem biztosított,
   d.) emberi életek közvetlenül veszélybe kerülnek, nagy számban következhetnek be személyi sérülések,
   e.) az anyagi kár az érintett szervezet költségvetését, szellemi és anyagi erőforrásait meghaladó, különösen nagy értékű üzleti titok, kiemelten érzékeny információt képező adat sérül,
   f.) lehetséges társadalmi-politikai hatásként súlyos bizalomvesztés következhet be a szervezettel szemben, alapvető jogok, a társadalom működése szempontjából kiemelt jogok sérülhetnek.

5.3.2. Az elektronikus információs rendszereket működtető szervezetek biztonsági szintbe sorolása

Az Ibtv. hatálya alá tartozó szervezet biztonsági szintjét a sértetlenség, bizalmasság, rendelkezésre állás követelményei alapján a szervezet feladataira, a vele szemben támasztott elvárásokra és a kockázatokkal arányosan kell megállapítani. A technológiai rendelet[141] alapján a szervezet biztonsági szintjét a 3.1.3. pontban leírtak figyelembevételével:

140 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 (továbbiakban: technológiai rendelet) 1. melléklete.

141 Technológiai rendelet 2. melléklete.

1. biztonsági szintként kell megállapítani, ha a szervezetnek nincs az 1. biztonsági osztálynál magasabb besorolású rendszere, és a szervezet elfogadja, hogy elektronikus információbiztonsági folyamatának csak egyes elemei és csak részben szabályozottak, azaz:
   a.) a biztonsági folyamatoknak nincsenek részletszabályai,
   b.) az irányítási jogkörében korlátozott személy feladata az elektronikus információs rendszerek biztonságával kapcsolatos felelősség,
   c.) a rendszerek biztonsága ki van szolgáltatva az azzal kapcsolatban álló egyének tudatosságának,
   d.) megkésve, a biztonsági esemény felmerülésekor foglalkoznak az elektronikus információs rendszerek biztonságával,
   e.) az elektronikus információs rendszerek biztonsági szintjét nem mérik,
   f.) a felelősségi körök nincsenek egyértelműen tisztázva,
   g.) a működtetett rendszer és a kezelt adatok védelme fizikai védelmi intézkedéseket nem igényel.
2. biztonsági szintként kell megállapítani, ha a szervezetnek nincs a 2. biztonsági osztálynál magasabb besorolású rendszere, és a szervezet elfogadja, hogy informatikai folyamatai részben szabályozottak, azaz:
   a.) a biztonsági folyamatoknak nincsenek részletszabályai,
   b.) az elektronikus információs rendszerek biztonságához kapcsolódó eljárások még nem kerültek kialakításra,
   c.) az irányítási jogkörében korlátozott személy felelőssége és feladata az elektronikus információs rendszerek biztonsága,
   d.) a biztonságára vonatkozó információkat a szervezet nem elemzi,
   e.) a biztonságra vonatkozó jelentések nem teljes körűek,
   f.) az elektronikus információs rendszerek biztonságát elszigetelten, nem a szervezet teljes körű biztonságának részeként kezelik,
   g.) a fizikai beléptetés ellenőrzés biztosításán kívül az elektronikus információs rendszerek és a kezelt adatok védelme nem igényel további fizikai intézkedést.
3. biztonsági szintként kell megállapítani, ha a szervezetnek nincs a 3. biztonsági osztálynál magasabb besorolású rendszere, a szervezetnél követelmény, hogy információbiztonsági folyamatai jól szabályozottak legyenek, azok dokumentálásra kerüljenek, és hatékony logikai védelmi intézkedések támogassák az adminisztratív védelmi intézkedéseket, azaz:
   a.) a magas szintű szabályzatokkal összehangoltak az elektronikus információs rendszerek biztonsági eljárásai,
   b.) az elektronikus információs rendszerek biztonságával kapcsolatos felelősség rögzített, azt az érintettek ismerik és elfogadják,
   c.) a biztonsági megoldások kidolgozásánál figyelembe vették a kockázatelemzés eredményeit,
   d.) meghatározásra kerültek a biztonságirányítási célok, módszerek, de azok alkalmazása még nem teljes körű,
   e.) biztonsági és sérülékenységi teszteket végeznek,
   f.) a biztonságtudatosságot kialakították, biztonsági képzéseket tartanak,
   g.) az információs rendszerelemekhez történő fizikai hozzáférések felügyelete fizikai védelmi intézkedéssel biztosított, a fizikai károk ellen védik a rendszer egységeit,
   h.) a tartalék munkahelyeket (munkaállomásokat) kialakították, vagy biztosított azok rendelkezésre állása,
   i.) a rendszerek fejlesztésénél célként került kitűzésre az integrált elektronikus információs rendszer biztonsági értékelése, tanúsítása.
4. biztonsági szintként kell megállapítani, ha a szervezet által működtetett elektronikus információs rendszernél nincs a 4. biztonsági osztálynál magasabb besorolású rendszer, a szervezetnél követelmény, hogy információbiztonsági folyamatai irányítottak és mérhetőek legyenek, azaz:
   a.) meghatározásra kerültek az elektronikus információs rendszerek biztonságával kapcsolatos felelősségi körök, azokat betartatják,
   b.) következetesen végrehajtják a biztonsági kockázat- és hatáselemzést,
   c.) a felhasználókra vonatkozó eljárások (azonosítás, hitelesítés, jogosultságkiosztás) szabványosítottak,
   d.) az elektronikus információs rendszerek biztonságáért felelős munkatársak szakmai képzésére kiemelt figyelmet fordítanak,
   e.) szabályozott a biztonság tesztelése,
   f.) az elektronikus információs rendszerek biztonsági folyamatai a szervezet általános biztonsági funkcióival összehangoltak,
   g.) következetesség érvényesül a biztonságtudatosság megteremtése és fenntartása terén,
   h.) nyilvántartják a biztonságirányítás eredményeit, mérik annak hatékonyságát,
   i.) az információs rendszerelemekhez történő fizikai hozzáférések felügyelete fizikai védelmi intézkedéssel biztosított, a fizikai károk ellen védik a rendszer egységeit,

j.) az elektronikus információs rendszerek elemeinek biztonságos elhelyezésével, tartalék munkahelyek (munkaállomások) kialakításával azok rendelkezésre állása biztosított,
k.) az üzembeállítást megelőzi a teljes rendszer független, külső sérülékenység-vizsgálaton alapuló pozitív eredményű rendszerértékelés vagy tanúsítás,
l.) a rendszerek fejlesztésénél biztonsági szempontból értékelt termékek beszerzésére törekednek.

5. biztonsági szintként kell megállapítani, ha az érintett szervezetnél van 5. biztonsági osztályba sorolt rendszer, a szervezetnél követelmény az elektronikus információbiztonsági folyamatok optimalizálása, a jól bevált gyakorlatok alkalmazása, azok automatizálása, azaz:
a.) a szakmai és informatikai vezetés közös felelőssége az elektronikus információs rendszerek biztonsága és a szervezet célkitűzéseivel összhangban áll,
b.) a biztonsági követelmények rögzítettek, optimalizáltak, a rendszerbiztonsági tervbe beépítettek,
c.) a felelősség egyénre szabott, a biztonsági elvárásokra és funkciókra a rendszerek tervezési szakában figyelemmel vannak,
d.) szabályozott, definiált eljárásokat alkalmaznak a rendkívüli biztonsági események kezelésére,
e.) a biztonsági felmérések rendszeresek, eredményeinek értékelése folyamatos,
f.) a fenyegetésekre és a sebezhetőségre vonatkozó információk gyűjtése és értékelése rendszeres,
g.) a kockázatok elhárítására vonatkozó ellenőrzési folyamat alkalmazására és elemzésére sor kerül,
h.) biztonsági tesztelések és rendkívüli biztonsági események feltáró elemzésére sor kerül,
i.) a kockázatok felismerésére irányuló tevékenységet folytatnak,
j.) a rendszerbiztonsági terv elemzése folyamatos,
k.) a fizikai védelmi intézkedések kidolgozottak, védik a rendszer fizikai egységeit a fizikai károk ellen,
l.) független, külső és belső sérülékenység-vizsgálaton alapuló pozitív eredményű, kiemelt garanciaszintű rendszerértékelésre vagy tanúsításra kerül sor,
m.) megteszik az azok minimalizálásához szükséges intézkedéseket, az elektronikus információs rendszer fejlesztésénél biztonsági szempontból értékelt termékeket szereznek be,
n.) a biztonsági funkciók beépítését az elektronikus információs rendszerek tervezésétől a felhasználáson át az üzemeltétetésig egyaránt érvényesítik.

5.3.3. Az elektronikus információs rendszerek védelmével, a biztonsági szintek kialakításával összefüggő intézkedések köre

Az Ibtv. alapelveinek figyelembevételével, az ún. kockázatokkal arányos védelem megvalósítása érdekében a szervezetnek a technológiai rendelet 4. melléklete szerinti adminisztratív, fizikai és logikai védelmi intézkedéseket kell megtennie. A védelmi intézkedések magvalósítása során a szervezet sajátosságaihoz igazodóan egyedi eltéréseket állapíthat meg:
a.) a működtetéssel, környezettel,
b.) a fizikai infrastruktúrával,
c.) a nyilvános hozzáféréssel,
d.) a technológiával,
e.) a biztonsági politikával és a szabályozással,
f.) a biztonsági intézkedések fokozatosságával,
g.) a biztonsági célokkal
h.) a technológiai rendeletben meghatározott feltételek esetén kerülhet sor.

A technológiai rendelet rögzíti, hogy mely eljárásokat tekint helyettesítő biztonsági intézkedéseknek és milyen feltételek teljesülése esetén alkalmazható ilyen intézkedés a szervezet által.[142]

1. Az adminisztratív védelmi intézkedések között kerültek meghatározásra:
a.) a szervezeti szintű alapfeladatok,
b.) a kockázatelemzés,
c.) a tervezés,
d.) a rendszer és szolgáltatás beszerzés,
e.) a biztonsági elemzés,
f.) az emberi tényezőket figyelembe vevő – személy – biztonság,

142 Technológiai rendelet 4. melléklet 2. pont.

g.) a tudatosság és a képzés
h.) körében végrehajtásra kerülő védelmi intézkedési típusok. Az egyes típusokhoz tartozó intézkedéseket a technológiai rendelet 4. mellékletének 3.1. pontja tartalmazza.

2. A fizikai védelmi intézkedésekhez tartozó, a fizikai és környezeti védelem egyes elemeit felsoroló intézkedéseket a technológiai rendelet 4. mellékletének 3.2. pontja tartalmazza.
3. Az elektronikus információs rendszerek védelmét szolgáló intézkedések legnagyobb csoportját a *logikai védelmi intézkedések alkotják*, amelyek az adminisztratív és fizikai védelmet kiegészítve lehetővé teszik a teljes körű védelem kialakítását. Ezek az intézkedések kiterjednek az alábbi területekre:
   a.) konfigurációkezelés,
   b.) üzletmenet, ügymenet folytonosság tervezése,
   c.) karbantartás,
   d.) adathordozók védelme,
   e.) azonosítás és hitelesítés,
   f.) hozzáférés ellenőrzése,
   g.) rendszer- és információsértetlenség,
   h.) naplózás és az elszámoltathatóság,
   i.) rendszer- és kommunikációvédelem,
   j.) a biztonsági eseményekre történő reagálás.

   Az egyes területekhez tartozó intézkedéseket a technológiai rendelet 4. mellékletének 3.3. pontja tartalmazza.

Az elektronikus információs rendszerek védelmével összefüggő követelmények teljesülésének elmaradása, a fentiekben részletezett intézkedések hiányos megvalósulása olyan kockázati tényező, amelynek megelőzése az elektronikus információs rendszer védelmében érintett minden szereplő feladata.

5.4. Elektronikus információbiztonság az oktatásban

Az Ibtv. 23. §-a a Nemzeti Közszolgálati Egyetemet (továbbiakban: NKE) a képzési tevékenység ellátásával összefüggésben kijelöli az elektronikus információs rendszerek védelméért felelős vezető, az elektronikus információs rendszer biztonságáért felelős személyek, valamint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek képzési, továbbképzési követelményeinek és oktatási programjának kidolgozásáért felelős intézménynek. A képzés, a továbbképzés és az éves továbbképzés tartalmát miniszteri rendelet[143] határozza meg, és rögzíti az NKE felelősségét és feladatait.

A miniszteri rendelet az Ibtv. rendelkezéseivel összhangban három képzési formát nevesít:

1. Az elektronikus információbiztonsági vezető képesítés (a továbbiakban: képesítés) megszerzésére irányuló két féléves, 300 órás szakirányú továbbképzést, amelyet alapesetben az Ibtv. hatálybalépését követő öt éven belül (2018. július 1-ig) kell megszereznie az elektronikus információs rendszer biztonságáért felelős személyeknek[144].

A képzési kötelezettség teljesítésére megállapított öt éves alaphatáridőt a 2014. július 1-jét követően a törvény hatálya alá kerülő szervezetek esetében[145]:

a) az Ibtv. 2. § (1) bekezdésének hatálya alá tartozó szervek (lásd: 3.1.2 pont) tekintetében a szervezet létesítését megalapozó döntés hatálybalépésétől;
b) az Ibtv. 2. § (1) bekezdésének hatálya alá tartozó szervek részére adatkezelést végző szervezetek (lásd: 3.1.2 pont) tekintetében az adatkezelés megkezdésétől;
c) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozójává történő jogszabályi kijelölés (lásd: 3.1.2 pont) tekintetében az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől;
d) létfontosságú rendszerelemmé történő kijelölés (lásd: 3.2 pont) tekintetében a kijelölő határozat jogerőre emelkedésétől

kell számítani.

Nem kell megszereznie a miniszteri rendelet szerinti képesítést annak a személynek, aki rendelkezik a miniszteri rendeletben meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal. A mentességek[146] *körét az alábbi érvényes oklevelek esetében állapítja meg:*

143 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 (továbbiakban: Miniszteri rendelet).
144 Ibtv. 26. § (4) bekezdés
145 Ibtv. 26. § (7) bekezdés
146 Miniszteri rendelet 7. §

– az Information Systems Audit and Control Association (ISACA) nemzetközi szervezet által kiadott Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC),
– az International Information Systems Security Certification Consortium, Inc. által kiadott Certified Information Systems Security Professional (CISSP).

A miniszteri rendelet rögzíti továbbá, hogy 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 tapasztalat ismerhető el.

Bemeneti feltételként került meghatározásra, hogy a képzésre csak az vehető fel, aki felsőfokú végzettséggel és angol nyelvből legalább alapfokú komplex nyelvvizsgával vagy ezzel egyenértékű bizonyítvánnyal, oklevéllel rendelkezik. További feltétel, hogy a jelentkező a képzés megkezdéséhez szükséges egyéb, a miniszteri rendeletben meghatározott további adminisztratív feltételeket teljesítse.

2. Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy 50 ór*ás továbbképzését* és az elektronikus információs rendszerek védelméért felelős vezető 8 órás továbbképzését, amelyen a részvétel egy alkalommal kötelező. Mentesül a továbbképzés alól, aki az elektronikus információbiztonsági vezető képesítést már megszerezte, illetve aki CISA, CISM, CRISC, vagy CISSP érvényes oklevéllel rendelkezik.
3. A kötelező *éves továbbképzés*eket, amely:
   a.) az elektronikus információs rendszer biztonságáért felelős személy esetében 50 órás,
   b.) az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy esetében 25 órás, és
   c.) az elektronikus információs rendszerek védelméért felelős vezető esetében 8 órás.

   A miniszteri rendelet meghatározza[147] a képzéssel érintett személyi kört.

5.5. Ágazati speciális szabályok

Az Ibtv. az elkülönített, rendészeti, honvédelmi, nemzetbiztonsági, valamint diplomáciai információs célokra használt ún. zárt célú elektronikus információs rendszerek[148] és a nemzetgazdasági szempontból kiemelt jelentőséggel bíró vagy törvényi felhatalmazás alapján speciális feladatokat ellátó információs rendszerek esetében felhatalmazást ad[149] az irányítási feladatokat gyakorló miniszter részére, hogy a 14-18. §-ban meghatározott hatósági, – ideértve az információbiztonsági felügyelő feladatellátását is – szakhatósági feladatok ellátásáról saját hatáskörében eljárva gondoskodjon. (lásd 4. fejezet) Fentiekre figyelemmel került kiadásra:

a.) a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet,
b.) a Nemzeti Adó- és Vámhivatal elektronikus információs rendszerei biztonságának felügyeletéről és ellenőrzéséről szóló 34/2013. (VIII. 30.) NGM rendelet,
c.) 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,
d.) a diplomáciai információs célokra használt zárt célú elektronikus információs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 3/2014. (II. 26.) KüM rendelet.
e.) az Információs Hivatal elektronikus információs rendszereinek biztonsági felügyeletéről és ellenőrzéséről szóló 12/2015. (III. 6.) MvM rendelet.

Az egyes rendeletekben rögzítésre került, hogy
a.) ki a felelős az adott elektronikus információs rendszer védelmének biztosításáért,
b.) ki látja el az elektronikus információs rendszer biztonságáért felelős személy feladatait,

147 Miniszteri rendelet 2. §
148 Ibtv. 1. § (1) bekezdés 47. pont
149 Ibtv. 24. § (2) bekezdés

c.) kinek a kötelezettsége az informatikai biztonságpolitika, az informatikai biztonsági stratégia, az informatikai biztonsági szabályzat előkészítése, ki jogosult annak jóváhagyására,
d.) mely szervezeti egység, hogyan és milyen módon, milyen eljárásrendben gondoskodik a hatósági, szakhatósági feladatokról (ezzel összefüggésben előírásra került az éves ellenőrzési terv készítése), valamint az, hogy a helyszíni ellenőrzések lefolytatására milyen rendelkezések az irányadóak,
e.) mely szervezet felel az elektronikus információs rendszerek osztályba, a szervezet biztonsági szintbe sorolásáért,
f.) a védelmi feladatokkal összefüggésben ki és milyen együttműködésre (pl. elektronikus ügyintézési felügyelet), kapcsolattartásra (pl. hatóság, polgári nemzetbiztonsági szakszolgálat, központi, valamint ágazati eseménykezelő központ, Nemzeti Média- és Hírközlési Tanács stb.) kötelezett, és
g.) részletezésre került a biztonsági események jelentésének, az adatok kezelésének, nyilvántartásának rendje.

A Nemzeti Biztonsági Felügyelet látja el:
a.) megkeresés alapján a HM rendelet hatálya alá tartozó szerveknél a szakhatósági feladatokat,
b.) a sérülékenység- és műszaki vizsgálatot a Nemzeti Adó- és Vámhivatal (továbbiakban: NAV) elektronikus információs rendszerei vonatkozásában, azzal, hogy annak lefolytatására kizárólag a NAV elnökének javaslata alapján a nemzetgazdasági miniszter általi megkeresést vagy felkérést követően kerülhet sor.

6. Felelősségi szabályok

6.1. Az elektronikus információs rendszerek védelmét biztosító kötelezettségek

Az elektronikus információs rendszerek biztonsága érdekében kialakított szabályozás teljessé tétele, az alapelvek megvalósulásának biztosítása érdekében az Ibtv. külön rendelkezik a szervezetnek az elektronikus információs rendszer védelmét biztosító kötelezettségeiről és meghatározza:

a.) a szervezet vezetőjének,
b.) az elektronikus információs rendszer biztonságáért felelős személynek, valamint
c.) az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személyeknek a feladatait és a kötelezettségeit.

6.1.1. A szervezet vezetőjének feladatai, kötelezettségei

A szervezet vezetőjének felelősségi körébe tartozó feladatok tárgyukat illetően az alábbi csoportokba sorolhatóak.

1. A szervezet vezetőjének humán igazgatási feladatai:
   a.) kinevezi, vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt, aki azonos lehet a minősített adat védelméről szóló jogszabály szerinti vezetővel (Ibtv. 11. § (1) bekezdés c) pont),
   b.) az elektronikus információs rendszerek védelmével összefüggően gondoskodik az oktatásról, az információbiztonsági ismeretek szinten tartásáról (Ibtv. 11. § (1) bekezdés g) pont),
   c.) ha a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egységet hozhat létre (Ibtv. 13. § (4) bekezdés).
2. A szervezet vezetőjének feladatai a belső szabályozást érintően:
   a.) kiadja – az ágazati biztonságpolitika figyelembevételével – az informatikai biztonságpolitikát[150] (Ibtv. 11. § (1) bekezdés d) pont),
   b.) meghatározza - az ágazati biztonsági informatikai stratégia figyelembevételével – az informatikai biztonsági stratégiát[151] (Ibtv. 11. § (1) bekezdés e) pont),
   c.) kiadja az informatikai biztonsági szabályzatot (Ibtv. 11. § (1) bekezdés f) pont),
   d.) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat (Ibtv. 11. § (1) bekezdés f) pont).

A szervezetek elektronikus információs rendszerei védelmének alapját képező informatikai biztonságpolitika és a hosszú távú célkitűzéseket rögzítő informatikai biztonsági stratégia tartalmában az Ibtv. és végrehajtási rendeleteinek követelménye várhatóan dinamikus változást hoz, új és fejlettebb dokumentumok megjelenését eredményezi. Mivel a ezen dokumentumok nem új elemei az elektronikus információs rendszerek védelmének és a szervezetek egy része már rendelkezik is ezekkel, felülvizsgálatuk mindenképpen indokolt.

3. A szervezet vezetőjének feladatai a szervezet elektronikus információs rendszerét érintően:[152]
   a.) az elektronikus információs rendszerre irányadó biztonsági osztály, valamint a szervezetre irányadó biztonsági szint tekintetében biztosítania kell a jogszabályban meghatározott követelmények teljesülését:
      – jóváhagyja a biztonsági osztályba sorolást, valamint a biztonsági szint meghatározását,
      – felel a biztonsági osztályba sorolás és a biztonsági szint meghatározás jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért,
      – felelős a biztonsági osztályba sorolás és a biztonsági szint meghatározás eredményeinek biztonsági szabályzatba foglalásáért;
   b.) biztonsági kockázatelemzések, ellenőrzések, auditok rendszeresen lefolytatása révén köteles meggyőződni arról, hogy az elektronikus információs rendszerek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
   c.) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről.

150 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. - Ibtv. 1. § (1) bekezdés 23. pont.

151 Informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. - Ibtv. 1. § (1) bekezdés 24. pont.

152 Ibtv. 7. § (3) bekezdés és 11. § (1) bekezdés.

4. A szervezet vezetőjének feladatai a szervezetnél bekövetkezett biztonsági események kezelését érintően:[153]
   a.) a biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrást felhasználva gondoskodnia kell a biztonsági eseményre történő gyors és hatékony reagálásról, a biztonsági esemény kezeléséről,
   b.) a lehetséges fenyegetésekre történő felhívással egyidejűleg haladéktalanul tájékoztatnia kell az érintetteket a biztonsági esemény bekövetkezéséről.
5. A szervezet vezetőjének feladata a szervezet feladatainak ellátásához közreműködő igénybevétele[154] esetén, hogy ha:
   a.) az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában vesz közreműködőt igénybe, vagy
   b.) ha az adatkezelési vagy az adatfeldolgozási tevékenységéhez vesz közreműködőt igénybe,

   gondoskodjon arról, hogy az Ibtv.-ben foglaltak a létrejött jogviszony keretein belül szerződéses kötelemként teljesüljenek. E szabály alól kivételt képeznek azok az esetek, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe vennie.[155] Ez esetben az elektronikus információs rendszer védelmét szolgáló intézkedések végrehajtását a szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval és a szervezet vezetőjével.[156]
6. A szervezet vezetője a Hatósággal való együttműködés keretében[157] a Hatóság részére:
   a.) tájékoztatást nyújt az elektronikus információs rendszer biztonságáért felelős személyről,
   b.) tájékoztatás céljából megküldi a szervezet informatikai biztonsági szabályzatát,
   c.) biztosítja az ellenőrzés lefolytatásához szükséges feltételeket.

6.1.2. Az elektronikus információs rendszer biztonságáért felelős személy feladatai, kötelezettségei

Az elektronikus információs rendszer védelme körében a szervezet vezetője mellett kiemelt feladatokat lát el a szervezet elektronikus rendszereinek biztonságáért felelős személy, aki a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladatok ellátásáért felel.[158] Ennek megfelelően fokozottak a vele szemben támasztott követelmények is, így:
   a.) az Ibtv.-ben előírt feladatai és felelőssége más személyre nem ruházható át,[159]
   b.) csak büntetlen előéletű személy lehet,
   c.) rendelkeznie kell a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.[160]

Megkülönböztetett helyzetére utal az Ibtv. azon rendelkezése, mely szerint e feladata ellátása körében[161] jogosult a szervezet vezetőjének közvetlenül tájékoztatást adni és jelentést tenni, továbbá az elektronikus információs rendszer működésével összefüggő feladatok ellátásához igénybe vett közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni.
1. A szervezetre vonatkozó belső szabályozást[162] érintően köteles:
   a.) a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról gondoskodni, amely keretében elvégzi vagy irányítja a tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
   b.) előkészíteni a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
   c.) véleményezni az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit.
2. A szervezet elektronikus információs rendszereit[163] érintően:
   a.) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

153 Ibtv. 11. § (1) bekezdés.
154 Ibtv. 11. § (1) bekezdés.
155 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.
156 Ibtv. 11. § (3) bekezdés
157 Ibtv. 12. §
158 Ibtv. 13. § (2) bekezdés.
159 Ibtv. 13. § (6) bekezdés.
160 Ibtv. 13. § (8) bekezdés.
161 Ibtv. 13. §
162 Ibtv. 13. § (2) bekezdés.
163 Ibtv. 13. § (2) és (5)-(6) bekezdései.

b.) a tervezésben, fejlesztésben, létrehozásban, üzemeltetésben, auditálásban, vizsgálatban, kockázatelemzésben és kockázatkezelésben, karbantartásban vagy javításban, illetve az adatkezelésben vagy az adatfeldolgozásban közreműködők igénybevétele során – át nem ruházható feladatkörében biztosítja – az Ibtv.-ben meghatározott követelmények teljesülését.

3. Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus információs rendszer védelmének összehangolása érdekében kapcsolatot tart a Hatósággal, valamint a GovCert-tel, és a bekövetkezett biztonsági eseményről tájékoztatást köteles adni az illetékes szervnek.

6.1.3. Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy feladatai

Az Ibtv. az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyre vonatkozóan – a miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen való részvételre kötelezés mellett – külön feladatokat nem állapít meg. Ezek rögzítésére a szervezetre vonatkozó belső szabályozásokban, az informatikai biztonsági stratégiában, a munkaköri leírásban kerülhet sor. Esetében is irányadóak ugyanakkor azok az alapelvek, amelyek betartása nélkül nem valósulhat meg az elektronikus információs rendszer védelme.

6.2. Az információs rendszerekkel kapcsolatos bűncselekmények

Korábban már kifejtettük az elektronikus információs rendszerek szerepének a mindennapi életben betöltött kiemelt jelentőségét és mindazokat az intézkedéseket, feladatokat, melyek ezen rendszerek biztonságos működését hivatottak szolgálni. Ezzel együtt fontos biztosítani az információs rendszerek, az abban kezelt adatok, a felhasználók és az üzemeltetők védelmét, és meghatározni azokat az információs rendszerekkel összefüggő magatartásszabályokat, amelyeket az állam büntetni rendel.

A 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[164].

A Btk. XXV. fejezete „A minősített adat és a nemzeti adatvagyon elleni bűncselekmények" között nevesíti a minősített adattal visszaélést,[165], és a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekményt.[166]

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. („Korlátozott terjesztésű!" – elzárás; „Bizalmas!" – 1 évig terjedő szabadságvesztés; „Titkos! – 3 évig terjedő szabadságvesztés; „Szigorúan titkos!" – 1-től 5 évig terjedő szabadságvesztés.) Minősített esetként kezeli a jogalkotó, ha a bűncselekményt minősített adat felhasználására törvény alapján jogosult személy követi el, és ehhez igazodóan állapítja meg a büntetési tételeket is. A minősített adat védelmének fontosságát jelzi, hogy a Btk. a bűncselekmény előkészületét is büntetni rendeli, ha az elkövető minősített adat felhasználására törvény alapján jogosult személy.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény esetén – ha más bűncselekmény nem valósul meg – bűntett miatt három évig terjedő szabadságvesztéssel büntetendő, 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. Ha a bűncselekmény jelentős érdeksérelmet okoz, a büntetés egy évtől öt évig terjedő szabadságvesztés.

A Btk. a vagyon elleni bűncselekmények között szabályozza *az információs rendszer felhasználásával elkövetett csalás*t.[167] A tényállás szerint ezen 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. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, amely az okozott kár mértékétől függően 5 évtől 10 évig terjedő szabadságvesztés büntetéssel jár.

164 Btk. 459. § (1) bekezdés 15. pont
165 Btk. 265. §
166 Btk. 267. §
167 Btk. 375. §

Az elkövetési magatartások vagyoni érdekeket sértő, csalásszerű magatartások, a tényállás csalástól elkülönített szabályozásának azonban az az indoka, hogy ez esetben hiányzik a csalás alapvető mozzanata, a tévedésbe ejtés vagy tévedésben tartás. A kár azáltal következik be, hogy az elkövető az információs rendszert jogtalanul befolyásolja.

Az információs rendszerek védelmének kiemelt fontosságát igazolja az is, hogy az információs rendszer elleni, alábbi bűncselekmények önálló fejezetben kerültek megfogalmazásra – az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározatban foglaltakkal összhangban – a Btk.-ban (XLIII. fejezet).

A Btk. 422. §-ában szabályozott *tiltott adatszerzés* **bűncselekmény** azáltal valósul meg, hogy az elkövető a személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot jogosulatlan módon akarja megismerni. Ezen adatok jogosulatlan megszerzése megvalósulhat

- más lakásának, egyéb helyiségének vagy az azokhoz tartozó bekerített helynek titokban való átkutatásával,
- az ott történtek technikai eszköz alkalmazásával való megfigyelésével, rögzítésével;
- más közlést tartalmazó zárt küldeményének felbontásával vagy megszerzésével, és tartalmának technikai eszközzel való rögzítésével;
- elektronikus hírközlő hálózat útján másnak továbbított vagy azon tárolt adat kifürkészésével, és az észleltek technikai eszközzel való rögzítésével.

A Btk. szerint ugyanúgy bűncselekménynek minősül az is, ha a fentiek szerinti információgyűjtésre a fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából kerül sor. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, minősített esetben (bűnszövetség, üzletszerűség, jelentős érdeksérelem okozása, hivatalos eljárás színlelésével) a büntetési tétel 5 év is lehet.

Az információs rendszer felhasználásával elkövetett csalás és a tiltott adatszerzés bűncselekményt a Btk. bűntettként súlyosabban minősíti. Az elkövetési módokat tekintve a bűntett olyan szándékosan elkövetett bűncselekmény, amelynek esetében az elkövető cselekményének következményeit kívánja, vagy e következményekbe belenyugszik, és amelyre a Btk. kétévi szabadságvesztésnél súlyosabb büntetés kiszabását rendeli.

A Btk. 423. §-a szerinti *információs rendszer vagy adat megsértése* bűncselekmény elkövetője olyan személy is lehet (pl. az információs rendszer biztonságáért felelő vezető), akinek a jogosultsága alapvetően kiterjed a szankcionált magatartásra (információs rendszerbe való belépés, adat megváltoztatása, törlése), azonban, ha e személy a jogosultsága kereteit túllépi, akkor már bűncselekményt követ el. A tényállás kapcsán fontos kiemelni azt, hogy az információs rendszerbe való jogosulatlan adatbevitel önmagában nem szankcionálandó magatartás, csak abban az esetben, ha az további, nem kívánt következményekhez vezet, így ha a rendszer működését akadályozza.

A Btk. 2015. január 1-jén hatályba lépett módosítása szigorította a bűncselekmény megítélését. A korábbi szabályoktól eltérően csak az büntetendő vétség miatt, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad. Büntettnek, tehát súlyosabban minősül annak a magatartása, aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

A módosítás indoka az volt, hogy az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló 2013. augusztus 12-i, 2013/40/Európai Parlamenti és Tanácsi irányelv 9. cikke meghatározza a szankciók minimumszintjét, így az információs rendszert vagy adatot érintő jogellenes beavatkozás bűncselekmények bűnszervezetben történő elkövetése esetére legalább öt évig terjedő szabadságvesztés büntetést határoz meg, melynek a 2015. január 1-je előtti magyar szabályozás nem tudott megfelelni.

Az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmény[168] tényállása akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, a tiltott adatszerzés egyes fordulata, 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).

168 Btk. 424. §

Az információs rendszer vagy adat megsértése, illetve az információs rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekmények alaptényállásai ezzel szemben a vétség azon típusának minősülnek, amelyet az elkövető szándékosan valósít meg, és amelyet a Btk. kétévi szabadságvesztéssel rendel büntetni.

6.3. Polgári jogi és munkajogi szabályok

Az Ibtv. alapján a szervezet vezetőjének abban az esetben, ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában, valamint az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe gondoskodnia kell arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek.[169]

A szervezet vezetőjének fokozott gondossággal kell eljárnia a fenti tevékenységekkel kapcsolatos szerződéseknek *a Polgári Törvénykönyvről szóló 2013. évi V. törvényben* (továbbiakban: Ptk.) – különösen annak III-XIII. címében – foglaltaknak megfelelően a szerződés előkészítése, a szerződő fél kiválasztása, a szerződés tartalmának (tárgy, jogok és kötelezettségek) meghatározása, a szerződés módosítása, és a teljesítés (mód, határid*ő*, késedelmes vagy hibás teljesítés, elmaradás, károkozás) során. Ennek keretében gondoskodnia kell arról, hogy az Ibtv. előírásai a szervezet elektronikus információs rendszereit érintő tevékenységek végzésére vonatkozó szerződésben megjelenjenek és érvényesüljenek.

Az Ibtv. előírásainak sérelme esetén a szerződés lesz a kiindulópontja a szerződő féllel szembeni fellépésnek, ez ad lehetőséget a Ptk. szerinti kötelemben foglaltak teljesítésének kikényszerítésére, és esetleges károkozás esetén a kártérítési igény alapját is megteremti.

Tekintettel arra, hogy az elektronikus információs rendszerek védelmére vonatkozó feladatok ellátásának, a kötelezettségek teljesítésének hiánya munkajogi következménnyel járhat, a következmények esetleges alkalmazása előtt meg kell állapítani azt is, hogy milyen körülmények tették lehetővé azok bekövetkezését. A felróhatóság vizsgálata során mind a munkáltató, mind a munkavállaló oldalán felmerülhet olyan ok, amely kizárja a felelősségre vonást. A felelősségre vonás megelőzése, a munkajogi következmények alkalmazásának elkerülése érdekében mind a munkáltatónak, mind a munkavállalónak fokozott gondossággal kell eljárnia a munkavégzés feltételeinek megteremtése, a feladatok meghatározása, azok teljesítése során.

Figyelemmel az Ibtv. hatálya alá tartozó szervezetek széles körére, a tevékenységet végzők jogviszonya különböző törvényeken[170] alapul, amely egyúttal megteremti az eltérő jogkövetkezmény alkalmazásának a lehetőségét is. Az Ibtv. hatálya alá tartozó szervezetek jelentős hányadánál *a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény* (továbbiakban: Kttv.) kerül alkalmazásra. A Kttv. hatálya alá tartozó közigazgatási szerveknél [171] létesített jogviszony esetében általános magatartási követelményként érvényesülő előírás, hogy *„a kormányzati szolgálati jogviszonyban és a közszolgálati jogviszonyban [...] a köz szolgálatának elsődlegessége alapján és a jó közigazgatásba vetett társadalmi bizalom fenntartásának szem előtt tartásával kell eljárni."*[172] A Kttv. az államigazgatási szerv kötelezettségei[173] *között rendelkezik a kormánytisztviselő feladatainak és a munkakör betöltésével kapcsolatos követelményeknek a munkaköri leírásban történő rögzítéséről és* a munkaköri feladatok elvégzéséhez szükséges tájékoztatás és irányítás megadásáról. Ezzel összhangban a Kttv. rögzíti a kormánytisztviselő kötelezettségeit és jogait, *és* rendelkezik[174] arról, hogy a kormánytisztviselő feladatait köteles a köz érdekében a jogszabályoknak, a hivatásetikai elveknek és a vezetői döntéseknek megfelelően, az általában elvárható szakértelemmel és gondossággal végezni, továbbá köteles felettese utasítását végrehajtani, meghatározott feltételek fennállása esetén annak végrehajt*ását megtagadni*.

A munkavégzésre vonatkozó jogszabályok megsértésének egyik következménye lehet a fegyelmi felelősség megállapítása. A Kttv. szerint *„fegyelmi vétséget követ el a kormánytisztviselő, ha kormányzati szolgálati jogviszonyból eredő kötelezettségét vétkesen megszegi."*[175] A fegyelmi vétséget elkövető kormánytisztviselővel szemben kiszabható fegyelmi büntetés eltérő mértékű lehet, a megrovástól a hivatalvesztés fegyelmi büntetésig terjedhet. A fegyelmi felelősség mellett a Kttv. rendelkezik a kormánytisztviselő kártérítési felelősségéről is és kimondja *„A kormánytisztviselő, ha nem úgy járt el, ahogy az adott helyzetben általában elvárható, a kormányzati szolgálati jogviszonyából eredő kötelezettség*

169 Ibtv. 11. § (1) bekezdés k) és l) pont

170 A munka törvénykönyvéről szóló 2012. évi I. törvény, a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (Kttv.), a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, a honvédek jogállásáról szóló 2012. évi CCV. törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény, a bírák jogállásáról és javadalmazásáról szóló 2011. évi CLXII. törvény, a legfőbb ügyész, az ügyészek és más ügyészségi alkalmazottak jogállásáról és az ügyészi életpályáról szóló 2011. évi CLXIV. törvény.

171 Kttv. 6. § 17. pont

172 Kttv. 9. § (1) bekezdés

173 Kttv. 75. §

174 Kttv. 76. §, 78. §

175 Kttv. 155. § (1) bekezdés

megszegésével okozott kárért kártérítési felelősséggel tartozik."[176] A felelősség megállapítása körében a bizonyítási teher a munkáltatónál jelentkezik, és az eljárás lefolytatásakor, a szankciók alkalmazásakor a vonatkozó előírások szerint kell eljárnia.

Az Ibtv. hatálya alá tartozó szervek más foglalkoztatottjai esetében az adott jogviszonyra vonatkozó szabályok szerint kerül sor a felelősség megállapítására, a jogkövetkezmények alkalmazására.

176 Kttv. 160. § (1) bekezdés

7. Felhasznált és kapcsolódó főbb jogszabályok jegyzéke:

1. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (Közzétéve: Magyar Közlöny 2013. évi 47. szám)
   a.) A kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet (Kihirdetve: Magyar Közlöny 2012. évi 29. szám)
   b.) Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat (Közzétéve: Magyar Közlöny 2012. évi 19. szám)
   c.) Az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" című közös közleménye

2. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: Magyar Közlöny 2013. évi 40. szám)

4. A minősített adat védelméről szóló 2009. évi CLV. törvény (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: 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 (Kihirdetve: Magyar Közlöny 2010. évi 69. szám)

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

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

7. A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény (Kihirdetve: Magyar Közlöny 2012. évi 2. szám)

8. A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Kihirdetve: Magyar Közlöny 2012. évi 92. szám)

8. Felhasznált internetes források jegyzéke:

Digitális Menetrend:
http://europa.eu/rapid/press-release_IP-10-1239_hu.htm
http://europa.eu/rapid/press-release_IP-10-581_hu.htm
http://europa.eu/rapid/press-release_MEMO-10-200_hu.htm

„Nyílt, biztonságos és megbízható kibertér" EU stratégia tervezete:
http://europa.eu/rapid/press-release_IP-13-94_hu.htm

Irányelvtervezet a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:HU:PDF
http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/HU/trans/138226.pdf

ENISA:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:HU:PDF

Számítástechnikai Bűnözés Elleni Európai Központ:
http://europa.eu/rapid/press-release_IP-14-129_hu.htm

eu-LISA:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:286:0001:0017:HU:PDF

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.