ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

PALLAGI ANDRÁS

Kritikus infrastruktúrák védelmének vizsgálata

Témavezető: Prof. Dr. Rajnai Zoltán

Prof. Dr. Kovács Tibor

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2023. December 10.

Szigorlati/komplex vizsga bizottság:

Elnök:

Prof. Dr. Berek Lajos

Tagok:

Dr. habil. Simon Ákos

Dr. habil Berek Tamás

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Em. Dr. Berek Lajos

Titkár:

Dr. Elek Barbara Júlia

Tagok:

Dr. Jobbágy Szabolcs

Dr. habil Berek Tamás

Dr. Fürstner Igor

Bírálók:

Dr. Szűcs Endre

Dr. habil Nagy Rudolf

Nyilvános védés időpontja:

2024.

TARTALOMJEGYZÉK

BEVEZETÉS

A folyamatosan változó világban egyre nagyobb figyelem összpontosul a kritikus infrastruktúrákra[1], mint a létfontosságú rendszerekre[2]. A globalizáció, a technológiai fejlődés és a növekvő népesség számos új kihívást és lehetőséget teremt, amelyek hatással vannak a kritikus infrastruktúrák védelmére és biztonságára.

A népesség és a társadalmi rétegek különbségének növekedésével egyre fontosabbá válik a kritikus infrastruktúrák üzemzavarmentes működése. Az energiaellátástól az információ- és kommunikációs technológiákig, valamint a közlekedéstől az egészségügyig terjedő kritikus infrastruktúrák hatékony működése és védelme elengedhetetlenül fontos a modern társadalmak stabilitása és jóléte szempontjából.

Azondban a szándékos cselekményekből eredő veszélyforrások folyamatosan bővülnek, egyre több a támadás a létesítmények ellen. A terrorizmus, az ipari kémkedés, a kiberbűnözés és a szabotázs növekvő fenyegetést jelentenek a kritikus infrastruktúrákra. Ezzel párhuzamosan az éghajlatváltozás és a természeti katasztrófák is komoly kihívások elé állítják a védelmi és biztonsági intézkedéseket.

A kritikus infrastruktúrák védelmének és biztonságának fenntartása érdekében a döntéshozóknak és a szakembereknek egyre inkább összehangolt, innovatív és előrelátó megközelítésekre van szükségük. A hatékony védelmi stratégiák kidolgozása és alkalmazása, valamint a megfelelő jogszabályi keretrendszer kialakítása és fenntartása elengedhetetlen a kritikus infrastruktúrák hosszú távú biztonsága és stabilitása érdekében.

Összefoglalva, a kritikus infrastruktúrák védelme és biztonsága napjainkban és a jövőben is kiemelten fontos kérdés marad. A folyamatosan változó világban való alkalmazkodás és az új fenyegetések kezelése érdekében a döntéshozóknak, a szakembereknek és az érintett szervezeteknek együtt kell működniük, hogy biztosítsák a kritikus infrastruktúrák hosszú távú stabilitását és biztonságát.

---

[1] A 2008/114/EK irányelv alapján: a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban. [1]

[2] A 2012. évi CLXVI. törvény alapján: meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. [2]

A tudományos probléma megfogalmazása

A probléma jelentősége a kritikus infrastruktúrák védelmének fontosságában rejlik, hiszen ezek a létfontosságú rendszerek a modern társadalmak zavartalan működésének alapját képezik. Ezért is különösen aggasztó, hogy a jelenlegi magyar jogszabályi környezet, az atomenergetikai szektort kivéve, nem rendelkezik olyan követelményrendszerrel, amely a kritikus infrastruktúrák különböző zónáinak védelmi szintjeit határozná meg.[3]

Ez a hiányosság nem csak a védelmi erőfeszítések hatékonyságát csökkenti, hanem azt is nehezíti, hogy a kritikus infrastruktúrák rezilienciáját[3], azaz rugalmas ellenálló képességét növelni tudjuk. Az ellenálló képesség fejlesztése pedig alapvető fontosságú, hiszen a különböző támadásokkal, kibertámadásokkal vagy természeti katasztrófákkal szemben csak így lehet hatékony védelmet nyújtani.

A megoldás kulcsa egy olyan zónabesorolási rendszer kidolgozása lehet, amely a különböző zónákban bekövetkezhető legsúlyosabb cselekmények hatását veszi alapul a kritikus infrastruktúra működésére nézve. Ennek a rendszernek a segítségével meghatározható lenne, hogy melyek azok a zónák, amelyek esetében a legnagyobb a kockázat, és így a védelmi erőforrásokat is hatékonyabban lehetne allokálni.

Ez a megközelítés nem csupán a védelmi rendszerek hatékonyságának növelését teszi lehetővé, de egyben a kockázatkezelési stratégiák kidolgozását is segíti. Hiszen a kockázatkezelés alapja a kockázatok pontos és megbízható azonosítása, mérés és értékelése, amihez elengedhetetlen a zónák szerinti besorolás.

Összefoglalva, a kritikus infrastruktúrák védelmének kérdése sokkal átfogóbb és összetettebb, mint amit a jelenlegi jogszabályi környezet képes kezelni. Egy új, a valós kockázatokra és veszélyekre alapozó zónabesorolási rendszer kidolgozása elengedhetetlen ahhoz, hogy a kritikus infrastruktúrák védelmét a jövőben hatékonyabban tudjon megvalósulni.

[3] A 2022/2557/EK irányelv alapján: valamely kritikus szervezet azon képessége, hogy megelőzzön egy eseményt, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt enyhítse, tompítsa, ahhoz alkalmazkodjon, és abból helyreálljon. [4]

Célkitűzések

Értekezésem célja a kritikus infrastruktúrák, mint létfontosságú rendszerelemek védelmének hatékonyabbá tétele. Ehhez elengedhetetlen, hogy megvizsgáljam a jelenlegi jogszabályi környezetet, feltárjam a hiányosságait és azok következményeit.

A célom egy olyan egységes zónabesorolási rendszer kifejlesztése, amely segítségével azonosítani lehet az egyes zónák legnagyobb kockázatait, ezáltal lehetővé válik a védelmi erőforrások hatékonyabb elosztása és a kritikus infrastruktúrák hatékonyabb védelme. További eredményként a zónarendszer segíthet a kockázatkezelési stratégiák kidolgozásában is, mivel alapvető fontosságú a kockázatok pontos azonosítása, mérése és értékelése.

Célom továbbá a zónabesorolás alapján meghatározni az egyes zónákhoz kapcsolódó minimális követelmények rendszerét, különös tekintettel az elektronikus beléptető rendszerek alkotóelemeire.

Legvégül célom a követelményrendszer alapján megalkotni egy segédletet, amely alapul szolgálhat az optimális beléptető rendszer kiválasztásához a kritikus infrastruktúrák tulajdonosai, üzemeltetői számára, valamint támogatást nyújt a biztonsági rendszerek tervezőinek, kivitelezőinek, biztonsági összekötőknek és az auditoroknak.

A téma kutatásának hipotézisei

H1: Meghatározhatók a kritikus infrastruktúrák védelmi zónái.

A kritikus infrastruktúrák védelmi zónáinak meghatározása különösen fontos az esetlegesen bekövetkező incidensek hatásának kezelésében. A zónabesorolás lehetővé teszi, hogy a védelmi erőforrásokat olyan módon lehessen allokálni, hogy azok a legnagyobb pozitív hatást gyakorolják a rendszer ellenálló képességére. Ezen kívül, a zónabesorolás lehetővé teszi a kockázatkezelési stratégiák finomhangolását, figyelembe véve az egyes zónákban bekövetkező legsúlyosabb eseményeket és azok hatását a kritikus infrastruktúra működésére.

Az eddigi jogszabályi környezetben a zónabesorolás meghatározásának csak a sugárzó anyagok kezelésével kapcsolatban találkozhatunk[4]. Ez a rendszer azonban nem teljesértékű, és nem alkalmazható minden esetre. Bár a sugárzó anyagok kezelése

[4] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről [3]

speciális követelményeket támaszt, a jelenlegi szabályozás nem veszi figyelembe a különféle kritikus infrastruktúrák széles körét és a velük járó különböző kockázatokat.
Ezért hipotézisem szerint szükség van egy átfogó, minden kritikus infrastruktúra számára alkalmazható védelmi zónabesorolási rendszer kialakítására, amely nem csak a fizikai védelmet, hanem az elektronikus védelmet is magában foglalná, figyelembe véve a modern társadalmakban a kibertámadások és más elektronikus fenyegetések növekvő jelentőségét. Az ilyen átfogó követelményrendszer lehetővé tenné a különböző helyiségek hatékonyabb zónabesorolását és kezelését, ezáltal növelve a kritikus infrastruktúrák rugalmas ellenállóképességét.

H2: Meghatározható a kritikus infrastruktúrák egyes védelmi zónáihoz társított beléptető rendszerek alapkövetelményei

Hipotézisem szerint a kritikus infrastruktúrák beléptető rendszereinek alapkövetelményei a korábban általam meghatározott védelmi zónák alapján kialakíthatóak. A célom az, hogy ezen alapkövetelményeket meghatározó nemzetközi és hazai szabályozásokat, valamint a gyakorlati tapasztalatokat egy kutatás keretében vizsgáljam meg.
A kritikus infrastruktúrák több közös jellemzővel bírnak, mint például a magas biztonsági szint, a folyamatos működési követelmények, az üzemzavarok minimalizálása és a szigorú adatvédelmi szint. A beléptető rendszereknek tehát biztosítaniuk kell a megfelelő felhasználóazonosítást, a belépő személyazonosságának ellenőrzését, valamint az adatok biztonságos kezelését. Ennek érdekében a védelmi zónák alapján kialakított követelményrendszer különös jelentőséggel bír.
Feltűnt, hogy a jelenlegi szabályozások nem veszik kellő mértékben figyelembe a gyakorlati tapasztalatokat és a legjobb gyakorlatokat. Ez azt sugallja, hogy szükség van egy új követelményrendszer kialakítására, amely a kritikus infrastruktúrák általános alapelveire és a legújabb technológiákra reflektál, valamint figyelembe veszi a védelmi zónák jelentőségét.
A beléptető rendszerek kiemelt szerepet játszanak a kritikus infrastruktúrák védelmében, hiszen hozzájárulnak olyan kockázatok csökkentéséhez, mint a belső fenyegetések, illetéktelen behatolások, lopások vagy terrorcselekmények. Emellett a beléptető

rendszereknek meg kell felelniük a GDPR[5] és a magyar jogszabályok előírásainak, így az új követelményrendszernek ezeket a szempontokat is figyelembe kell vennie.

H3: Megalkotható a követelményrendszer alapján egy olyan segédlet, amely támogatást nyújt a kritikus infrastruktúrák beléptető rendszereinek tervezéséhez és kialakításához.

Hipotézisem szerint az előzőekben meghatározott alapkövetelmények alapján létrehozható egy segédlet, amely jelentős támogatást nyújt a kritikus infrastruktúrák beléptető rendszereinek kiválasztásában. Ez a segédlet olyan univerzális eszközzé válhat, amely a tervezők, kivitelezők, megrendelők, üzemeltetők, valamint az auditálók számára is hasznos iránymutatást nyújt a beléptető rendszerek kialakításának és működtetésének minden lépésében.

A segédlet alkalmazása révén a különböző érintettek képesek lesznek az optimális beléptető rendszer kiválasztására, figyelembe véve a különböző jogszabályi előírásokat, a technológiai fejlődést és a kritikus infrastruktúrák sajátos igényeit. Az általam javasolt segédlet így hozzájárulhat a kritikus infrastruktúrák védelmének megerősítéséhez, és egyben elősegítheti a hatékony és biztonságos beléptető rendszerek kiválasztását és alkalmazását.

Kutatási módszerek

A kutatási folyamat során több különböző módszertant alkalmaztam, melyek mindegyike hozzáadott értéket a kutatásom eredményeihez. Az elsődleges módszertan, amit alkalmaztam, a hazai és nemzetközi kritikus infrastruktúrákkal kapcsolatos jogszabályok elemzése volt. A jogszabályok alapos áttekintése lehetővé tette, hogy jobban megértsem a kritikus infrastruktúrákkal kapcsolatos szabályozásokat, és meghatározzam, hogy ezek hogyan befolyásolják a kritikus infrastruktúrák védelmét és működését.

Második módszertanom a külföldi kritikus infrastruktúrákkal kapcsolatos irányelvek és műszaki követelmények vizsgálata volt. Ennek segítségével megismerhettem más országok gyakorlatait, és összehasonlíthattam a magyarországi szabályozási környezetet a nemzetközi normákkal. Ez lehetőséget adott arra, hogy megvizsgáljam, melyek a

[5] GDPR: General Data Protection Regulation: A GDPR az új európai adatvédelmi rendelet rövidítése. A rendelet az egész Európai Unióban érvényes 2018. május 25. óta, ezzel egységesítve a 28 tagállam adatvédelmi rendelkezéseit.

legjobb nemzetközi gyakorlatok, és hogyan alkalmazhatók ezek a magyar jogrendszerben.

Ezen kívül, a kutatási módszertanom részét képezte a kritikus infrastruktúrákkal foglalkozó szakemberekkel készített interjúk. Ezek az interjúk lehetőséget nyújtottak a szakértőkkel való közvetlen párbeszédre, és betekintést nyújtottak a legjobb gyakorlati („best practice")[6] megoldásokba. A szakértőkkel való interakció lehetőséget nyújtott arra is, hogy közvetlenül megértsem a kritikus infrastruktúrák működésének és védelmének gyakorlati kihívásait.

Mindezen módszertanok kombinációja lehetővé tette számomra, hogy összeállítsam a magyarországi kritikus infrastruktúrák fizikai és elektronikai védelmi szabályozásának teljes képét. A jogszabályok elemzésétől kezdve a szakértői interjúkig mindegyik módszertan segített abban, hogy jobban megértsem a kritikus infrastruktúrák védelmének jelenlegi helyzetét és a lehetséges fejlesztési irányokat. A kutatási eredmények továbbá elősegítették egy új segédlet kidolgozását, amely a kritikus infrastruktúrák beléptető rendszereinek kiválasztásában nyújt segítséget a tervezők, kivitelezők, megrendelők, üzemeltetők, biztonsági összekötők és auditorok számára. Mindezek alapján állíthatom, hogy a választott kutatási módszertanok jelentős mértékben hozzájárultak a kutatás sikeréhez és a hipotéziseim igazolásához.

Kutatásomat 2023. május 10-én zártam le, ezen a napon elérhető volt az irodalomjegyzékben található összes hivatkozás.

Alaki és formai megjelenés

A szakirodalomi hivatkozásokat az értekezés törzsszövegében, az Óbudai Egyetem Biztonságtudományi Doktori Iskola formai követelményeben meghatározottaknak[7] megfelelően szögletes zárójelben" [ ] ", számmal ellátva alkalmaztam és az „Felhasznált irodalom” fejezetcím alatt rendszereztem. A megjegyzéseimet a sorszámozott lábjegyzetben fejtettem ki. A disszertációban megjelenített ábrákat az "Ábrajegyzék" című fejezetben sorolom fel. A disszertációban megjelenített táblázatokat a "Táblázatjegyzék" fejezetben sorolom fel, a táblázatok a saját kutatási eredményeimet tartalmazzák.

[6] Best practice: A jó gyakorlat vagy bevált gyakorlat (angolul best practice) a vállalati menedzsment és minőségbiztosítás területén olyan, rutinszerűen végzett tevékenységre utal, ami széles körű tapasztalatokon alapul, és több szervezetben is sikeresnek bizonyult.

[7] https://bdi.uni-obuda.hu/wp-content/uploads/2023/10/A-doktori-ertekezes-formai-kovetelmenyei.docx (letöltve: 2023.11.02.)

1 KRITIKUS INFRASTRUKTÚRÁK JOGSZABÁLYI KÖRNYEZETE

1.1 Európai Uniós jogszabályi háttér

Az európai kritikus infrastruktúrák védelmével foglalkozó jogszabályok története igen rövid, az első intézkedések csak a 2004. március 11-i madridi vonatrobbantások után születtek [5 p. 92]. Ezen események hatására az Európai Unió ráébredt, hogy a korábbi katonai konfliktusokkal ellentétben, a modern világban az ellenséges cselekmények (terrorcselekmények) már nem csak a távoli hadszíntereket veszélyeztetik, hanem az élet minden területét, az alapvető szolgáltatásokat. Ennek megfelelően az EU és tagállamai olyan jogszabályi környezetet hoztak létre, amelyek célja a kritikus infrastruktúrák védelme és az ezek elleni fenyegetések elleni védelem megerősítése. [6][7]

Az új jogszabályok már az összehangolt uniós megközelítést és az önkéntes alapú rugalmas ellenállóképesség növelését szorgalmazzák, a felkészültség és a reagálás megerősítésére, valamint a nemzetközi együttműködésre fókuszálnak. A fejezet ezen pontjában összegyűjtöttem és elemeztem az Európai Unió kritikus infrastruktúrákkal kapcsolatos jogszabályainak fejlődését a 2004-2022 időszakban.

COM/2004/0702 közlemény

Az Európai Tanács 2004. júniusában tartott ülésén felkérte az Európai Bizottságot, hogy készítsenek egy átfogó stratégiát a létfontosságú infrastruktúrák védelmére. A Bizottság „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben” címmel közleményt adott ki 2004. október 20-án, amely az alábbiakban definiálta a létfontosságú infrastruktúrák fogalmát:

*„A **létfontosságú infrastruktúrákhoz** azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából. A létfontosságú infrastruktúrák több gazdasági ágazatra kiterjednek, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány létfontosságú*

eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják. Például a jelentős városi térségek élelmiszer- vagy vízellátása néhány kulcsfontosságú létesítménytől függ, ugyanakkor a termelők, feldolgozók, gyártók, forgalmazók és kiskereskedők összetett hálózata is szükséges az ellátás biztosításához.". [8 3.1.]

COM/2005/0576 – Zöld könyv

Ezt követően az Európai Biztosság 2005.11.17-én kiadta a Zöld könyvet a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, amelynek elsődleges célkitűzése az volt, hogy „*nagyszámú résztvevő bevonásával visszajelzéseket kapjon az EPCIP[8] lehetséges megközelítési irányairól. A létfontosságú infrastruktúrák hatékony védelme megköveteli a valamennyi érintett fél – az infrastruktúrák tulajdonosai és üzemeltetői, a hatóságok, szakmai szervek és ágazati szövetségek – közötti kommunikációt, összehangolásukat és együttműködésüket nemzeti és uniós szinten egyaránt, úgy, hogy közben együttműködnek valamennyi kormányzati szinttel és a nyilvánossággal."* [9 2.]

A Zöld Könyv keretdokumentumként szolgált, amely meghatározta az EPCIP alapvető fogalmait, mint az európai (European Critical Infrastructure , a továbbiakban: ECI) és a nemzeti (National Critical Infrastructure, a továbbiakban: NCI) kritikus infrastruktúra, valamint javaslatot tett a létfontosságú infrastruktúrák figyelmeztető információs hálózat (Critical Infrastructure Warning Information Network, a továbbiakban: CIWIN) létrehozására.

A dokumentum meghatározta az EPCIP irányelveit és részletesen foglalkozott a módszeres és teljes körű kockázatelemzéssel és kockázatkezeléssel, a felülvizsgálatokkal, valamint az összes kritikus infrastruktúra hálózatának vizsgálatával, figyelembe véve az interdependenciális[9] kapcsolatokat. Bár a Zöld Könyv pozitív fogadtatásban részesült a tagállamok részéről, konkrét intézkedéseket nem tartalmazott, valamint nehézségeket okozott a határokon átnyúló hatások elemzése a tagállamok részére.

[8] EPCIP: European Critical Infratrucure Program: Kritikus Infrastruktúra Védelem Európai Program
[9] egymástól függőség, azaz függőség két infrastruktúra között, ahol az adott infrastruktúra tevékenysége, üzemzavara hatással és befolyással van a másik infrastruktúra működésére

COM/2006/0786 – „EPCIP” közlemény

2006. december 12-én az Európai Bizottság kiadta „A létfontosságú infrastruktúrák védelmére vonatkozó európai programról” elnevezésű közleményét, amely bemutatja az EPCIP végrehajtása érdekében javasolt elveket, eljárásokat és eszközöket. A célja az volt létrehozzanak egy uniós keretet a létfontosságú infrastruktúrák védelmére. [10]

A keret tartalmazta többek között az európai kritikus infrastruktúrák azonosítására és kijelölésére szolgáló eljárás meghatározását egységes szempontrendszer alapján, valamint a nemzeti kritikus infrastruktúrák védelmére vonatkozó alapvető megközelítést.

A dokumentumban a Bizottság javaslatot tett arra, hogy az egyes tagállamok bemutassák a területükön található KI[10]-k védelmével kapcsolatos megközelítésüket. Ennek keretében foglalkoztak a nemzeti kritikus infrastruktúrák azonosításával és kijelölésével a tagállam által meghatározott kritériumok alapján figyelembe véve, hogy az infrastruktúra megzavarása, vagy megsemmisülése által okozott hatásnak milyen a várható terjedelme (földrajzi hatókör), vagy a súlyossága (társadalmi, gazdasági, környezeti, politikai, pszichológiai és közegészségügyi hatás).

COM/2006/0787 – irányelv javaslat az ECIP-ről

2006. december 12-én az Európai Bizottság irányelvjavaslatot tett közzé „A Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről” címmel. [11]

Az irányelvjavaslat szövegezében már szerepeltek azok az intézkedések, amelyeket a Bizottság az európai létfontosságú infrastruktúrák azonosítása és kijelölése, valamint annak értékelése céljából javasolt.

COM/2008/0676 – határozat javaslat a CIWIN-ről

2008. október 27-én az Európai Bizottság tanács határozat javaslatot terjesztett elő a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN).[12] A javaslat célja az volt, hogy támogassa a tagállamokat a megosztott veszélyekkel,

[10] KI: kritikus infrastruktúra

sebezhetőségi pontokkal és megfelelő intézkedésekkel kapcsolatos információk cseréjében, és így csökkentve a létfontosságú infrastruktúrák védelmével kapcsolatos kockázatokat. A javaslatot több egyeztetést követően, mint elavult bizottsági javaslatot 2012.06.02-án visszavonták. [13 p. 1]

2008/114/EK irányelv

2008. december 8-án új fejezet kezdődött az európai kritikus infrastruktúrák szabályozási környezetében. Kiadásra került a 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.[1] Az irányelv magában foglalta azokat az intézkedéseket, amelyek segítik az azonosítást, az értékelést és azonosítják a kritikus infrastruktúrákat, valamint javasolja azoknak a védelmi szinteknek a meghatározását, amelyekre szükség van az adott infrastruktúra megfelelő védelme érdekében.

Az irányelv azt is előírja, hogy az infrastruktúra védelme érdekében a tagállamoknak azonosítaniuk kell a lehetséges veszélyeket, kockázatokat és fenyegetéseket, és megfelelő intézkedéseket kell hozniuk a védelemre. Az irányelv továbbá előírja, hogy a tagállamoknak egységes értékelési kritériumokat kell használniuk az infrastruktúra veszélyeztetettségének meghatározásához, valamint, hogy az infrastruktúra védelmének fejlesztése érdekében az érintett feleknek együtt kell működniük.

Az irányelv továbbá javasolta az információk cseréjét és az együttműködést a tagállamok között a létfontosságú infrastruktúrák védelmének érdekében, beleértve az információk széleskörű cseréjét a megosztott veszélyekről, a sebezhetőségi pontokról és a megfelelő intézkedésekről és stratégiákról. Az irányelv a tagállamokat arra is ösztönözte, hogy biztosítsák a hatékony védelmi intézkedéseket a létfontosságú infrastruktúrák számára, ideértve a megelőzést, a felkészülést, a válaszadást és a helyreállítást.

COM/2020/829 – irányelv javaslat

2020.12.16-án az európai Bizottság egy irányelv javaslatot terjesztett elő az Európai palament és az Európai Tanács elé a kritikus fontosságú szervezetek rezilienciájáról [14].

„*A **2008/114/EK irányelv** 2019-ben elvégzett értékelése azonban azt állapította meg, hogy a kritikus infrastruktúra használatával végzett műveletek egyre inkább összekapcsolódó és **határokon átnyúló jellege** miatt a kizárólag az egyes eszközökre vonatkozó védelmi intézkedések **nem elegendőek a zavarok megelőzéséhez**. Ezért változtatni kell a megközelítésen, és a kockázatok megfelelőbb figyelembevételének biztosítására kell összpontosítani, valamint arra, hogy a belső piac működése szempontjából alapvető szolgáltatásokat nyújtó kritikus szervezetek szerepe és feladatai jobban meg legyenek határozva és koherensek legyenek, valamint, hogy uniós szabályok elfogadására kerüljön sor a kritikus szervezetek rezilienciájának fokozása érdekében.*" [14 p. 14]

Az irányelvajánlás a kritikus infrastruktúrák védelmének fontosságára hívta fel a figyelmet, melyekre egyre nagyobb kihívásokat jelentenek az új fenyegetések, például a kiberbiztonsági támadások és a természeti katasztrófák. Az ajánlás két fő célkitűzése az uniós tagállamokban található kritikus infrastruktúrák védelmének növelése és a tagállamok közötti együttműködés javítása volt. A javasolt intézkedések közé tartozott a kritikus infrastruktúrák felmérése és az azonosított kockázatok értékelése, valamint a rugalmas ellenállóképesség növelése érdekében alkalmazható intézkedések meghatározása.

Az irányelvajánlás az uniós tagállamok kormányainak szóló felhívást is tartalmazott, hogy hozzanak létre hatékony és koordinált nemzeti stratégiákat a kritikus infrastruktúrák védelmére. A javaslat arra is felhívta a figyelmet, hogy az egyes tagállamoknak a védelem terén kialakított sajátos helyzetük figyelembevételével kell megválasztaniuk a megfelelő intézkedéseket és módszereket. Az ajánlásnak az volt a célja, hogy megerősítse az uniós tagállamok kritikus infrastruktúráinak rugalmas ellenállóképességét és javítsa a tagállamok közötti együttműködést, annak érdekében, hogy hatékonyabb védelmet biztosítson az uniós polgárok és gazdaság számára.

COM/2022/551 – javaslat ajánlás kiadására

2022.10.18-án az Európai Bizottság javaslatot tett az Európai Tanács részére egy ajánlás kiadására kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről. [15] Ennek apropóját Oroszország Ukrajna elleni agresszív háborúja adta, valamint az Északi Áramlat gázvezeték – mint európai kritikus infrastruktúra - elleni

szabotázs akció. [15 p. 1] Az Európai Unió határán lévő háborús cselekmény teljesen új kockázatokat és fenyegetettségeket generált az európai kritikus infrastruktúrák tekintetében.

ST/15623/2022/INIT – ajánlás

2022.12.08-án az Európai tanács kiadta ajánlását a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről. [16]

Az ajánlás célja, hogy támogassa és fokozza a kritikus infrastruktúrák önkéntes alapú rugalmas ellenállóképességét uniós és nemzeti szintű célzott intézkedések révén. A kritikus infrastruktúrák közé tartoznak az olyan ágazatok, mint az energetikai, digitális, közlekedési és űrinfrastruktúrák, amelyek fontos határokon átnyúló szerepet töltenek be. A célzott intézkedések a felkészültség és reagálás megerősítésére, valamint a nemzetközi együttműködés elősegítésére fókuszálnak.

2022/2557 irányelv

2022.12.14-én az Európai parlement és az Európai Tanács kiadta 2022/2557 irányelvet a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről. [4]

Az irányelv tagállami kötelezettségként határozza meg olyan intézkedések meghozatalát, amely célja, hogy biztosítsa az alapvetően fontos társadalmi funkciók, vagy gazdasági tevékenységek akadálytalan nyújtását a belső piacon. Szintén kötelezettségként szerepel a tagállamok részére az előzőekben említett funkciókat és tevékenységeket végző szervezetek rugalmas ellenállóképességének fokozása. Szabályokat állapított meg a kritikus szervezetek felügyeletére, a jogérvényesítésre, valamint a különös európai kritikus szervezetek azonosítására, valamint ezen szervezetekkel kapcsolatos tanácsadói missziók intézkedéseinek értékelésére. Közös eljárásokat határozott meg ezen irányelv alkalmazásával kapcsolatos együttműködésre és jelentéstételére. Intézkedéseket állapított a kritikus szervezetek magas szintű rugalmas ellenállóképességének elérése céljából az alapvető szolgáltatások Unión belüli nyújtásának és a belső piac működésének javítása érdekében.

1.2 Magyarországi jogszabályi háttér

A következő fejezetben a magyarországi kritikus infrastruktúrák jogszabályi környezetét vizsgálom meg. Ahogyan az Európai Uniós jogszabályok elemzésénél is tettem, itt is bemutatom a kritikus infrastruktúrákat érintő hazai jogszabályokat, kiemelve azok jelentős elemeit és azokat a célkitűzéseket, amelyeket szolgálnak. A jogszabályi elemzés során különös hangsúlyt fektetek a jogszabályok által meghatározott követelményekre, valamint arra, hogy ezek hogyan hatnak a kritikus infrastruktúrák védelmére és működésére. A fejezet célja, hogy átfogó képet adjon a magyarországi kritikus infrastruktúrákat szabályozó jogi környezetről, és az abban rejlő kihívásokról és lehetőségekről. [17][18]

2112/2004. (V. 7.) Kormány határozat

A magyarországi jogalkotásban a Kritikus Infrastruktúra Védelem Európai Programmal összefüggő feladatok a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V. 7.) Kormány határozat 1. számú mellékletében szerepelnek, amelyek a 2046/2007. (III. 19.) Kormány határozattal kerültek bele a jogszabályba. Hazai intézkedésként a következőt határozta meg: *„A Kritikus Infrastruktúra Védelem Európai Programjának megközelítését tükröző, a különböző ágazati feladat- és hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek közös keretrendszerbe foglalásáról, ágazatközi összehangolásáról szóló előterjesztés benyújtása a Kormánynak.”* Az intézkedés felelőseként több állami szervet jelölt ki az egyes ágazatoknak megfelelően, 2007. december 31-i határidővel. [19 1.sz. melléklet 2.3.1.)]

1/2007. (III.29.) Kormányzati Kordinációs Bizottság határozat

A 2000. január 1-én létrejött Kormányzati Koordinációs Bizottság 1/2007. (III.29.) számú határozatának 5. pontja alapján elfogadták a kritikus infrastruktúra védelem hazai helyzetéről, valamint a további feladatokról szóló OKF[11] előterjesztést és a feladatok végrehajtásával összefüggésben munkacsoport felállítását írta elő. Ezen felül kormány-előterjesztés elkészítését írta elő a kritikus infrastruktúra védelem nemzeti programjának kidolgozásáról, hazai koordinációjáról, valamint feladatairól a 2112/2004. (V. 7.) Korm. határozatot módosító 2046/2007. (III. 19.) Korm. határozatban foglaltakkal összhangban. [20]

[11] Országos Katasztrófavédelmi Főigazgatóság

2080/2008. (VI. 30.) Kormány határozat

2008. június 30-án a Kormány a 2080/2008. (VI. 30.) Kormány határozat útján kihirdette a Kritikus Infrastruktúra Védelem Nemzeti Programját. Ezzel a jogszabállyal implementálták a következő Európai Uniós előírásokat:

- COM/2005/0576 (2005.11.17) - Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról
- COM/2006/0786 (2006.12.12.) - A Bizottság közleménye - A létfontosságú infrastruktúrák védelmére vonatkozó európai programról
- COM/2006/0787 (2006.12.12.) - Javaslat a Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

A határozatban kihirdették a (magyar) Zöld Könyv-et, amelynek *„elsődleges célkitűzése, hogy biztosítsa a nemzeti kritikus infrastruktúrák védelméről (NKIV) szóló nemzeti program megvalósítását és egy jogszabály megalkotását, összegezze a kormányzati szereplők NKIV-vel kapcsolatos célokra, szempontokra, alapelvekre, fogalmakra és a megvalósítás alapvető formáira vonatkozó álláspontját.”* [21 1. sz. melléklet, 2.]

A 2080/2008. (VI. 30.) Kormány határozat 1. melléklete, 3.2. pontjában meghatározásra került a kritikus infrastruktúrák fogalma:

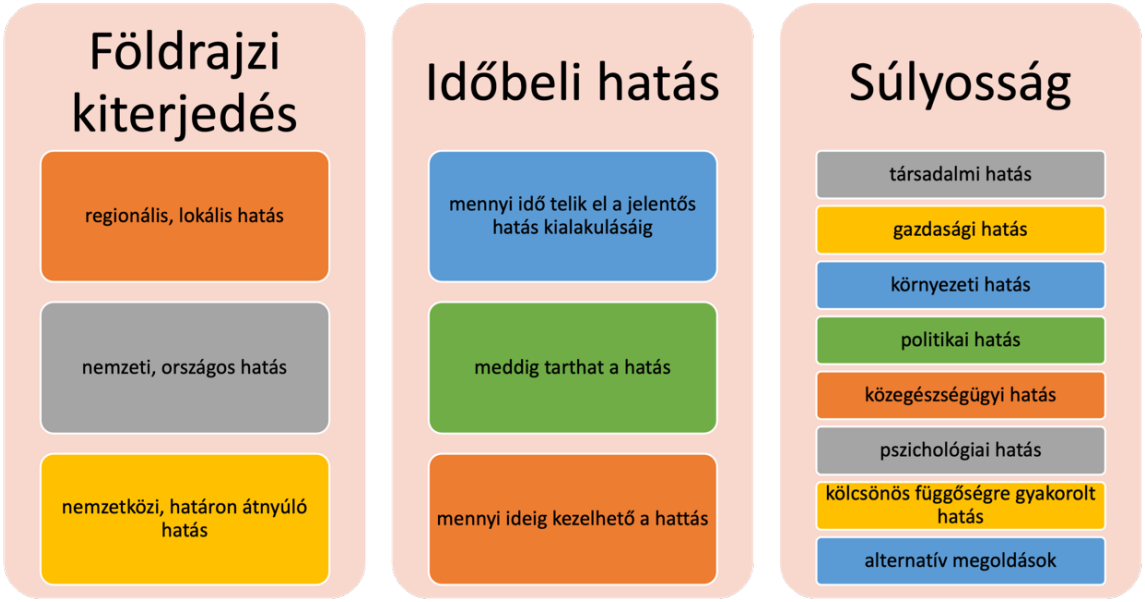
„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.” [21 1.sz. melléklet, 3.1.]

A KI-k védelmi intézkedéseinek meghatározásának érdekében bevezetésre került a következmény alapú kritikusság fogalma, amely az esetlegesen bekövetkezhető események hatásait elemezi. Három kategória került meghatározásra a hatások elemzésére:

- kiterjedés: az esemény mekkora földrajzi területre terjedhet ki, regionális, nemzeti, nemzetközi.
- súlyosság: amely a KI meghibásodásából, vagy kieséséből fakadó hatás mértékét jelenti. Értékelési szint: nincs hatás, minimális hatás, mérsékelt hatás, jelentős hatás
- időbeli hatás: mennyi idővel elteltével fejthet ki jelentős hatást, illetve mennyi ideig tarthat.

A súlyosság mértékének megállapításához figyelembe kell venni a társadalomra, a gazdaságra, a környezetre, a politikára, a közegészségügyre, a pszichológiára és a kölcsönös függőségre gyakorolt hatását, valamint vizsgálni szükséges a KI alternatív lehetőségeit.



1. ábra: Következmény alapú kritikusság három kategóriája, a szerző saját szerkesztése

A 2080/2008. (VI. 30.) Kormány határozat 1. melléklete, 3.3. pontjában meghatározásra került a kritikus infrastruktúrák szektorai (ágazatai), alágazatai. Kijelölésre kerültek az egyes ágazatokhoz tartozó KI-kért felelős állami szervek a határozat 2. számú mellékletében.

2. ábra: A KI-k ágazatai a 2080/2008. Korm. rendelet alapján, a szerző saját szerkesztése

Meghatározásra kerültek a KI-t veszélyeztető tényezők köre[12], amelyeket három fő csoportba bonthatók:

- „szándékos, illetve ártó jellegű cselekményekkel, tevékenységekkel összefüggő veszélyek”
- „természeti eredetű veszélyek, melyek az emberi tevékenységtől függetlenül, klímaváltozás, a természet erőinek hatására, elemi csapásként fordulnak elő”
- „civilizációs eredetű, technológiai veszélyek, melyek az emberi tevékenységgel összefüggésben, helytelen emberi beavatkozás, mulasztás, figyelmetlenség, vagy technikai, konstrukciós hibák hatására következnek be”

A 2080/2008 (VI.30.) Kormány határozat 2014.03.04-én hatályát vesztette, azonban a kritikus infrastruktúrákat érintő veszélyforrások csoportosítását és a bekövetkezhető események súlyosságának alapelveit, célkitűzéseit veszélyhelyzeti és üzletmenet-folytonossági tervek elkészítésénél a mai napig felhasználják állami és gazdasági szereplők.

[12] 2080/2008. (VI. 30.) Kormány határozat 1. melléklet, 3.5. pont

1249/2010. (XI. 19.) Kormány határozat

Az Európai Unió Tanács 2008. december 8-án kiadta a 2008/114/EK irányelvet az európai kritikus infrastruktúrák (EKI) azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Ebben az irányelvben a tagállamok kormányzataira több feladatot és felelősséget delegált. Ennek kezelésére 2010. november 19-én megjelent a Közlönyben a „*1249/2010. (XI. 19.) Kormány határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról"* címmel. [22]

A határozatban meghatározásra kerültek az egyes feladatok felelőse(i):

- Az európai kritikus infrastruktúra védelem nemzeti koordinációjáért: **a belügyminiszter**;
- az európai kritikus infrastruktúra védelmével kapcsolatos ügyekben a nemzeti és nemzetközi kapcsolattartó és koordinációs feladatokért: **a belügyminiszter**;
- a 2008/114/EK irányelv hatálya alá tartozó ágazatok(szektorok) tekintetében egyeztetéseket lefolytatásáért, valamint megállapodások kötéséért az Európai Bizottsággal, valamint az EU tagállamai által kijelölt kapcsolattartókkal: **a belügyminiszter, az egyes ágazatok felügyeletét ellátó miniszter**;
- szakmai munkacsoport létrehozásáért az Alkotmányvédelmi Hivatal, a Magyar Energia Hivatal, a Budapest Főváros Kormányhivatala, a Nemzeti Biztonsági Felügyelet, az Országos Katasztrófavédelmi Főigazgatóság, az Országos Rendőr-főkapitányság és a Terrorelhárítási Központ bevonásával: **a belügyminiszter, a nemzeti fejlesztési miniszter, a nemzetgazdasági miniszter, a közigazgatási és igazságügyi miniszter, a honvédelmi miniszter;**
- a munkacsoporton belül az EKI azonosításához szükséges kritériumrendszer kidolgozására, az NKIV intézmény- és kritériumrendszerének kidolgozására, valamint a EKI kijelölésével kapcsolatos kijelölésre, vagy felülvizsgálatra: **a munkacsoport tagjai**;
- a munkacsoportban meghatározott kritériumrendszerrel összhangban a honvédelmi érdekből kritikus infrastruktúrák védelmére vonatkozó intézmény- és követelményrendszert kidolgozásáért: **a honvédelmi miniszter;**

- a 2008/114/EK irányelv hatálya alá tartozó ágazatok(szektorok) hatósági engedélyezése és felügyelete terén meglévő ágazati jogszabályok felméréséért és szükség esetén jogszabály-módosításáért: **a nemzeti fejlesztési miniszter;**
- jelentés készítéséért az Európai Bizottság részére az azon infrastruktúrák ágazatonkénti számáról, amelyek tekintetében a horizontális kritériumok küszöbértékeivel kapcsolatban megbeszéléseket folytattak, valamint az EKI-nak kijelölt infrastruktúrák ágazatonkénti számáról, továbbá az Európai Unió azon tagállamainak számáról, amelyek a kijelölt infrastruktúrától függnek: **a belügyminiszter, a nemzeti fejlesztési miniszter, a nemzetgazdasági miniszter, külügyminiszter;**
- jelentés készítéséért az Európai Bizottság részére azon ágazatok sebezhetőségi pontjainak, az azokat fenyegető veszélyeknek és kockázatoknak típusairól, amelyekben európai kritikus infrastruktúrát jelöltek ki: **a belügyminiszter, a nemzeti fejlesztési miniszter, a nemzetgazdasági miniszter, külügyminiszter;**
- a kritikus infrastruktúra védelmi konzultációs fórum felállításáért és működtetéséért, valamint az ezen fórumokon felvetődött jogszabály-tervezetek elkészítéséért: **a nemzeti fejlesztési miniszter, az egyes ágazatok felügyeletét ellátó miniszter**;

  került(ek) kijelölésre. [22]

295/2010. (XII. 22.) Kormány rendelet

Az 1249/2010. (XI. 19.) Kormány határozatában a Terrorelhárítási Központ kijelölésre került abba a szakmai munkacsoportba, amelynek feladata az európai kritikus infrastruktúrák azonosításához szükséges kritériumrendszerének, valamint a nemzeti kritikus infrastruktúra védelem intézmény- és kritériumrendszerének kidolgozása volt.[22 4.] Ezen felül a munkacsoport feladata volt még a 2008/114/EK irányelv III. Mellékletében foglalt eljárási rend alapján szükségesnek vélt európai kritikus infrastruktúra kijelölésére, vagy a kijelölés felülvizsgálatára teendő javaslat elkészítése. A fentiekkel összefüggésben került kiadásra a 295/2010. (XII. 22.) Kormány rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól, amely 3.§ (1) c) pontjában szerepelnek a kritikus infrastruktúrákkal kapcsolatos feladatok: *„részt vesz a kritikus infrastruktúrák védelmére vonatkozó nemzeti program kidolgozásában, a veszélyeztetettség értékelésében és biztonsági intézkedési tervek*

kidolgozásában, továbbá külön szerződés alapján ellátja a terrorveszélyeztetettség szempontjából jelentős, kritikus infrastruktúrák védelmét".[23. 3.§ (1) c)]

2011. évi CXXVIII. törvény

A 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról című, 2021. január 1-től hatályos jogszabály, amely a 8.§ (2) i) alpontjában megjelöli a **katasztrófák elleni védekezésért felelős minisztert** a katasztrófák elleni védekezés területén a **kritikus infrastruktúrák védelmének felelőseként**. Ezen túlmenően az 52.§ g) pontjában polgári védelmi feladatként jelöli meg a létfenntartáshoz szükséges anyagi javakról történő gondoskodást, valamint a kritikus infrastruktúrák védelmét. [24] [25 p. 84]

234/2011. (XI. 10.) Kormány rendelet

A rendelet a 2011. évi CXXVIII. törvény végrehajtási rendelete. Ebben a jogszabályban a következőképpen kerül meghatározásra a kritikus infrastruktúra fogalma: *„Kritikus infrastruktúra: Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."* [26, 1.§ 25.]

A rendelet kibontja és részletezi a 2011. évi CXXVIII. törvényben, a katasztrófák elleni védekezésért felelős miniszter részére általánosan meghatározott feladatát a kritikus infrastruktúrák tekintetében:

- *„k) a hivatásos katasztrófavédelmi szerv központi szerve útján **koordinálja és ellátja a katasztrófák elleni védekezés feladatkörében** a kritikus infrastruktúrával kapcsolatos feladatokat, ezen belül a nemzeti kapcsolattartó és koordinációs feladatokat az Európai Bizottság és az Európai Unió tagállamai felé, ...*
- *m) az élet és anyagi javak védelme, az alapvető szolgáltatások biztosításának folyamatossága érdekében **javaslatot tesz** a szükséges **szabályozások kidolgozására** a kritikus infrastruktúrák katasztrófák elleni védelme tekintetében,*
- *n) **közreműködik** a kritikus infrastruktúra védelemmel összefüggő oktatási, képzési, felkészítési, tudományos kutatási és műszaki fejlesztési tevékenység összehangolásában,*

- *p) a kritikus infrastruktúra védelem feladatrendszerén belül **képviseli** a katasztrófavédelmi szempontrendszer érvényesítését,*
- *q) **közreműködik a kritikus infrastruktúra védelem horizontális kritériumrendszerének kialakításában,***
- *r) **részt vesz az ágazati miniszterek által előterjesztett potenciális ágazati kritikus infrastruktúra elemek horizontális kritériumok alapján történő beazonosításában,***
- ***s) gondoskodik a kijelölt kritikus infrastruktúra elemek katasztrófák elleni fokozott védelmének megszervezéséről...”*** [26, 5.§]

Ezen rendelet meghatározza a települések katasztrófavédelmi osztályba sorolásának szabályait és az osztályhoz tartozó védelmi követelményeket. A besorolási eljárás a kockázatok azonosításával kezdődik, majd következik a kockázatelemzés. A kockázatelemzés az egyes veszélyeztető hatások következményeit, valamint a bekövetkezés valószínűségét rendezi mátrixos formába figyelemmel a veszélyeztető hatások egymásra gyakorolt hatásával. I-III. osztályba sorolja a településeket. [26, 2. melléklet, 4. b)]

62/2011. (XII. 29.) BM rendelet

A Belügyminisztérium által kiadott rendelet feladatokat határoz meg a belügyminiszter alá tartozó egyes szervezeteknek a katasztrófák elleni védekezésben. [27] A kritikus infrastruktúrákhoz kapcsolódó feladatok az alábbiak:

- A rendelet 4.§ (1) i) alapján az **általános rendőrségi feladatok ellátására létrehozott szerv** részt vesz *„a BM OKF[13] koordinálásával a kritikus infrastruktúra védelem horizontális kritériumrendszerének kialakításában, a beazonosítási folyamatban, ezekhez adatot szolgáltat.”*
- A rendelet 5.§ (2) alapján *„A BM OKF koordinálásával a **büntetés-végrehajtás országos parancsnoka** közreműködik a kritikus infrastruktúra védelem horizontális kritériumrendszerének kialakításában, a beazonosítási folyamatban, ezekhez adatot szolgáltat.”*
- A rendelet 6.§ (2) alapján *„A BM OKF koordinálásával a **Terrorelhárítási Központ** közreműködik a kritikus infrastruktúra védelem horizontális kritériumrendszerének kialakításában, a beazonosítási folyamatban.”*

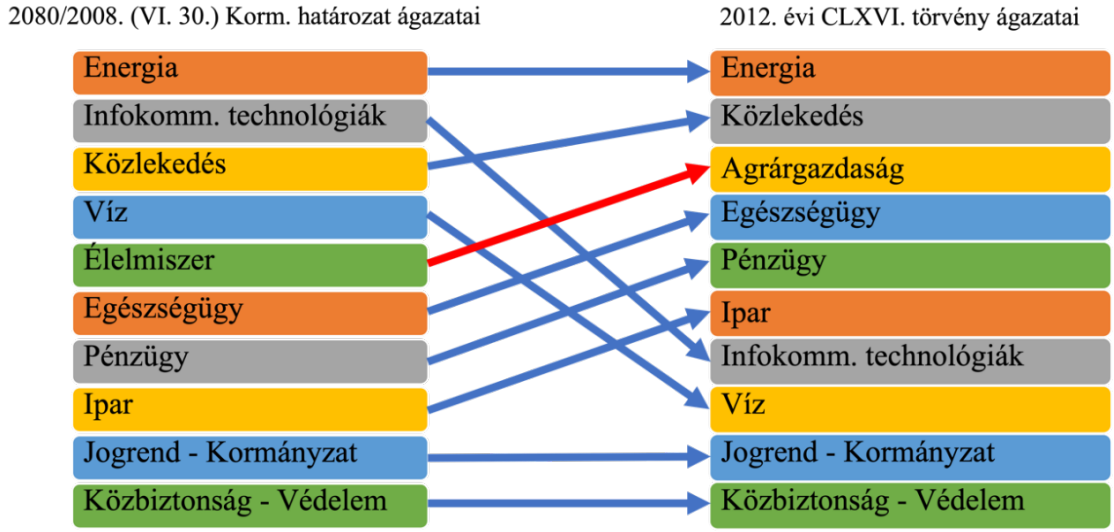
[13] Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság

- A hivatásos **katasztrófavédelmi szerv főigazgatója** a 12.§ alapján *„kapcsolatot tart a kiemelt informatikai és távközlési szolgáltatókkal, a kritikus infrastruktúra elemek üzemeltetőivel, valamint az országos médiaszolgáltatókkal”*
- A hivatásos **katasztrófavédelmi szerv igazgatóság vezetője** a
    - 13.§ g) alapján *„ellátja a katasztrófák elleni védekezés feladatkörében a kritikus infrastruktúra védelemmel kapcsolatos feladatokat,”*
    - 13.§ h) alapján *„közreműködik a kritikus infrastruktúra védelem horizontális kritériumrendszerének kialakításában, a kritikus infrastruktúra elemek beazonosítási folyamatában,”*
    - 13.§ i) alapján *„irányítja az illetékességi területén található európai, vagy nemzeti kritikus infrastruktúra elemek védelmének erősítését célzó területi katasztrófavédelmi gyakorlatok tervezését és végrehajtását,”*
    - 13.§ j) alapján *„követi, összesíti, a tervezés során felhasználja az illetékességi területén található európai, vagy nemzeti kritikus infrastruktúra elemek védelmét ellátó szervezetek, valamint az érintett hálózat üzemeltetőjének tapasztalatait és igényeit,”*
    - 13.§ l) alapján *„kapcsolatot tart az illetékességi területén található európai, vagy nemzeti kritikus infrastruktúra elemek tulajdonosaival, üzemeltetőivel, az azok védelmét ellátó szervezetekkel, valamint az érintett hálózat üzemeltetőivel,”*

2012. évi CLXVI. törvény

A 2013. 03. 01-én hatályba lépett törvény bevezette az európai és a nemzeti létfontosságú rendszerelem kifejezést. Maga a létfontosságú rendszerelem e törvény értelmezésében a következőket tartalmazza: *„az 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna,”*. [2 1. § j)] Ezt a megfogalmazást összevetve a 234/2011. (XI. 10.) Korm. rendeletben található kritikus infrastruktúra fogalom magyarázatával, szinte teljes egyezést találhatunk.

E törvényt követően jogalkotók a kritikus infrastruktúra megfogalmazás helyett a létfontosságú rendszerek és létesítmények kifejezést használták. A 2080/2008. (VI. 30.) Kormány határozatban szereplő ágazatok (szektorok) alapjait felhasználva új ágazati struktúra került kialakításra. A következő ábrán összehasonlítom a két ágazati besorolási rendszerben szereplő tételeket a jogszabályokban meghatározott sorrendben.



3. ábra: Összehasonlító ábra a 2080/2008. Korm. rendeletben és a 2012. évi CLXVI törvényben meghatározott ágazatokról, a szerző saját szerkesztése

Az összehasonlításból levezethető, hogy az egyes ágazati elnevezések egy kivételével nem is változtak. A tartalmuk sem sokban tér el, de azért fellelhetők különbségek, például releváns eltérés van az Élelmiszer és az Agrárgazdaság, valamint a két Ipar ágazatok alágazataiban.

Ezen törvény 14. §-a felhatalmazta a Kormányt, hogy rendeletben állapítsa meg az egyes ágazatok különös szabályait és állapítsa meg az ágazati és a horizontális kritériumokat. Ennek megfelelően elkészültek az ágazati rendeletek. 2023. május 10-i állapot alapján a következő ágazati jogszabályok vannak hatályban a létfontosságú rendszerekkel és létesítményekkel kapcsolatban:

- 512/2013. (XII. 29.) Korm. rendelet egyes **rendvédelmi szervek** létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról
- 540/2013. (XII. 30.) Korm. rendelet a létfontosságú **agrárgazdasági** rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről

- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú **vízgazdálkodási** rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről
- 246/2015. (IX. 8.) Korm. rendelet az **egészségügyi** létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 330/2015. (XI. 10.) Korm. rendelet a **pénzügyi ágazat**hoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 359/2015. (XII. 2.) Korm. rendelet a **honvédelmi** létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről
- 249/2017. (IX. 5.) Korm. rendelet az **infokommunikációs technológiák ágazat**hoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 161/2019. (VII. 4.) Korm. rendelet a **közlekedési** létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 374/2020. (VII. 30.) Korm. rendelet az **energetikai** létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

65/2013. (III. 8.) Kormány rendelet

a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

E rendelet további részletszabályokat állapít meg a létfontosságú rendszerelemek azonosításáról, a kijelölésről, az Integrált Hatósági Rendszer alkalmazásáról, a biztonsági összekötő személy képesítési követelményeiről, az üzemeltetői biztonsági terv tartalmi követelményeiről. Továbbá meghatározza az ellenőrzésre vonatkozó különös szabályokat, a kiszabható közigazgatási bírságok összegeit, a nyilvántartási és adatbiztonsági előírásokat, az együttműködés előírásait, a komplex gyakorlatok előírásait, valamint az összehangolt védelmi tevékenységre vonatkozó eltérő szabályokat. A rendeletben és a kapcsolódó törvényben bevezetésre került az üzemeltetői biztonsági terv, mint a (nemzeti/európai) létfontosságú rendszerelemek teljes bemutatását tartalmazó dokumentum. [28]

1.3 Következtetések

A magyar jogalkotás részletesen, mélységében szabályozza a kritikus infrastruktúrákkal, illetve a létfontosságú rendszerelemekkel kapcsolatos előírásokat a kijelöléstől kezdve az üzemeltetésig, azonban az Európai Unió által kiadott jogszabályok implementálása a magyar jogrendbe lassan megy. Például az Európai Biztosság által 2005.11.17-én kiadott Zöld könyv csak a 2080/2008. (VI. 30.) Kormány határozatban került bevezetése a magyar jogszabályok közé. Kevesebb mint fél évre rá, 2008. december 8-án az Európai Bizottság kiadta a 2008/114/EK irányelvet a Zöld könyv utódjaként. Ezt az irányelvet a 1249/2010. (XI. 19.) Kormány határozattal fogadta be a törvénykezés. Megközelítőleg két év volt az implementálási időszak mindkét esetben, amelyet ebben a rohamosan változó világban nagyon hosszú időszaknak tartok.

A kutatási időszakom alatt, 2022.12.14-én az Európai parlement és az Európai Tanács kiadta 2022/2557 irányelvet a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről. Ezen irányelv nagy előrelépés a kritikus infrastruktúrák védelmével kapcsolatban. A magyarországi bevezetéssel kapcsolatban, tudomásom szerint az Országos Katasztrófavédelmi Főigazgatóság erre a célra létrehozott munkacsoportja foglalkozik, egyeztetéseket folynak az egyes ágazatok (szektorok) képviselőivel. Véleményem szerint az irányelv implementálása során kiemelt figyelmet kellene fordítani a kritikus infrastruktúrák fizikai és elektronikus védelmével kapcsolatos előírások, követelményrendszerek kialakítására, amelyek megfelelő alkalmazása esetén hozzájárulnak az egyes kritikus infrastruktúrák rugalmas ellenállóképességének növeléséhez.

Értekezésem további részében a kritikus infrastruktúráknál felmerülő veszélyforrásokat és kockázatokat ismertetem, valamint bemutatom az általam javasolt kockázatkezelési módszereket.

Az általam megvizsgált 2080/2008. (VI. 30.) Kormány határozatban szereplő feladatok, megfogalmazások, célkitűzések és elvek mind a mai napig alapul szolgálnak állami és gazdasági szektorban is a veszélyelhárítási és üzletmenet-folytonossági tervek elkészítésénél. Ezen felül a határozatban kifejtett veszélyforrások csoportosításának elve kitűnő vizsgálati és fejlesztési alapot adott a kutatásomnak.

2 VESZÉLYFORRÁSOK, KOCKÁZATOK

Ebben a fejezetben a kritikus infrastruktúrákkal kapcsolatos veszélyforrások azonosítását és csoportosítási rendszerét vizsgálom. A veszélyforrások megfelelő azonosítása és csoportosítása nélkülözhetetlen a kockázatkezelési folyamatban, és ez a kulcsa annak, hogy hatékonyan óvjuk kritikus infrastruktúráinkat.

A veszélyforrások azonosításával és csoportosításával kapcsolatos módszertan és eszközök mélyreható bemutatása után, a fejezet további részében a kockázatkezelést érintő folyamatokat fogom részletezni. A kockázatkezelés területe nagyon összetett, és a védelmi stratégiákat olyan sokféle tényező befolyásolhatja, hogy a kockázatkezelés minden egyes irányának megértése kulcsfontosságú a hatékony és kiegyensúlyozott védelmi rendszer kialakításához. [29]

2.1 Veszélyforrások azonosítása és osztályozása

Kutatómunkám során elsőként a magyarországi jogrendszerben kerestem olyan jogszabályt, amely a veszélyforrások csoportosításával foglalkozik. Az egyetlen ilyen jogszabály, a 2014. 03. 04-én hatályon kívül helyezett 2080/2008 (VI. 30.) Kormány határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. [21] Ezen jogszabály 1. számú melléklete a „Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról” 3.5. pontja foglalkozik a kritikus infrastruktúrákat veszélyeztető tényezők körével.

A forráskutatás során kigyűjtöttem a kritikus infrastruktúrák védelméhez kapcsolódó, nyilvánosan elérhető, PhD értekezéseket, amelyek között Bonya Tünde disszertációjában, valamint az egyik publikációjában találtam egy lehetséges megoldást a veszélyforrások csoportosítására. [30 pp. 17-19][31 pp. 215-216] Az értekezésében kifejti, hogy „Zöld könyv” (2080/2008 (VI. 30.) Kormány határozat melléklete) alapján újra gondolta az infrastruktúrák potenciális veszélyforrásainak besorolását.

A két itthoni forráson túl megvizsgáltam az Amerikai Egyesült Államok, a Nagy Britannia és a Kanada által kialakított, a veszélyforrásokkal foglalkozó, osztályozási gyakorlatait. [32][33][34] A nemzetközi kitekintés során a Kanadai Közbiztonsági Minisztérium által kiadott „Kockázatkezelési útmutató a kritikus infrastruktúra szektornak” kiadványban szereplő osztályozási rendszert találtam a legmegfelelőbbnek a felépítésének hasonlósága miatt. [34 pp. 36-37]

A csoportosítás során a kanadai osztályozásnál az alábbi elvet határozták meg:

- természeti veszélyek
    - meteorológiai veszélyek (viharok, áradás, extrém időjárás)
    - gleccserek, jéghegyek olvadása, mozgása
    - geofizikai veszélyek
    - tűzvész
    - biológiai veszélyek
- szándékos fenyegetések, magatartások
    - támadások (kémiai, biológiai, radiológiai, nukleáris, robbantásos, informatikai, hagyományos fegyveres támadások)
    - ellenséges támadás, háború
    - elektromágneses impulzus (EMP[14])
    - szabotázs
    - kémkedés (ipari és egyéb irányú)
    - bűncselekmények (például lopás, emberrablás, gyújtogatás, zsarolás)
    - társadalmi zavargások (lázadás, tüntetés, rendbontás)
    - sztrájk, munkaerő zavar
    - egyéb, nem rosszindulatú cselekmények amelyek hatással lehetnek az infrastruktúra működésére (határzár, szabályozási környezet változása)
- balesetek/műszaki veszélyek
    - balesetek (szállítás, veszélyes anyag szadba kerülés, tűz, robbanás)
    - műszaki meghibásodások (technikai-, mechanikai-, szoftver-, kezelői-, folyamat- és strukturális hiba)

A 2080/2008 (VI. 30.) Kormány határozat mellékletében, a Bonnyai Tünde PhD értékezésben és publikációjában kifejtett, valamint a Kanadai Közbiztonsági Minisztérium által kiadott „Kockázatkezelési útmutató a kritikus infrastruktúra szektornak” kiadványban szereplő osztályozási rendszerek ötvözésével megteremtettem a saját csoportosítási elvemet a veszélyforrások tekintetében [21][30 pp. 18-19][31 pp. 215-216][34 pp. 36-37][35]:

- katasztrófa jellegű események
    - természeti katasztrófák

[14] EMP: az EMP fegyver által létrehozott energiaimpulzus olyan erős elektromágneses mezőt generál, amely képes rövidre zárni az elektronikus berendezések széles körét, különösen a számítógépeket, műholdakat, rádiókat, radarvevőket és még a polgári közlekedési lámpákat is.

        - hidrológiai események: ár- és belvíz (Gatwick repülőtér, 2013) [36], villámárvíz,
        - meteorológiai események: viharok, havazás, jégeső, extrém hőmérséklet (Sandy hurrikán, 2012) [37]
        - geológiai események: tsunami (Haiti, 2010; Fukusima, 2011) [38][39], földcsuszamlás, földrengés (Törökország 2023) [40], vulkánkitörés (Izland, 2010) [41]
        - tűzvészek: erdőtűz, városi tűz, földrengés utáni tűzvész (Tokió 1923) [42]
        - napkitörések (1989; Starlink, 2022) [43]
    - ipari katasztrófák, amelyet technológiai/tervezési hiba (St. Francis gát, 1928; Csernobil, 1986) [44][45], helytelen emberi beavatkozás (Csernobil 1986; Fukusima, 2011) [39][45], vagy baleset miatt következtek be (Ohio vonatbaleset, 2023) [46].
- civilizációs eredetű veszélyek
    - űrobjektum becsapódása [47]
    - globális felmelegedés okozta katasztrófák (Uttarakhand-i árvíz, India, 2021) [48 p. 39-40][49]
    - humán- és állategészségügyi, vagy növényeket érintő járványok, (Covid-19, pestis, H5N1, veszettség, lisztharmat, sáskajárás) [50]
    - migrációs hullámok: háborús helyzet, éhínség miatt (Ukrajna, Afganisztán, Szíria) [51]
    - infrastruktúrák teljesítőképességének kimerülése [52]
- szándékos magatartás okozta veszélyek
    - támadások, terrorcselekmények (Madrid, 2014; London, 2015) [53 p.151] [54 p. 27]
    - fegyveres konfliktussal, háborúkkal kapcsolatos veszélyek (Zaporizzsja)
    - kibertámadások, vírusok (Stuxnet) [55 p. 1499][56]
    - társadalmi eredetű események: sztrájk, tüntetés (Budapest, 2006), blokád (Budapest, 1990)
    - kémkedés, szabotázs (Északi áramlat, 2022) [57]
    - gazdasági, politikai okkal elkövetett visszaélések
    - nem rosszindulatú veszélyek: határzár; jogszabály, irányelv változás

A továbbiakban, a beléptető rendszerek műszaki és logikai követelményrendszerének meghatározásához, a szándékos magatartás okozta veszélyek bekövetkezésének valószínűségét és annak hatásait fogom vizsgálni.

Terror cselekmények, fegyveres támadások, mint veszélyforrás

A kritikus infrastruktúrákat érintő terrorcselekmények kockázatával a 2004-es madridi vonatrobbantásokat követően kezdtek el foglalkozni az Európai Unióban. Az azóta eltelt időszakban számos terrorcselekmény történt, amelyek fő *„célja nem a létesítmények, közszolgáltatók működésképtelenné tétele volt, hanem a nagyszámú áldozaton keresztül a lakosság jelentős részében félelem, pánik előidézése”.* [58 p. 6]

Az Institute for Economics and Peace által készített Global Terrorism Index megmutatja az egyes országok terrorfenyegetettségének helyzetét. Az index (pontszám) számítása nemcsak a haláleseteket, hanem a terrorizmusból származó incidenseket, túszokat és sérüléseket is figyelembe veszi, ötéves időszakra súlyozva. 2022. év alapján a világ összes országát tekintve Afganisztán, Burkina Faso, Szomália, Európát tekintve Törökország, Görögország, Franciaország volt az első három a listán. Magyarország terrorizmusnak való kitettségének indexe 0.00 az 2023. évi kiadása alapján, ami azt jelenti, hogy nem történt a terrorcselekmény az elmúlt éveben hazánkban. [59][60]. Ezzel szemben a Belügyminisztérium Bűnügyi Statisztikai Rendszerében[15] 2019-ben 4 darab, 2020-ban 15 darab, 2021-ben 8 darabt és 2022-ben 11 darab esetet jelöltek meg terrorcselekménynek.

A fegyveres támadásokat kiindulási helyük szerint két csoportra bonthatjuk, a kívülről indulókra és a belülről indulókra. Mindkét támadással kapcsolatos kockázatokat az őrség folyamatos képzésével, a beléptetési szabályok meghatározásával, a megfelelő fizikai védelmi rendszerekkel és a zsilipszerű beléptető rendszerrel csökkenthetjük.[61] A beléptetés során végzett személy- és csomagvizsgálattal megelőzhető a védett zónába történő lőfegyver bevitele. Azonban figyelemmel kell lenni azokra az esetekre is, amikor a fegyver már a kritikus infrastruktúra területén belül található védelmi céllal, például a Fegyveres Biztonsági Őrség (FBŐ)[16] által [62]. Ebben az esetben a kockázat csökkentését a védelmi zónák beléptetési szabályozásával, zsiliprendszer kialakításával, valamint az

[15] https://bsr.bm.hu/

[16] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról. *„Az Országgyűlés az állam működése, illetőleg a lakosság ellátása szempontjából* ***kiemelkedően fontos létesítmények és tevékenységek****, ... jogellenes cselekményekkel szembeni fokozottabb védelme...”*

egyes védelmi zónáknál lövedékálló felületek létrehozásával maximalizálhatjuk. Természetesen a rendszeres pszichológiai vizsgálat és az őrség tagjainak háttérellenőrzése is elengedhetetlen. [63]

Fegyveres konfliktussal, háborúkkal kapcsolatos veszélyek

Az Európai Unióban háborús cselekménnyel összefüggésben több kritikus infrastruktúra megsérül a 2000-es években. 2000-2010 közötti időszakban a Grúziában és Koszovóban alakultak ki fegyveres konfliktusok, amely során közlekedési, energiaellátási és távközlési infrastruktúrák sérültek, vagy semmisültek meg.[64] Ezt követően 2014-ben majd 2022-ben Oroszország katonai műveleteket indított Ukrajna ellen. A művelet során a kritikus infrastruktúrák elleni célzott támadásokban többször összeomlott már az ukrán energia és távközlési hálózat is. Ezek hatásai nem terjedtek át a többi tagállamra, azonban az Északi áramlat gázvezetéket ért szabotázs akció már hatással volt az Európai Unió több tagállamára az orosz gáztól való függőségi viszony miatt.

A háborúkkal kapcsolatos veszélyek a hadtudomány kategóriába tartoznak, továbbá a háborúk kialakulása és bekövetkezése több összetett tényezőtől függ, amelyek között geopolitikai, politikai, gazdasági és más fontos elemek találhatók, ezért az értekezés keretében az ilyen veszélyek bekövetkezésének valószínűsége nem határozható meg.

Kibertámadások, szabotázsok és visszaélések veszélye

A támadás kiindulása szempontjából lehet külső, vagy belső elkövető által elkövetett támadás. A külső kibertámadások jellemzően DDoS[17], malware[18], ransomware[19] támadások, amelyek ellen a legegyszerűbb védekezési módszer a hálózatok szeparációja, azaz dedikáltan külső és belső hálózat létrehozása összeköttetés nélkül. [5][55][65][66 p. 47-49]

A belülről induló támadás esetén az elkövető vagy a kritikus infrastruktúra alkalmazottja, vagy beszállítója és rendelkezik hozzáféréssel a belső hálózathoz. [67 p. 101] A támadást módszere alapján háromféle csoportba rendeztem:

- visszaélés a jogosultsággal: fájlok, rendszerek módosítása, törlése

[17] DDoS (Distributed Denial of Service): túlterheléses kibertámadási forma.
[18] malware: olyan kártékony szoftver vagy program, amely célja a számítógépek, hálózatok vagy eszközök megsértése, károsítása vagy felhasználói információk megszerzése.
[19] ransomware (zsarolóvírus) olyan kártékony szoftver, amely célja a felhasználók fájljainak titkosítása és váltságdíj követelése a fájlok visszaállításáért.

- adatlopás: érzékeny információk, adatok lopása, szivárogtatása
- szabotázs: szándékos károkozás a rendszerekben, amely akár fizikai károkat is okozhat.

A belső elkövetők motivációi változatosak lehetnek, és az egyéni körülményektől függenek. Néhány lehetséges motivációs tényező a következők:

- pénzügyi okok: anyagi előnyöket remélnek a támadástól, például az adatok értékesítéséből vagy zsarolásból
- személyes bosszú vagy elégedetlenség
- ideológiai vagy politikai okok
- külső motivációk: zsarolás, social engineering[20] [68 p. 28]

A belső elkövetők elleni védekezés

- jogosultságkezelési rendszer folyamatos felülvizsgálata
- portvédelmi programok használata: pl. DLP[21]
- csomag és személy vizsgálat (adathordozók)
- biztonsági átvilágítás kritikus pozíciókban lévő munkatársaknál
- hálózat rétegezése és elszeparálása: irodai, biztonsági, üzemeltetési

Összefoglalás

A fejezetben áttekintést adtam a kritikus infrastruktúrákkal kapcsolatos szándékos magatartás okozta veszélyekről, amelyek különböző területeken nyílvánulhat meg, mint például a kiberbiztonság, a fizikai támadások, a terrorizmus vagy a gazdasági károkozás. Az ilyen veszélyforrások komoly fenyegetést jelenthetnek a társadalmi stabilitásra és a gazdasági működésre.

A veszélyforrások azonosítását követően, a következő részben a kockázatok értékelési módszereinek és a kockázatkezelés módszereinek bemutatására kerül sor.

2.2 A kockázatok értékelési módszerei

A kockázatok azonosítása után a következő lépés a kockázatértékelés, egy olyan mélyreható elemzési folyamat, amely lehetővé teszi számunkra, hogy megértsük az

[20] A social engineering támadási módszer a manipuláció és pszichológiai befolyásolás eszközeit használja, hogy megtévessze az embereket, és rávegye őket arra, hogy kiszolgáltassák érzékeny információikat vagy hozzáférési jogosultságaikat.
[21] DLP (Data Leak Protection) egy olyan technológia és módszer, amelynek célja az érzékeny adatok védelme és a nem kívánt adatszivárgás megelőzése

azonosított kockázatok valószínűségét és súlyosságát.[69][70 p. 21-27] Ez a folyamat alapvetően két módszerrel végezhető el: **kvalitatív** és **kvantitatív** módszerekkel, amelyek különböző szempontokból közelítenek a kockázatértékeléshez.[30][71]

A **kvantitív** kockázatértékelési eljárás célja a kockázatok számszerűsítése és hierarchizálása. Az eljárás segítségével a kritikus infrastruktúra tulajdonosai és/vagy üzemeltetői képesek objektív, numerikus adatokon alapuló döntéseket hozni a kockázatkezelési stratégiáikról.[72 p. 63-64] Az alábbiakban összefoglalom a kvantitív kockázatértékelési eljárás lépéseit, és példákkal illusztrálva az egyes fázisokat.

1. **Kockázati tényezők azonosítása**: Első lépésként meg kell határozni, hogy mely kockázatok jelenthetnek fenyegetést a kritikus infrastruktúrára. Például egy hőerőmű esetén a hőtermelést végző gépek, irányító berendezések, akár szándékos cselekmény általi meghibásodása.
2. **Kockázatok mértékének becslése**: A kockázatok mértékét a bekövetkezésük valószínűsége és a bekövetkezésük esetén bekövetkező veszteség nagysága alapján becsülhetjük meg. Például, ha egy hőerőműnél nagy a hőtermelőgépek meghibásodásának valószínűsége, és a meghibásodás jelentős kiesést okoz a termelésben, akkor ez a kockázat nagy mértékűnek minősül.
3. **Kockázatok rangsorolása**: A becsült mérték alapján a kockázatokat rangsorolni lehet. Például egy hőerőmű esetében a hőtermelőgépek meghibásodása nagyobb kockázatot jelenthet, mint egy részleges rendszerleállás, ha a gépek meghibásodásának valószínűsége és a bekövetkezés esetén bekövetkező veszteség nagysága nagyobb.
4. **Kockázatkezelési stratégiák kidolgozása**: A rangsorolt kockázatok alapján kidolgozhatók a kockázatkezelési stratégiák. Például, ha a gépek meghibásodása jelenti a legnagyobb kockázatot, akkor a vállalat befektethet karbantartási programokba, pótalkatrész-készletekbe, vagy a gépek modernizálásába.

Az eljárás előnye, hogy segít a szervezetnek racionális döntéseket hozni a kockázatkezelés területén, és lehetővé teszi a korlátozott erőforrások hatékony elosztását. A kvantitatív módszerek közé tartoznak a statisztikai elemzések, a szimulációs modellek, és az olyan technikák, mint a hibafa-analízis[22] vagy a Monte Carlo-szimuláció[23]. Azonban

[22] A hibafa analízis a hibák okainak feltárására és megelőzésére szolgáló módszer, amely az események gyökérokkal történő elemzésére és a megfelelő intézkedések meghozatalára összpontosít.
[23] A Monte Carlo szimuláció egy számítási módszer, amely a véletlenszerű változók használatával modellezi és szimulálja a valós világ különböző jelenségeit vagy folyamatait. Ez a módszer nagy

fontos megjegyezni, hogy a kvantitív kockázatértékelési eljárás eredményei a becslések és feltételezések pontosságától függenek, ezért a kockázatkezelési döntések meghozatalakor figyelembe kell venni a becslések és a modellezés bizonytalanságait is.

A **kvalitatív** kockázatértékelés a kockázatok relatív jelentőségét és hatását vizsgálja. Ez a megközelítés gyakran használatos olyan helyzetekben, ahol a kockázati tényezők nem számszerűsíthetők könnyen vagy egyértelműen.[73] A kvalitatív módszerek közé tartozik az interjúk és műhelybeszélgetések alkalmazása, a szakértői vélemények gyűjtése, és a kockázatok rangsorolása aszerint, hogy mennyire valószínűek és mennyire súlyosak lehetnek a hatásaik. Az alábbiakban összefoglalom a kvalitatív kockázatértékelési módszer lépéseit, és példákkal illusztráljuk az egyes fázisokat.

1. **Kockázati tényezők azonosítása**: Az első lépésben a tulajdonosnak/üzembentartónak azonosítania kell a kritikus infrastruktúrák működését befolyásoló potenciális kockázatokat. Például egy energetikai hálózat számára a kockázatok között lehet a természeti katasztrófák (pl. földrengés, árvíz), a szándékos emberi beavatkozások (pl. terrorizmus, kibertámadás), vagy a technológiai hibák (pl. rendszermeghibásodás).
2. **Kockázatok értékelése**: A kockázatok értékelése során a tulajdonosnak/üzembentartónak meg kell határoznia a kockázatok bekövetkezésének valószínűségét és potenciális hatásait. Például egy természeti katasztrófa esetén meg kell határozni, hogy milyen valószínűséggel következik be, és milyen hatása lehet a kritikus infrastruktúrára.
3. **Kockázatok rangsorolása**: A kockázatokat a bekövetkezésük valószínűsége és a potenciális hatások alapján rangsorolhatjuk. Például, ha egy energetikai hálózat esetében a természeti katasztrófák nagyobb valószínűséggel következnek be és nagyobb hatást gyakorolnak, mint a technológiai hibák, akkor a természeti katasztrófák nagyobb prioritást kapnak.
4. **Kockázatkezelési stratégiák kidolgozása**: A rangsorolt kockázatok alapján kidolgozhatóak a kockázatkezelési stratégiák. Például, ha a természeti katasztrófák jelentik a legnagyobb kockázatot egy energetikai hálózat számára,

mennyiségű véletlenszerű adat generálásával és ismételt próbálkozással működik, majd ezek alapján statisztikai eredményeket és valószínűségi becsléseket hoz létre.

akkor a tulajdonosnak/üzembentartónak olyan stratégiákat szükséges kidolgoznia, amelyekkel ezek a kockázatok csökkenthetők, mint például katasztrófaelhárítási tervek készítése, redundáns rendszerelemek kialakítása, vagy az kritikus infrastruktúra rugalmas ellenállóképességének növelése.

A kvalitatív kockázatértékelési módszer előnye, hogy nagyobb hangsúlyt fektet a kockázatok minőségi aspektusaira, beleértve a kockázatok természetét, forrását és lehetséges hatásait. Ez segíthet a szervezetnek abban, hogy jobban megértsék a kockázatokat, és olyan kockázatkezelési stratégiákat dolgozzanak ki, amelyek hatékonyan kezelik azokat. Ugyanakkor fontos megjegyezni, hogy mivel a kvalitatív kockázatértékelés szubjektív, a különböző személyek eltérően értékelhetik a kockázatokat, és a kockázatkezelési döntések megkérdőjelezhetőek lehetnek.

Mindkét módszernek megvannak a maga előnyei és hátrányai, és gyakran a legjobb eredményeket akkor érhetjük el, ha kombináljuk őket. A lényeg, hogy a kiválasztott módszernek megfeleljen a kockázatkezelési céljainknak, és képes legyen értékes információt szolgáltatni a döntéshozatalhoz.

2.3 Kockázatkezelési módszerek, elvek

A kockázatkezelés célja a lehetséges veszélyek és kockázatok azonosítása, értékelése és hatékony kezelése.[74 p. 351] A kockázatkezelés során a kritikus infrastruktúrák tulajdonosai/üzemeltetői és a kockázatkezeléssel foglalkozó szakértők olyan intézkedéseket határoznak meg, amelyek csökkentik a kockázatok bekövetkezésének valószínűségét, illetve minimalizálják az esetleges károk mértékét.[32]

A kockázatkezelés négy fő irányba csoportosítható, amelyek segítenek az esetleges kockázatok megfelelő kezelésében. Az első irány az **elkerülés**, amely arra törekszik, hogy a kockázatos tevékenységeket vagy helyzeteket elkerüljék vagy minimalizálják. A második irány a **csökkentés**, amely a kockázatok mértékét csökkenti a megfelelő intézkedések és biztonsági óvintézkedések alkalmazásával. A harmadik irány az **áthárítás**, amely során a kockázatokat és felelősséget más félre vagy biztosítóra terelik át. Végül, a negyedik irány az **elfogadás**, amely esetén a szervezetek tudatosan vállalnak bizonyos kockázatokat a potenciális előnyök vagy lehetőségek érdekében. A következőkben részletesebben elemzem a kockázatkezelési irányokat.

A kockázatok elkerülése

A kockázat elkerülésének módszere az, hogy a kockázatos tevékenységet vagy helyzetet elkerüljük, vagy elkerüljük a kockázatos cselekedetet. Ez azt jelenti, hogy a tevékenységet vagy helyzetet, ami kockázatot hordoz, egyszerűen nem hajtjuk végre. A kockázat elkerülése azonban nem mindig lehetséges, különösen akkor, ha az adott tevékenység elengedhetetlen az üzleti folyamatokhoz vagy a szolgáltatásokhoz.

A kockázat elkerülésének egyik módja lehet az alternatív megoldások keresése, amelyek ugyanazt a célt szolgálják, de kevesebb kockázattal járnak. Például, ha egy adott tevékenység bizonyos kockázatokkal jár, akkor meg lehet keresni azokat a helyettesítő tevékenységeket, amelyek ugyanazt a célt szolgálják, de kevesebb kockázatot hordoznak. A kockázat elkerülése azonban nem mindig lehetséges, és ha nem lehet alternatív megoldást találni, akkor lehet, hogy más kockázatkezelési módszereket kell alkalmazni, például a kockázat átvállalását vagy csökkentését. A kockázatkezelési stratégiák közötti választás a konkrét körülményektől függ, és általában a kockázatokkal kapcsolatos kockázatértékeléssel kezdődik.

A kockázatok csökkentése

A kockázatok csökkentése a kockázatkezelés másik stratégiája, amely azt jelenti, hogy a kockázatokat csökkentjük, de nem szüntetjük meg teljesen. A kockázatok csökkentése lehetőséget ad arra, hogy a kockázatokat olyan szintre csökkentsük, amely elfogadható az adott szervezet számára.

A kockázatok csökkentésének folyamata több lépésből áll. Először is meg kell határozni a kockázatokat, majd értékelni kell azokat annak meghatározása érdekében, hogy melyik kockázat a legnagyobb és melyik a legkisebb. Ezután meg kell tervezni és végrehajtani azokat a tevékenységeket, amelyek csökkenthetik a kockázatokat.

A kockázatok csökkentésének különböző módszerei közé tartozik például az eszközök és rendszerek javítása, a személyzet képzése és oktatása, valamint az operációs eljárások és irányelvek javítása. A kockázatok csökkentése általában hosszabb időt vesz igénybe, mint a kockázatok elkerülése vagy elfogadása, és általában több erőforrást igényel.

A kockázatok csökkentése azonban lehetővé teszi az adott szervezet számára, hogy hatékonyabban kezelje a kockázatokat és csökkentse az esetleges károk mértékét, amennyiben mégis bekövetkeznének. A kockázatok csökkentése fontos része a kockázatkezelésnek, és hozzájárulhat az adott szervezet biztonságának növeléséhez és a kritikus üzleti folyamatok folytonosságának biztosításához.

A kockázatok áthárítása

Az áthárítás a kockázatkezelés egy fontos és stratégiai módszere, amely széles körben alkalmazható a különböző iparágakban és szervezetekben. A fő célja a kockázatok terheinek és felelősségének átvitele más felekre vagy biztosítókra, akik hajlandóak és képesek kezelni és elviselni ezeket a kockázatokat.

Az áthárítás során a **felelősség megosztása** a kockázatvállalók között a hangsúly. Ez lehetőséget teremt arra, hogy a felelősség ne csak egyetlen félre háruljon, hanem megoszlik több fél között, akik jobban felkészültek vagy képesek kezelni a kockázatokkal járó következményeket. Ezáltal a kockázatok terhei és felelőssége egyenlőbbé válik és csökkentheti a kockázatvállaló egyéni terheit.

A **pénzügyi védelem** egy másik fontos célja az áthárításnak. Amikor egy szervezet áthárítja a kockázatokat más felekre vagy biztosítókra, azzal pénzügyi biztosítékot nyújthat magának a potenciális károk vagy veszteségek esetére. A biztosítók vagy más átvállaló fél képes lehet fedezni a károk okozta pénzügyi terheket, amelyeket a kockázatvállaló egyedül nehezen vagy teljes mértékben tudna elviselni.

Az áthárítás másik előnye a **szakértői segítség igénybevétele**. Biztosítók, kockázatkezelési szolgáltatók vagy más szakértők széleskörű ismeretekkel és tapasztalattal rendelkezhetnek a kockázatkezelés területén. Az áthárítás lehetőséget nyújt arra, hogy a szervezetek igénybe vegyék ezen szakértők segítségét, akik segíthetnek a megfelelő kockázatkezelési stratégiák kidolgozásában és a kockázatok hatékony kezelésében.

Az áthárítás továbbá lehetővé teszi a **kockázatok diverzifikációját**. Amikor a kockázatokat több félre osztják, csökkenthető az egyes kockázatokra való kitettség mértéke. Ez azt jelenti, hogy a kockázatvállalók nem csak egyetlen kockázatforrásra vagy helyzetre támaszkodnak, hanem szélesebb körű kockázatportfólióval rendelkeznek. Ennek eredményeként a kockázatok diverzifikációja növelheti a kockázatkezelés hatékonyságát és csökkentheti a kockázatok általános kockázatát.

A kockázatok elfogadása

A kockázat elfogadás a negyedik irány a kockázatkezelési stratégiák között. Ebben az esetben az üzemeltető/tulajdonos úgy dönt, hogy elfogadja a fentmaradó kockázatot, és nem hajlandó, vagy nem gazdaságos tenni annak csökkentése érdekében. Ez a megközelítés általában akkor alkalmazható, ha a kockázat kis mértékű, és az esetleges veszteség vagy káros hatás elfogadható a szervezet számára.

Az elfogadás lehetősége lehetőséget ad a szervezetnek, hogy fókuszáljon más prioritásokra, és a figyelmét a kockázatok kezelésére szoruló területekről áthelyezze olyan területekre, amelyek fontosabbak vagy sürgősebbek. Az elfogadás döntése azonban nem jelent inaktivitást, hanem azt, hogy a szervezet tudatában van a kockázatnak, és kész arra, hogy az esetleges következményeket elviselje.

A kockázat elfogadása nem azt jelenti, hogy a szervezet nem tesz semmit a kockázat kezelése érdekében. A szervezetnek továbbra is fel kell készülnie az esetleges károkra, és olyan intézkedéseket kell hoznia, amelyek minimalizálják az esetleges veszteségeket. Ebben az esetben a szervezetnek mérlegelnie kell a kockázatot és az elfogadás előnyeit, hogy eldöntse, hogy az elfogadás a legmegfelelőbb megoldás-e a konkrét kockázatra.

2.4 Veszélyhelyzeti tervek készítése

A kockázatkezelés során meghatározott maradék kockázatok kezelésére veszélyhelyzeti tervek készülnek.[75 p. 56-64] Ezek a tervek olyan stratégiai dokumentumok, amelyek meghatározzák a váratlan helyzetekre adandó válaszlépéseket és intézkedéseket a kritikus infrastruktúrák védelme érdekében. [35]

A veszélyhelyzeti tervben az általános bevezetőt követően bemutatásra kerül kritikus infrastruktúra jellege, a fontossága (nemzeti, ECI) és a kapcsolódó kockázati tényezők. Ezt követően ismertetni kell a vészhelyzeti szcenáriókat és az ezekre adandó válaszlépéseket, figyelembe véve a kritikus infrastruktúra specifikus jellemzőit. A veszélyhelyzeti terveknek részletesen le kell írniuk a kritikus infrastruktúrák működésének fenntartásához, helyreállításához és védelméhez szükséges intézkedéseket és eljárásokat.

A veszélyhelyzeti terveknek tartalmazniuk kell a kritikus infrastruktúrával kapcsolatos felelősségi feladatokat és szerepköröket, beleértve a vészhelyzeti szervezeteket, a kommunikációs csatornákat és a döntéshozatali mechanizmusokat. Fontos, hogy a tervek konkrét lépéseket és időkereteket határozzanak meg az intézkedések végrehajtására, valamint definiálva legyenek a vészhelyzetek alatt és után szükséges teendők. Az egyes területekre és folyamatokra vonatkozóan a veszélyhelyzeti terveknek részletes útmutatást kell tartalmazniuk. Ez magában foglalhatja az élet- és vagyonbiztonsági intézkedéseket, a kommunikációs és információs rendszereket, az erőforrások és ellátási láncok kezelését, valamint a helyreállítási folyamatokat és tesztelési eljárásokat.

Az éles és az elméleti gyakorlatok rendkívül fontosak a veszélyhelyzeti tervek hatékonyságának és alkalmazhatóságának ellenőrzésére. A tervek gyakorlati alkalmazása lehetővé teszi a szereplők számára, hogy megismerjék és gyakorolják a vészhelyzeti eljárásokat, valamint az esetleges hiányosságokat és fejlesztési lehetőségeket azonosítsák.

A veszélyhelyzeti tervek készítése és fenntartása ciklikus folyamat, amely időről időre felülvizsgálatot és frissítést igényel. Az új kockázati tényezők és technológiai fejlemények figyelembevételével a terveknek aktuálisnak és alkalmazkodóképesnek kell lenniük a változó körülményekhez.[76 p. 28-36]

Összességében elmondható, hogy a veszélyhelyzeti tervek készítése és rendszeres felülvizsgálata létfontosságú a kritikus infrastruktúrák hatékony védelmi rendszereinek kialakításához. Ezek a tervek biztosítják a gyors és koordinált válaszlépéseket váratlan helyzetekben, valamint hozzájárulnak a kritikus infrastruktúra üzemszerű működési körülményeinek fenntartásához a legmagasabb szinten.

2.5 Kockázatkezelési folyamatok rendszeres felülvizsgálata és frissítése

A kritikus infrastruktúra tulajdonosai és üzemeltetői számára rendszeres kockázatkezelési folyamatok felülvizsgálata lehetővé teszi az újonnan felmerült kockázatok azonosítását és kezelését, amelyek a technológiai fejlődés, társadalmi változások és környezeti hatások következtében jelentkezhetnek. Ez a felülvizsgálat lehetővé teszi a szervezetek számára, hogy felmérjék az új kockázatokat és szükséges intézkedéseket hozzanak a kezelésük érdekében. A felülvizsgálat továbbá biztosítja, hogy a kockázatkezelési stratégiák és politikák relevánsak és hatékonyak maradjanak a változó környezetben. A változó kockázati tényezők, a kockázatkezelési technikák fejlődése és a szervezeti változások mind befolyásolhatják a stratégiák hatékonyságát. Emiatt a felülvizsgálat lehetőséget ad a szervezetek számára, hogy azonosítsák a változásokat és szükséges módosításokat hajtsanak végre a kockázatkezelési stratégiákban. Az ilyen felülvizsgálat során azonosított új veszélyforrások és kockázatok pedig segítenek a szervezetnek felkészülni a váratlan eseményekre.

2.6 Következtetések

A kritikus infrastruktúrákkal kapcsolatos veszélyforrások azonosítása és csoportosítása, valamint a kockázatkezelési folyamat részletezése fontos lépéseket jelent a kritikus infrastruktúrák hatékony védelmi rendszerének kialakításában. Az általam meghatározott kockázati osztályozási rendszer lehetővé tette a veszélyforrások strukturált és módszeres azonosítását és csoportosítását, míg a kvantitatív és kvalitatív kockázatértékelési módszerek együttes alkalmazása lehetővé tette a kockázatok objektív és szubjektív elemekkel történő értékelését.

A kockázatkezelés négy iránya - elkerülés, elfogadás, csökkentés és átvállalás - olyan stratégiai lehetőségeket kínál a szakemberek számára, amelyekkel a kritikus infrastruktúrák védelmi rendszereinek alkalmazkodó és ellenálló képessége növelhető.

A veszélyhelyzeti tervek kiemelt szerepet játszanak a maradék kockázatok kezelésében, és biztosítják a hatékony válaszlépéseket vészhelyzetekben. Ezek a tervek olyan stratégiai intézkedéseket és eljárásokat foglalnak magukban, amelyek biztosítják a kritikus infrastruktúrák folyamatosságát és fenntartását a váratlan helyzetekben is.

A kutatásom során megállapítottam, hogy a kockázatok felismerése és hatékony kezelése kiemelten fontosságú a kritikus infrastruktúrák védelmi rendszereiben, legyenek azok informatikai, fizikai, elektronikai vagy személyi jellegűek.

Az veszélyforrások azonosítása és a kockázatok értékelése alapján képesek vagyunk felmérni azokat a hatásokat, amelyek kritikusak lehetnek az infrastruktúra működésére. A következő fejezetben részletesebben tárgyalom ezt a témát, bemutatva a védelmi zónák kialakításának módszereit és a kritikus infrastruktúrák védelmi rendszereinek lépéseit.

3 VÉDELMI ZÓNÁK MEGHATÁROZÁSA

Az Európai Kritikus Infrastruktúra Védelmi Program (EPCIP)[24] olyan stratégiai keretrendszert biztosít az európai kritikus infrastruktúrák védelmére, amely hangsúlyozza a kritikus infrastruktúrák jelentőségét és hatását a társadalomra és a gazdaságra, valamint meghatározza azok meghibásodásának, megtámadásának és megsemmisülésének következményeit. A 2080/2008. (VI.30.) Kormány határozattal implementálásra került az Európai Uniós Zöld Könyv a magyarországi jogrendbe. Ezen jogszabályban került kihirdetésre a *„Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról”*, melynek 3.2. pontja foglalkozik a következmény alapú kritikussági megközelítéssel.[21]

Értekezésem jelen fejezetében kifejtem, hogyan használható az EPCIP kritikusság alapú megközelítése védelmi zónák meghatározására, és milyen előnyöket kínál a zónabesorolás a beléptető rendszerek tervezése és implementálása során.

A kritikusság alapú megközelítés az infrastruktúrák helyiségeinek rangsorolására és védelmének priorálására összpontosít. Első lépésként a „worst-case”[25] modell felhasználásával meghatároztam az adott zóna kritikusságát, azaz a legrosszabb esetben milyen hatással lehet az illetéktelen belépés a kritikus infrastruktúra működésére, és ennek a hatásnak mekkora lehet az időbeli és térbeli kiterjedése. Ez magában foglalja a szándékos külső, vagy belső támadásokat, a védelmi rések kihasználását és más potenciális veszélyeket. Az ilyen elemzések alapján kialakított védelmi zónák biztosítják, hogy még a legkedvezőtlenebb körülmények között is fenntartható legyen a kritikus infrastruktúra működése, biztonsága, valamint helyreállíthatósága. [76 p. 28-36][77][78]

Az infrastruktúrák helyiségeinek kritikusságának értékelése alapján azokat a helyiségeket, amelyekben a sebezhetőség hatása nagyobb, magasabb védelmi zónába soroltam. Az így létrehozott azonosítási és besorolási metodika három előnyt kínál:

1. a kritikusság alapú megközelítés lehetővé teszi a korlátozott erőforrások hatékony felhasználását, így a magasabb védelmi szintű zónákban a védelmi intézkedések és erőforrások koncentráltabbak lehetnek.
2. a kritikusság alapú megközelítés lehetővé teszi a fizikai és elektronikai védelmi rendszerek összehangolt üzemeltetését és a hatékonyabb kockázatkezelést. Az

[24] COM/2005/0576 – Zöld Könyv – A létfontosságú infrastruktúrák védelmére vonatkozó Európai programról

[25] A worst-case modell a legrosszabb lehetséges forgatókönyvet veszi alapul, és a kockázatkezelés során a maximális kockázati hatásokat és következményeket vizsgálja.

infrastruktúrák kritikusságának alapos értékelése segít azonosítani azokat a sebezhetőségeket és gyenge pontokat, amelyekre kiemelt figyelmet kell fordítani a biztonsági zónák kialakításakor. Ez lehetővé teszi a célzott védelmi intézkedések kidolgozását, például fokozottabb ellenőrzéseket, redundáns rendszereket vagy speciális védelmi protokollokat.

3. a kritikusság alapú megközelítés összhangban van a fenyegetés dinamikájával és a változó kockázati helyzettel. Az infrastruktúrák környezete és a veszélyforrások folyamatosan változnak, új fenyegetések jelenhetnek meg. A kritikusság alapú megközelítés lehetővé teszi a rugalmas és dinamikus biztonsági zónák meghatározását, amelyek alkalmazkodnak az aktuális kockázati helyzethez és a fenyegetésekhez.

Összességében a kritikusság alapú megközelítés és a „worst-case" modell kombinálása értékes alapot biztosított a kritikus infrastruktúrák védelmi zónainak kialakításában. A következőkben bemutatom az általam meghatározott védelmi zónákat, azok jellemzőit és néhány lehetséges kockázatot.

3.1 0. zóna

A **0. védelmi zónába** történő illetéktelen belépéssel kapcsolatban nincs ismert sérülékenység, ami azt jelenti, hogy a kritikus infrastruktúra működésében nem lép fel üzemzavar, az alapvető szolgáltatások zavartalanul működnek. Az illetéktelen belépés „hatása" csak a kritikus infrastruktúra 0. védelmi zónájára korlátozódik. Az események kezelése a legtöbb esetben helyi erőforrásokkal (biztonsági személyzet) megoldható.

A 0. védelmi zónába az alábbi helyiségeket soroltam:

- **parkoló**: fizikai leválasztás szükséges a vendég és a dolgozói parkoló közé. A parkolóba történő behajtás engedélyezése belépőkártyával, rendszámazonosítással, vagy őrszolgálat által is történhet. Lehetőség van fizikai akadályokkal is védeni az illetéktelen behajtást, például sorompókkal, bollard[26]-okkal.
- **közösségi terek, előcsarnok**: az épület azon zónája, ahol az érkező vendégek fogadása történik. A területet videómegfigyelő rendszer és őrszolgálat tartja ellenőrzés alatt. Tilos olyan védtelen hálózati végpont elhelyezése, amely a belső, vagy a biztonsági hálózathoz kapcsolódik.

[26] bollard: olyan süllyedő oszlop, amely meggátolja az áthajtást

- **vendég tárgyalók**: az előcsarnokból nyíló olyan helyiségek, ahol a külsős partnerekkel megbeszélés folytatható. Tilos ebben a helyiségben is olyan végpont elhelyezése, amely a belső hálózathoz kapcsolódik.
- **vendég mosdók, étterem, büfé**: olyan egyéb helyiségek, amelyek az előcsarnokból nyílnak.

Lehetséges kockázatok és kezelésük:

- a kritikus infrastruktúrát körülvevő területre történő behatolás és kísérlete:
    - a peremeterek védelme fizikai eszközökkel: kerítésrendszerek, falazatok, GYODA[27]
    - a peremeterek védelme elektronikus vagyonvédelmi rendszerekkel: kerítésvédelemi-, videómegfigyelő- és behatolásjelző rendszerek alkalmazása.
    - a peremeterek körül járőrtevékenység megszervezése belső vagy külső szolgáltató által biztosított biztonsági személyzettel.
    - szituációs gyakorlatokkal történő felkészülés
- behajtási kísérlet a kritikus infrastruktúra területére:
    - fizikai védelmi akadályok használata: sorompó, biztonsági kapu, bollard, wedge barrier[28]. [79]
    - elektronikai azonosítórendszerek használata: rendszám azonosítás, személy azonosítása belépőkártyával, biometrikus azonosítóval.
    - őrszolgálat/portaszolgálat megszervezése a behajtási jogosultságok ellenőrzésére.
    - a behajtással és parkolással kapcsolatos szabályrendszerek kialakítása: ki, mikor, hogyan hajthat be a területre, vendégek kezelése.
- belépési kísérlet a kritikus infrastruktúra területére:
    - fizikai védelmi akadályok használata: forgókapu, portaépület
    - elektronikai vagyonvédelmi rendszerek használata: beléptető rendszer a dolgozók azonosítására; kaputelefon az érkező vendégek számára; videómegfigyelő- és behatolásjelző rendszer a terület ellenőrzésére.

[27] GYODA: gyorsan telepíthető drótakadály, más néven NATO-drót. Olyan pengés dróthuzal, amelyet széthúzva rugószerű hurkos hengert képez.
[28] wedge barrier: olyan süllyedő lemez alakú szerkezet, amely a behajtás irányával szemben nyílik fel és meggátolja az áthajtást

    - őrszolgálat/portaszolgálat megszervezése a belépési jogosultságok ellenőrzésére.
    - a belépéssel kapcsolatos szabályrendszerek kialakítása: az ott dolgozó személyek mikor léphet be a területre (műszakok, munkaidő kezelése), vendégek belépésének kezelése, hatóságok és közjogi méltóságok belépésének kezelése.
- személyzet ellen irányuló atrocitás a 0. védelmi zónában:
    - elektronikus támadásjelző és dőlésérzékelő rendszer használata.
    - őrszolgálat szakmai képzése a konfliktuskezelésre, kényszerítő eszközök használata.
- fegyveres támadás elleni védelmi megoldások:
    - őrszolgálat szakmai képzése a kialakulóban lévő helyzet időbeli felismerésére, a kialakult helyzet higgadt kezelésére.
    - fizikai zárlat lehetőségének kialakítása rácsszerkezettel, vagy a beléptetési pontok blokkolásával.
    - lövedékálló recepciós-ügyfélirányító helyiség kialakítása, vészjelzés leadása a reagáló erők részére (FBŐ, biztonsági szolgálat, rendvédelmi szervek).

3.2 1. zóna

Az **1. védelmi zónába** jogosulatlanul belépő személyek által elkövethető akciók hatásai a kritikus infrastruktúra 0. és 1. védelmi zónára korlátozódnak, azonban ennek következményeként előfordulhat rövid ideig, maximum 12 óráig tartó üzemzavar. A meghibásodás hatása(i) nem terjed(nek) túl a kritikus infrastruktúra határain. Az üzemzavar kezelése a legtöbb esetben nem igényel külső beavatkozást vagy támogatást, a helyben rendelkezésre álló erőforrásokkal (személyzet és eszköz) kezelhető.

Az 1. védelmi zónába az alábbi helyiségeket soroltam:

- **recepció, munkavállalói bejárat**: a 0. és az 1. védelmi zóna határán helyezkedik el. Fő feladata a kritikus infrastruktúra belső területeire, a saját és a szerződéses megállapodás alapján tevékenységet végző külső munkavállalók beléptetésének biztosítása.

- **irodák, adminisztráció**: ezekben a helyiségekben nincs közvetlen hozzáférés a kritikus infrastruktúra vezérléséhez, csak a szegregált irodai hálózathoz lehet hozzáférni.
- **raktárak**: olyan helyiségek, ahol az általános működtetéshez szükséges eszközök, szerszámok és vegyianyagok kerülnek eltárolásra. A kritikus infrastruktúra működésével kapcsolatos iratok tárolása nem ebben a védelmi zónában történik.
- **műhelyek**: a napi működéshez szükséges karbantartási és üzemeltetői feladatok ellátását biztosító helyiség

Lehetséges további kockázatok és kezelésük a 0. védelmi zónában meghatározottakon felül:

- belső (saját és a szerződéses jogviszony alapján foglalkoztatott külsős munkavállaló) elkövető által indított tűz
    - automatikus tűzjelző rendszer üzemeltetése.
- belső elkövető általi adatlopás
    - felhasználói tevékenység naplózása, portvédelmi megoldások (DLP) alkalmazása
    - csomag- és személyátvizsgálás a recepción (adathordozók, dokumentumok keresése).
- belső elkövető által elkövetett kibertámadás
    - szegregált hálózat kialakítása: irodai, vezérlői, biztonsági hálózat.
    - mentési- és helyreállítási szabályozás kialakítása
- belső elkövető által elkövetett fizikai támadások
    - csomag- és személyátvizsgálás a recepción (szúró- és vágófegyverek, lőfegyverek kiszűrése)
    - biztonsági szolgálati jelenlét, járőrtevékenység a zónában

3.3 2. zóna

A **2. védelmi** zónába történő illetéktelen belépés már nagyobb kockázatot jelenthet a kritikus infrastruktúrára nézve. Az üzemzavar mértéke rövid (0-12 óra), azonban a kiterjedése már nem korlátozódik a KI területére, hanem regionális szinten jelentkezhet. A meghibásodás elhárításához a lokális személyzeten túl külső szakértők és erőforrások bevonása is szükséges lehet.

A 2. védelmi zónába történő illetéktelen belépés általában nem jelent közvetlen veszélyt a lakosságra, azonban a regionális kiterjedés miatt már kiemelt figyelmet kell fordítani a kölcsönös függőséggel rendelkező többi kritikus infrastruktúra kapcsolatára. [80 p. 134-137]

A 2. védelmi zónába az alábbi helyiségeket soroltam:

- **mérőlaboratóriumok:** a kritikus infrastruktúrákkal kapcsolatos anyagok, vagy folyamatok mérését biztosító helyiségek, például vegyi elemző laborok.
- **műszaki helyiségek**: a kritikus infrastruktúra működését biztosító közművekkel kapcsolatos helyiségek, például gázfogadó, kazán, transzformátor.
- **irattár, archívum, MAK**[29] helyiség: az infrastruktúra műszaki felépítésével, valamint a minősített adatok tárolásával kapcsolatos helyiségek.

Lehetséges további kockázatok és kezelésük az 1. védelmi zónában meghatározottakon felül:

- belső elkövető általi indított vegyi reakció indítása a laboratóriumban
    - vegyi anyag detektáló védelmi rendszer kiépítése az épület biztonsági rendszerébe integrálva
    - videómegfigyelő rendszer alkalmazása a helyiségekben
    - heves/kritikus reakciókat kiváltó vegyi anyagok használatának, tárolásának és hozzáférhetőségének szabályozása
    - közömbösítő anyagok biztosítása
    - rendszeres oktatások és képzések megtartása.
- belső elkövető általi szabotázs a műszaki helyiségekben
    - videómegfigyelő rendszer alkalmazása
    - többirányú közmű ellátás kiépítése

[29] MAK helyiség: a 90/2010. (III.26.) Korm rendelet előírása alapján kialakított, a minősített adat felhasználására és tárolására szolgáló helyiség. [81]

- belső elkövető általi iratlopás, vagy iratmegsemmisítés
    - személy- és csomagátvizsgáló berendezés használata
    - videómegfigyelő rendszer használata
    - az irattárba, a MAK helyiségbe történő belépés rendjének szabályozása és dokumentálása

3.4 3. zóna

A **3. védelmi zónába** történő illetéktelen belépés a kritikus infrastruktúra sérülékenysége szempontjából már nagyon magas kockázatú területet jelent. Az itt található rendszerek, hálózatok és szolgáltatások működésének zavara már hosszabb távú, akár több napos kieséssel (17-72 óra), nemzeti szinten jelentkezhet. A kölcsönös függésben lévő határtúli kritikus infrastruktúrákkal kialakított hálózatszerűség miatt reális kockázatként lehet számontartani a dominó-elv szerű láncreakciót.[82 pp. 36-39] Az alapvető szolgáltatás helyreállításához a lokális személyzeten túl külső szakértők és erőforrások bevonása is szükséges lehet.

A 3. védelmi zónába történő illetéktelen belépés okozta lehetséges meghibásodás hatással lehet például a társadalomra, a gazdaságra, vagy akár a közegészségügyre.[83] Ilyen meghibásodás lehet például az áramszolgáltatás teljes megszűnése, az internetkapcsolat megszakadása, a vízellátás megszűnése stb. [84]

A 3. védelmi zónába az alábbi helyiségeket soroltam:

- **biztonsági (vagyonvédelmi) központ:** a kritikus infrastruktúra elektronikai és élőerős védelmét irányító vezetési pont.
- **adatközpont, szerver szoba**: a kritikus infrastruktúra működését biztosító informatikai hálózat központi egységeit tartalmazó helyiség.
- **kommunikációs központ**: az infrastruktúrán belüli és a többi infrastruktúrával kiépített kommunikációs hálózat központi elemeit tartalmazó helyiség
- **részfolyamatok irányító központja:** olyan szekciók/részlegek vezérlése, amelyek kiesése nagyfokú üzemzavarhoz járhat.

Lehetséges további kockázatok és kezelésük az 2. védelmi zónában meghatározottakon felül:

- a belső vezérlő hálózati infrastruktúra elleni támadás

- adatközpontok, szerverek bejáratainál zsilipes beléptetés és biztonsági szolgálat felállítása
- végpontvédelmi megoldások használata, szoftveres (port security) vagy fizikai (nem használt végpontok kapcsolatának tiltása)
- EMC védelem[30] kialakítása

- adatlopás a vezérlő hálózatból
  - végpont- és szerveroldali rendszerfelügyeleti megoldások használata
- a vagyonvédelmi központ és a személyzete ellen irányuló támadás
  - zsilipes beléptetés kialakítása
  - külön fegyverszoba kialakítása[31]
  - EMC védelem kialakítása a biztonságtechnikai rendszerek központi elemei körül.
- a kommunikáció blokkolása, elterelése
  - a belső vészhelyzeti kommunikáció különválasztása az általános belső kommunikációtól
  - a kölcsönös függésben lévő kritikus infrastruktúrák felé alternatív kommunikációs csatornák létrehozása

3.5 4. zóna

A **4. védelmi zónába** történő illetéktelen belépés a kritikus infrastruktúra teljes kiesésével, megsemmisülésével, valamint a kölcsönös függésben lévő KI-k meghibásodásával járhat. A szolgáltatás kiesés időbeli kiterjedése meghaladja a 72 órát, a területi kiterjedése már nem csak regionális, vagy nemzeti szinten jelentkezik, hanem az országhatáron átnyúlhat és több tagállamot érinthet a kölcsönös függőség miatt. A meghibásodás kezeléséhez, helyreállításához nem elégséges a lokális erőforrás, külső, akár másik tagállamból érkező szakértők bevonása és összehangolása szükséges.

A 4. védelmi zónába történő illetéktelen belépés okozta lehetséges hatások közvetlen veszélyt jelenthetnek a lakosságra.

[30] EMC (Elektromágneses kompatibilitás) védelem olyan intézkedések és tervezési módszerek összessége, amelyek célja az elektromágneses interferencia minimalizálása és a berendezések, rendszerek vagy eszközök megfelelő működésének biztosítása a környezeti elektromágneses hatásokkal szemben.

[31] Fegyverszoba: a szolgálati lőfegyverek és a hozzájuk kiadott tartozékok, valamint a szolgálati lőszerek tárolására kialakított, ráccsal, biztonsági zárral, valamint az átlátható tárolást biztosító berendezési tárgyakkal (állványok, rekeszek, szekrények stb.) felszerelt helyiség, amely biztonságtechnikai védelemmel és egyéb megfelelő mechanikus őrzés-védelmi rendszerrel is felszerelhető. Forrás: 32/2012 (VII.19.) BM utasítás

A 4. védelmi zónába az alábbi helyiségeket soroltam:

- a kritikus infrastruktúra vezérlőterme
- biológiai veszélyforrásokkal foglalkozó laboratóriumok
- nemzeti informatikai központok (BIX[32], Dataneum[33], Dataplex[34])
- nemzetközi repülőterek irányítótornya
- katonai irányítási központok
- A-szintű fizika védelmet igénylő nukleáris anyagok tárolását biztosító helyiség [3]

Lehetséges további kockázatok és kezelésük az 3. védelmi zónában meghatározottakon felül:

- a vezérlőterem megtámadása
    - fegyveres őrszolgálati pont a zóna bejáratainál
    - személy- és csomagátvizsgálás
    - zsilip alapú be- és kiléptetés
    - bent tartózkodók létszámának figyelése
    - videómegfigyelő rendszer üzemeltetése
    - vészhelyzeti protokollok meghatározása és gyakorlatok megtartása
- további nemzeti és tagállami infrastruktúrák elleni hálózati támadás
    - azonnali hálózati leválasztás kialakítása
    - alternatív kommunikációs csatornákon értesítés küldése
- a sugárzó anyag eltulajdonítása
    - sugárkapuk, detektorok működtetése
    - zsilip alapú be- és kiléptetés
- biológiai veszélyforrás eltulajdonítása
    - zsilip alapú be- és kiléptetés
    - videómegfigyelő rendszer
    - detektálási rendszer kidolgozása, például mintatárolókban érzékelők

[32] Budapest Internet Exchange
[33] Invitech DC10
[34] T-Systems Cloud & Datacenter Budapest

3.6 Következtetések

A védelmi zónák kialakítása és a megfelelő védelmi funkciók kezelése a kritikus infrastruktúrák esetében alapvető fontosságú. Ebben a fejezetben bemutattam egy innovatív módszert, amely a kritikusság hatásán és a "worst-case" modellezésen alapulva definiált védelmi zónákat a 0-tól 4-ig terjedő skálán. Ez a zónákra osztott védelmi rendszer stratégiai lépéseket épít egymásra, figyelembe véve a mélységi védelem elvét (protection-in-depth) [85 pp 63-66][86 pp. 145-146]

A védelmi zónák kialakításakor 86a fizikai és logikai hozzáférés-ellenőrzés kiemelkedő szerepet kapott. Az elektronikus beléptető rendszerek használatával lehetővé válik a fizikai hozzáférés precíz és kontrollált kezelése. Ezáltal a szervezetek pontosan beállíthatják, hogy kik jogosultak a belépésre, milyen időpontban és mely területekre. Az ilyen rendszerek lehetővé teszik a hozzáférési jogosultságok könnyed kezelését és dinamikus módosítását, valamint rögzítik a belépési eseményeket és logokat/naplókat generálnak.

A megfelelő fizikai és logikai hozzáférés-kezelés szabályozása kulcsfontosságú a kritikus infrastruktúrák hatékony védelme szempontjából. Az elektronikus beléptető rendszerek használatával a hozzáférés precíz szabályozása és ellenőrzése valósítható meg, csökkentve a jogosulatlan belépések kockázatát és növelve a biztonság és védelem szintjét. Ezáltal minimalizálhatóak a potenciális fenyegetések és károk, és biztosítottá válik a kontrollált hozzáférés a kritikus területekre.

Az általam kialakított védelmi zónabesorolási rendszer, amely figyelembe veszi a fizikai és logikai hozzáférés-ellenőrzés szabályozását, hozzájárulhat az Európai Unió új 2022/2557/EK irányelvében meghatározott reziliencia szint növeléséhez.[4] Ezáltal az infrastruktúrák még jobban felkészültek lehetnek a potenciális külső és belső veszélyekkel szemben, és növelhetik a rugalmas ellenállóképességüket. A megfelelő hozzáférés-ellenőrzés biztosítása a védelmi rendszer alapvető pillére, amely elősegíti a kritikus infrastruktúrák hatékony védelmét a változó környezetben.[87]

A zónabesorolás alapjait jelentő hatások időbeli, térbeli kiterjedését és a hatás kezeléséhez szükséges erőforrások meghatározását az 1. számú táblázat tartalmazza.

védelmi zóna száma	illetéktelen belépés legrosszabb hatása	a hatás kiterjedése	a hatás kezelése
0	nincs ismert sérülékenység	lokális, a KI adott védelmi zónájára korlátozódik	lokális beavatkozás elégséges
1	rövid ideig, maximum 12 órán át tartó üzemzavar előfordulhat	lokális a KI-területére korlátozódik	lokális beavatkozás elégséges
2	rövid ideig, maximum 12 órán át tartó üzemzavar előfordulhat	a hatása regionális szintű lehet, nem korlátozódik a KI területére	lokális beavatkozás és külső szakértő bevonása szükséges
3	hosszabb, 12-72 órán át tartó üzemzavar előfordulhat	a hatása nemzeti szintű lehet	lokális beavatkozás és külső szakértő bevonása szükséges
4	hosszabb, 72 óránál tovább tartó üzemzavar, vagy a KI megsemmisülése	a hatása kiterjedhet több KI működésére a kölcsönös függőség elve alapján, hatása határon átnyúló lehet	lokális beavatkozás és külső, akár másik országból érkező szakértő bevonása szükséges

1. táblázat Összefoglaló táblázat a védelmi zónákról, a táblázatot a szerző szerkesztette

4 A BELÉPTETŐ RENDSZEREK

A beléptetőrendszerek fogalmát sokan és sokféleképpen határozták meg, de biztonságszakmai véleményem szerint Filkorn József írta körül a legjobban egy 2009. évi előadásában azt, hogy mi is a beléptetőrendszer: *„Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrzőpontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését."* „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beleptetés felügyeletéhez szükségesek" [88].

A fogalommeghatározás alapján az elektronikus beléptető rendszerek három fő funkcióval rendelkeznek:

1. az áthaladni szándékozó személy, vagy tárgy érzékelése és azonosítása,
2. az azonosítás eredményének összehasonlítása a rögzített (jogosultsági) adatbázisban szereplő azonosítókkal és a döntés meghozatala,
3. a meghozott döntés alapján az áthaladást biztosító eszköz vezérlése.

A fejezet további részében az elektronikus beléptető rendszerek fogalmával, kizárólag a személyek beléptetésével kapcsolatos elektromechanikai eszközöket azonosítom. [89 pp. 39-50][90 pp. 19-24]

4.1 Alapfogalmak

Anti-passback – a beléptető rendszer azon biztonsági funkciója, amely megakadályozza, hogy ugyanaz az azonosító többször használható legyen egymást követő belépési vagy kilépési pontokon, ezzel csökkentve az illetéktelen behatolás lehetőségét. Lehet soft-, hard- és global anti-passback beállítás is.

Áteresztőképesség – azon emberek száma, akik egy adott időszak alatt áthaladhatnak az áteresztő ponton.

Azonosítás – az az esemény, amikor a felhasználó adatait összevetve az adatbázisban tárolt adatokkal egyetlen egyezést találunk.

Belépőkártya – kódolt kártya, amelyet azonosításra használnak a beléptető rendszerekben. Megszemélyesítés esetén igazolványként is használható.

Beléptetési/áteresztési pont – A védett területre történő be- és kilépési pontja.

Billentyűzet, tasztatúra, PIN-pad – bemeneti eszköz a PIN-kódok bevitelére a beléptető rendszerben.

Biometrikus adatok – az egyén fizikai és/vagy viselkedési jellemzőinek érzékeléséből keletkezett adatsor.

Elektronikus áteresztő szerkezetek – A védett térhez való hozzáférést szabályozó elektronikus alkatrészek, például zárak, olvasók, érzékelők vagy gombok használatával.

Fail-safe (életvédelmi célú) zárszerkezet – tápellátás megszűnése esetén a beléptető rendszer elektromos zárszerkezetei nyitott állapotba kerülnek, lehetségessé válik az áthaladás.

Fail-secure (vagyonvédelmi cél) zárszerkezet – tápellátás megszűnése esetén a beléptető rendszer zárszerkezete resteszelve marad, továbbra is gátolja az áthaladást.

Forgókapu, forgóvilla, forgókereszt, forgókar – olyan mechanikus áteresztő eszköz, amely egyszerre csak egy személy áthaladását biztosítja.

Global anti-passback – olyan biztonsági intézkedés, amely a beléptető rendszerben a teljes területre (épületre, infrastruktúrára) kiterjedően megakadályozza, hogy ugyanaz a kártya egyidejűleg több helyen legyen jelen, ezáltal fokozva a biztonságot és megelőzve az illetéktelen mozgást a rendszeren belül.

Gyorskapu – olyan

Hard anti-passback – olyan biztonsági intézkedés, amely a beléptető rendszer adott védett zónára vonatkozóan megakadályozza, hogy ugyanaz a kártya egyidejűleg többször be-, vagy kilépjen.

Igazolvány – megszemélyesített belépőkártya.

Jogosult személy – olyan személy, aki hozzáféréssel rendelkezik az adott védett zónához.

Kártyaolvasó – a belépőkártya adatainak értelmezésére szolgáló eszköz.

Kéz geometria alapú azonosítás – a felhasználót a kézfej jellegzetes pontjainak geometriai távolságai alapján azonosítja.

Kontroller, vezérlő – az egyes beléptetési pontokon történő áthaladást biztosító, vagy tiltó elektronikus eszköz.

Mágnescsík – vas tartalmú anyagból álló adatokat tartalmazó sáv, amely az azonosító kártyán található.

Multimodális azonosítás – többféle azonosítási technológia kombinálásának lehetősége egy munkamenetben. Például belépőkártya-PIN kód, belépőkártya-biometrikus azonosítás.

Műveleti (biztonsági) központ – olyan helyiség az infrastruktúrán belül, ahol a (biztonsági) személyzet figyeli, értékeli és reagál a riasztásokra és/vagy hibajelzésekre.

PIN-kód (személyes azonosító szám) – egyedi numerikus, vagy alfanumerikus karakterkészlet, amely a beléptető rendszerben azonosításra használnak.

Proximity kártya – A proximity kártya egy olyan RFID (Radio Frequency Identification) technológián alapuló eszköz, amely a kártyaolvasó aktiválási zónájába lépve vezeték nélküli kommunikáció révén képes adatok küldeni az olvasóeszköznek.

Smart card – olyan azonosító kártya, amely integrált áramkört tartalmaz, amely lehetővé teszi adatok fogadását és tárolását, amelyeket aztán a beléptető rendszer ki tud olvasni.

Soft anti-passback – olyan biztonsági funkció, amely a beléptető rendszer adott védett zónára vonatkozóan figyeli a belépőkártyák mozgásait és riasztással jelzi, ha ugyanaz a kártya egyidejűleg többször be-, vagy kilépett.

Stand-alone (önálló) működés – a beléptetési pont működésére nincs hatással a kontroller és a szerver közötti kommunikációs vonal megszakadása. Az utolsó érvényes konfigurációnak megfelelően biztosítja, vagy tiltja az áthaladást.

Tailgating, piggybacking – az a cselekmény, amikor egy illetéktelen személy egy belépési jogosultsággal rendelkező személyt szorosan követve próbál bejutni az ellenőrzött térbe.

Ujjnyomat-érzékelő – biometrikus érzékelő, amely ujjnyomatot olvas. Lehet optikai, kapacitív, véna felismeréssel kombinál is.

Vegyes technológiájú (biometrikus) érzékelő – olyan érzékelő, amely két vagy több érzékelési technológiát használ a téves riasztások csökkentésére. Például ujjnyomat és ujj vénatérkép érzékelése egy szenzorban.

Videómegfigyelő rendszer – Videokamerákat használó videó megfigyelő rendszer, az élőképeket adott helyen monitoron megjeleníti.

Zsilip, személyzsilip – a zsilip egy olyan helység, vagy eszköz két egymásba nyíló ajtóból áll. Az egyik ajtónak be kell záródnia, mielőtt a másik nyitható lenne. Kombinálható további biztonsági berendezésekkel, például személyátvizsgáló készülékekkel, valamint biometrikus azonosítási folyamatokkal.

4.2 Beléptetési pont

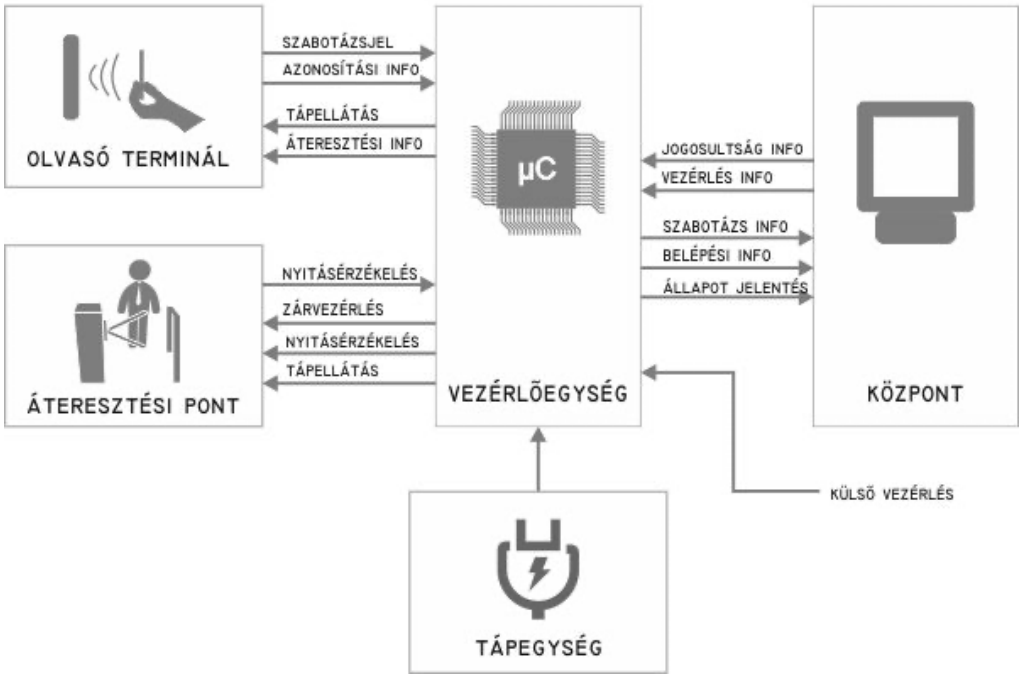
A beléptetési pont négy fő részből áll:

- áteresztést/beléptetést szabályozó eszközök: feladatuk a vezérlőegységből érkező döntés alapján az áthaladás biztosítása, vagy gátlása. A működési elvük alapján lehet életvédelmi (fail safe), vagy vagyonvédelmi (fail secure) típusúak. Az

életvédelmi típusnál az energiaellátás megszűnésekor a szabályozó eszköz nyitott állapotba kerül, így biztosítva a menekülés lehetőségét. A fail secure eszközök a tápellátás megszűnése esetén reteszelve maradnak.

- beléptető vezérlőegység, kontroller: az azonosító eszközből érkező adatokat összehasonlítja a korábban eltárolt adatokkal. Egyezés esetén a felhasználóhoz rendelt jogosultságnak megfelelően döntést hoz az áthaladás engedélyezéséről vagy tiltásáról. Eredménytelen összehasonlítás esetén tiltja az áthaladást.
- adatátviteli hálózat: az azonosító eszköz és a kontroller, a kontroller és az áteresztési pont, valamint több kontroller közötti információk cseréjére szolgáló összeköttetés. Korábban RS-485, most jellemzően IP protokollon keresztül ment a kommunikáció.
- azonosító eszközök: célja a személy azonosítása az előre definiált módszer és technológia alapján. Lehet tudás alapú, tárgy alapú, vagy biometrikus jellemzőn alapuló azonosítás.

A beléptetési pont egyszerűsített működési vázlatát az 5. ábra tartalmazza.



4. ábra A beléptető rendszer egyszerűsített működési vázlata, forrás: [91]

4.3 Azonosítási módszerek

Az elektronikus beléptető rendszerekben az azonosítás kiemelt fontossággal bír, hiszen a rendszernek megbízhatóan és hatékonyan kell meghatároznia, hogy ki az a felhasználó és jogosult-e a belépésre. Az azonosítási folyamatnak gyorsnak, pontosnak és

biztonságosnak kell lennie annak érdekében, hogy megvédje az értékes erőforrásokat, infrastruktúrákat és adatokat.[92 pp. 3-6][93] A következőkben röviden bemutatom a tudás alapú, a tárgy alapú és a biometria alapú azonosítás alapvető módszereit.[94]

4.3.1 Tudás alapú azonosítás

A tudás alapú azonosítás egy olyan módszer, amelyben a felhasználóknak egy bizonyos információval kell rendelkezniük ahhoz, hogy igazolják azonosságukat és be tudjanak lépni a zárt területre, vagy hozzáférjenek egy adott rendszerhez. Az egyik leggyakoribb forma a PIN-kód[35] használata, amely numerikus vagy akár alfanumerikus karakterekből áll.

A PIN-kód egy rövid numerikus vagy alfanumerikus jelsorozat, amely a felhasználóhoz van társítva. A numerikus PIN-kódok csak számjegyekből állnak, például négy- vagy hatjegyű számokból. A felhasználóknak meg kell jegyezniük ezt a jelsorozatot, és be kell írniuk azt a megfelelő terminálon vagy eszközön, hogy igazolják azonosságukat. Az ilyen típusú PIN-kódok egyszerűek és könnyen megjegyezhetők, de kevésbé biztonságosak, mivel korlátozott számú kombinációt kínálnak.

Az alfanumerikus PIN-kódok a numerikus és betűs karaktereket kombinálják, így bonyolultabb jelsorozatot eredményeznek. Ezek a kódok biztonságosabbak, mivel nagyobb kombinációs lehetőségeket kínálnak, amelyek nehezebben törhetők fel. A felhasználóknak ezeket a kódokat is meg kell jegyezniük és be kell írniuk az azonosítási folyamat során. [95 p. 77-91]

Előnyei többek között az azonosító eszköz (billentyűzet) alacsony költsége és a könnyű használhatóság. Hátránya az azonosító könnyű átadhatósága és kifigyelhetősége.

A következő összefoglaló táblázatban (2. számú) bemutatom néhány numerikus és alfanumerikus kód lehetséges variációinak számát, ahol a betűk tekintetében az angol ábécé betűkészletét vettem alapul.

[35] Personal Identification Number: személyi azonosító szám

4 db számjegy (4N)	10.000
5 db számjegy (5N)	100.000
6 db számjegy (6N)	1.000.000
3 db 2 számjegyű természetes szám (2N+2N+2N)	729.000
2 db 3 számjegyű természetes szám (3N+3N)	810.000
1 betű 3 számjegy 1 betű (A+3N+A)	676.000
2 betű 4 szám (2A+4N)	6.760.000
3 betű 3 szám (3A+3N)	17.576.000

2. táblázat: Lehetséges variációk száma, a táblázatot a szerző szerkesztette

4.3.2 Tárgyalapú azonosítás

A tárgyalapú azonosítás során a felhasználót, a korábban hozzá rendelt fizikai tárgy használatával azonosítja a beléptető rendszer. Az 1960-as években fejlesztették ki az első ilyen tárgy alapú azonosító rendszereket, amelyek még lyukkártyákat használtak azonosításra. Pár évvel később kifejlesztették az első mágnescsíkos beléptető rendszert. A rádiófrekvenciás azonosítási technológia a beléptető rendszereknél az 1990-es években jelent meg, majd a technológia rohamos fejlődésével a 2000-es évek elején megjelentek a Smat-card-ok. [96][97] Előnyei a könnyű használhatósága, az elfogadottsága. a gazdaságos üzemeltethetősége és a többcélú használhatósága. Legfőbb hátránya az azonosító tárgy könnyű eltulajdoníthatósága.

Mágnescsíkos belépőkártya

A mágnescsíkos kártyák hasonló összetételűek és megjelenésűek, mint a bank- vagy hitelkártyák. A kártya csíkjában körülbelül 140 számjegy és karakter található, amelyeket 1-3 sávra osztottak szabadalmaztatott formátumban. A kártyákat az olvasósávon át kell húzni az vagy teljesen be kell dugni az olvasóba, majd kihúzni az adatok leolvasásához.

A mágnescsík olvasók érzékelik a kártya csíkjában azokat a pontokat, ahol a mágneses kódolás megfordítja a polaritást. Amikor két északi vagy két déli mágneses pólus találkozik egymással, kis feszültségtranziens keletkezik a kártyaolvasóban. Ezeket a tranzienseket algoritmusok segítségével (órajel, hibakereső) kiértékelik, majd a kapott bináris számsort továbbítják a kontrollernek.

A kártyaolvasók könnyen és egyszerűen telepíthetők szinte minden felületre, például falakra, ajtókeretekre. Az olvasóegységeken gyakran találhatók vizuális állapot visszajelző piros és zöld LED-ek. Érvényes belépési engedély esetén a zöld, érvénytelen belépési engedély esetén a piros LED világít/villog.

A mágnescsíkos kártyák előnyei között szerepel az alacsony telepítési költség és a könnyű megszemélyesíthetőség. A kártyákon fel lehet tüntetni a felhasználó nevét, azonosító számát, fényképét, a vállalati logót, így azok azonosítókártyaként is használhatók.

A mágnescsíkos kártyák hátrányai közé tartozik, hogy másolásukra és kódolásukra használt eszközök szabadon kaphatók a kereskedelemben, ami lehetővé teszi a viszonylag könnyű másolást és hamisítást. Ezért fontos, hogy a mágnescsíkon kódolt információk különbözzenek a kártya előlapján található információktól, így megnehezítve a hamisítók számára, hogy egyszerűen a kártya előlapjáról kódolják az adatokat.

Rádiófrekvenciás azonosítás (RFID)

Az RFID[36] azonosítás egy gyakran alkalmazott technológia a beléptető rendszerekben. Az RFID alapú azonosítás lehetővé teszi a vezeték nélküli kommunikációt egy RFID kártya és az olvasó között. Az RFID kártyákban egyedileg azonosítható adatok találhatók, amelyeket az olvasók érzékelnek és értelmeznek. Az RFID rendszerben az olvasó eszköz azonosítja az RFID kártyát és továbbítja az azonosítási adatokat a beléptető rendszernek. [98]

Smart card

A kontaktusos és az beágyazott antennával rendelkező kontaktusmentes smart-card alapú beléptetőrendszerek hatékony és biztonságos megoldást kínálnak olyan környezetekben is, ahol a felhasználók száma meghaladja a 100.000-et. Ezek a rendszerek rugalmasan képesek kezelni a különböző jogosultsági szinteket, amelyek lehetővé teszik a pontos és differenciált hozzáférésszabályozást. A sokoldalúság és kombinálhatóság miatt a smart-card olvasók gyakran rendelkeznek beépített numerikus billentyűzettel a PIN-kódok

[36] Radio Frequency Identification: automatikus azonosításhoz és adatközléshez használt technológia

beviteléhez, valamint lehetőséget biztosítanak a biometrikus eszközök csatlakoztatásához a kétfaktoros hitelesítés érdekében.[99]
A smart-card-ok általában kinézetükben hasonlítanak a hagyományos chip-es bankkártyákra. Az ilyen kártyákba beépített chip-eknek két alapvető típusa van: a memóriaáramkörös és a mikroprocesszoros. A memóriaáramkörös kártyák esetén lehetőség van több memóriaszekció elkülönítésére eltérő titkosítási szintekkel, ami segít az adatok biztonságos kezelésében és korlátozott hozzáférés biztosításában.

A mikroprocesszoros áramkörrel rendelkező okoskártyák további előnyökkel járnak. A kártyán található mikroprocesszor lehetővé teszi a beléptető rendszer adminisztrátor számára, hogy a különböző, a hitelesítési eljárásokhoz kapcsolódó alkalmazásokat és titkosító kulcsokat együtt tárolja az adatokkal a kártyán. Például, ha második azonosítási faktorként biometrikus rendszert használnak a hitelesítéshez, a biometrikus sablon eltárolható a felhasználó smart-card-ján. Abban az estben, ha a hitelesítési algoritmus is a kártyán található, akkor a kártyaolvasónak csak saját hitelesítő programját kell futtatnia a kártyán. A kártya a tárolt és feldolgozott biometrikus adatok összehasonlítását követően küldi elfogadási, vagy elutasítási parancsot a kontroller számára.

A működtetéshez a felhasználónak kontaktusos azonosítás esetén be kell helyeznie a kártyát az olvasóba, kontaktusmentes azonosítás esetén az olvasási távolságra kell közelítenie a kártyát az olvasóhoz.

A smart-card alapú beléptető rendszerek előnye a magasabb szintű biztonság, valamint az azonosítási módszerek kombinálhatósága, paraméterezhetősége. A kártya jól kombinálható más tudásalapú vagy biometriai azonosítási módszerekkel, lehetővé téve a megbízhatóbb és pontosabb felhasználóazonosítást. Emellett a kártya megszemélyesíthető nyomtatással, vagy előlappal, így azonosító kártyaként is használható. A smart-card-ok ideálisak közepes áteresztőképességű beléptetőrendszerekhez. Ugyanakkor a smart-card alapú beléptető rendszereknek vannak bizonyos hátrányai is. Az azonosítási folyamat lassabb lehet a kontaktusos rendszerek esetében, amely csökkentheti az áteresztőképességet és rendszer elfogadottságát a felhasználóknál. Emellett ezek a típusú kártyák általában nem alkalmasak kültéri kontaktos alkalmazásokra, mivel az időjárási körülmények befolyásolhatják az olvasók érintkezési pontjait, valamint az erős mágneses terek tönkre tehetik a kártyák mikroprocesszorait.

Azonosítás mobiltelefon használatával

Az okostelefonoknál alkalmazott NFC[37] egyedi azonosítási technológia lehetővé tette, hogy a telefonok is beintegrálásra kerüljenek a beléptető rendszerekbe. Elég csak közelíteni a mobiltelefont az olvasóhoz és megtörténik az azonosítás. A folyamat gyors és hatékony, azonban a biztonság növelése érdekében az NFC alapú azonosítás első lépéseként a felhasználónak azonosítania kell magát a mobiltelefonon (ujjnyomat, arcfelismerés). Ezt követően nyílik lehetősége az NFC alapú beléptető azonosításra.

4.3.3 Biometrikus azonosítási technológiák

A biometrikus azonosítás során a felhasználót az egyedi fiziológiai vagy viselkedésbeli jellemzői alapján azonosítják.[100] Az elektronikai vagyonvédelmi rendszerekben gyakrabban használt biometria jellemzőket a következő táblázatban (3. számú) kerültek összefoglalásra.

biometrikus jellemző	fizikai	viselkedési
arc	+	
ujjnyomat	+	
ujj/kézgeometria	+	
vénaszkenner	+	
írisz	+	
hang	+	+
járás	+	+

3. táblázat Biometrikus jellemzők, a táblázatot a szerző szerkesztette

A biometrikus azonosítás lépései általában az alábbiak szerint alakulnak. Első lépésként rögzítik az adatbázisban a felhasználó biometrikus azonosítóját, szükség esetén ezt az adatot eltárolják a belépőkártyán (smart-card) is. A biometrikus beléptető rendszer használatakor az szenzor rögzíti a felhasználó biometriai mintáját, az azonosítást végző algoritmus kiemeli a jellegzetes (azonosításra alkalmas) jegyeket. Az összehasonlító algoritmus összeveti „egy a kevéshez” elven a mintát az adatbázisban tárolt mintákkal. Amennyiben egyezést talál, akkor a felhasználó sikeresen beazonosításra került és a jogosultságának megfelelően engedélyezi, vagy tiltja az áthaladást. Abban az esetben, ha nem talál egyezést az adatbázisban, automatikusan tiltja az áthaladást.

[37] Near Field Communication: rövid távú kommunikációs szabvány

A biometrikus azonosítás kiemelkedően megbízható és pontos módszer, mivel az egyedi biometriai jellemzőket nehezen vagy gyakorlatilag lehetetlen másolni, vagy hamisítani. Az emberi test jellemzői általában állandóak és rendkívül egyediek, ami jelentős előrelépést jelent a hagyományos jelszavak vagy kártyák alapú azonosítási módszerekhez képest.[101]

Az azonosítási rendszerek hatékonysága és megbízhatósága három speciális jellemzővel értékelhető:

- a False Rejection Rate (FRR), vagyis téves elutasítási arány,
- a False Acceptance Rate (FAR) azaz téves elfogadási arány,
- a Crossover Error Rate (CER), vagyis az keresztezési hibaarány és
- a Failure to Enroll Rate (FER), azaz bevonhatósági hiba valószínűsége.

Téves elutasításról akkor beszélünk, amikor a beleptető rendszer az arra jogosult felhasználónak megtagadja a belépést. Több oka is lehetséges, például a hibás mintavételezés, vagy akár a minta kiértékelésének időtúllépése. Téves elfogadás esetén jogosulatlan személyeket azonosít az algoritmus jogosultként. Ennek lehetséges oka a minta hamisítása, vagy az algoritmus téves kiértékelése. Az azonos hibamérték a különböző típusú azonosítási rendszerek objektív összehasonlításának érdekében került bevezetésre. A keresztezési hibaarány leírja azt a pontot, ahol az FRR és a FAR egyenlő, ezzel leírja a biometrikus rendszer általános pontosságát. A bevonhatósági hiba valószínűsége alatt azt a számot mutatja meg számunkra, hogy mekkora az esély arra, hogy valaki kiessen a biometrikus mérés alól. A fenti négy jellemző közül a legfontosabb jellemző, a FAR index. Ugyanis ez mutatja meg számunkra, hogy milyen arányban azonosítja téves jogosultként az arra nem jogosult személyt. [100][101]

Ugyanakkor a biometrikus azonosításnak is vannak biztonsági és adatvédelmi kérdései. Mivel a biometriai jellemzők különleges személyes adatnak minősülnek kritikus fontosságú, hogy ezeket az adatokat megfelelően védjék. Az adatvédelem biztosítása érdekében szigorú protokollokat és intézkedéseket kell alkalmazni a biometriai adatok tárolására és kezelésére, hogy megakadályozzák az illetéktelen hozzáférést vagy visszaélést ezekkel az érzékeny információkkal.

Arc(geometria) alapú azonosító rendszerek

Az arcfelismerés során az kiértékelő algoritmus egy vagy több fényképet/állóképet használ fel egy személy felismerésére és azonosítására az arcon található jellemző pontok alapján. Ilyen referencia pontok a szemek és az arc széle közötti távolság, a szemek

közötti távolság, az orr hossza, valamint a szem- és szájszélessége. Az arcfelismerő rendszerek nem igényelnek fizikai kontaktust a felhasználóval, ezért magas a felhasználói elfogadási aránya.

Az arcfelismerést nem befolyásolják a faji vagy nemi alapú megjelenési különbségek. Ez a technológia képes kezelni a különböző testtípusok és arctulajdonságok széles skáláját, azonban az arcszőrzet vagy a testsúly nagyobb változásai befolyásolják az arcvonásokat és nehezítik az azonosítást. Az arcfelismerést világszerte használják olyan változatos iparágakban, mint a bankszektor, a szerencsejáték, az egészségügy, a bűnüldözés, a vámügyek és a kiskereskedelem. A technológiát sikeresen tesztelték semleges iparági összehasonlításokban, és jelenleg a biometrikus azonosítás piacának leggyorsabban növekvő szegmense, azonban nem ajánlott olyan területeken, ahol a megvilágítás nem homogén, vagy ahol személyi védőfelszerelés, például szájmaszk, vagy védőszemüveg használata szükséges. [68][102][103]

Ujjnyomat alapú azonosítás

Az ujjnyomat az egyik legszélesebb körben használt biometrikus azonosító a beléptető rendszerekben. Ennek az az oka, hogy az ujjnyomat a személyazonosítás egyik legrégebbi formája, gyűjtése és elemzése kevés költséggel jár. Az ujjnyomat olvasási technikákat megkülönböztethetjük az optikai, a kapacitív, a rádiófrekvenciás, az ultrahangos és a nyomásérzékelésen alapuló módszer alapján.[104 pp.199-207]

Az optikai elven működő ujjnyomat olvasók a feldolgozandó képet egy optikai rendszerrel (CCD)[38] egy képbontó eszköz felületére képezik le, amely elektromos jellé alakítja azt. A redőket sötét színnel, a barázdákat világos színnel emeli ki az algoritmus. Ez a legelterjedtebb módszer a beléptető rendszerekben. Előnye a nagy felhasználói elfogadottsága és a technológia alacsony költsége. Hátránya az olvasó felületének elkoszolódása és karcolódása okozta olvasási, azonosítási hibák gyakori előfordulása.

A kapacitív elvű ujjnyomat olvasók működése arra épül, hogy a szenzor felületére helyezett ujj völgyei és fodorszálai eltérő kapacitásképet mutatnak. Ez a kapacitás „térkép” kerül detektálásra és feldolgozásra. A hagyományos optikai alapú érzékelőkkel összehasonlítva a kapacitív ujjnyomat érzékelők gyorsabban és pontosabban dolgozzák fel az érzékelt ujjat. Hátrányai között az elektrosztatikus kisülésre való érzékenysége, valamint a száraz, sérült ujjak nehézkes azonosítása szerepel.

[38] Charge-coupled Device, azaz töltés-csatolt eszköz. Fényérzékeny alkatrésszel, fotodiódával kombinálva a fényt elektronikus jelekké alakító eszköz.

„A rádiófrekvenciás elven alapuló ujjnyomat olvasók esetében a szenzor keretén keresztül rádiófrekvenciás jelet juttatnak az ujjra, amely adóantennaként visszasugározza azt a vevőantennaként szolgáló szenzor-felületre. A szenzor által alkotott kép nemcsak az ujj felületét képezi le, hanem mélységi képalkotást is szolgáltat. Ennek köszönhetően a képalkotás sérült, nagyon száraz vagy szennyezett ujjak esetén is sikeres lehet." [68 p. 37]

Az ultrahangos elven alapuló ujjnyomat olvasók esetén a szenzor ultrahangot küld a felültre helyezett ujjbegyre. A hanghullámok áthatolnak a szennyeződéseken, zsírokon és egyéb szennyeződéseken, hogy képet kapjanak az ujj szöveteiről és erezetéről. Ezzel az eljárással olyan esetekben is azonosíthatóak az ujjnyomatok, ahol az optikai technológia nem működne, például a kopott ujjvégek esetén. Az ultrahangos elven működő ujjnyomat azonosítás további előnye, hogy különbséget tud tenni az élő és a nem élő minta között. Hátránya a lassabb azonosítás, valamint az eszköz magasabb költsége.

Azok az ujjnyomatolvasók, amelyek a nyomásérzékelés elvén működnek, olyan szenzorokat használnak, amelyek alatt piezo-elektromos nyomásérzékelő mátrix található. Ezek a szenzorok képesek érzékelni az ujj redői és barázdái által kialakított egyenetlenségeket és ezek alapján képet alkotni. Mivel a szenzorok a nyomás érzékelésén alapulnak, ezért a szennyeződések vagy piszok nem zavarják jelentősen a szenzorok működését.

Összességében a megfelelő technológia kiválasztásával beltérben és kültérben is használható a beléptető rendszer részeként az ujjnyomatazonosítás. Azonban nem ajánlott olyan környezetben, ahol folyamatosan egyéni védőeszközként kesztyűt kell viselni, vagy nagy az ujjak sérülésének, kopásának valószínűsége.

Kézgeometria

A kézgeometria azonosítás során az olvasó a tenyér és az ujjak formáját, méretét, körvonalát érzékelve egy térképet készít az adott kézről. Figyelembe veszi az ujjak hosszúságát és szélességét, a kézfej méretét, a tenyér és az ujjak méretarányát. A megfelelő azonosítást öt pozícionáló tüske segíti, amelyek a kézfej és az ujjak helyét határozza meg. Az azonosítás során a rendszer figyelmen kívül hagyja a felület részleteit, például az ujjnyomatokat, a hegeket és a szennyeződéseket.

Előnye a viszonylag gyors azonosítást, és a szennyezett környezetben való alkalmazhatóság. Hátránya azonban, hogy kevés azonosító pontot használ, így a téves azonosítás és a téves elutasítás aránya magasabb, mint a többi biometrikus azonosításnál.

Vénaszkenner

A vaszkuláris mintázatfelismerés, ismertebb nevén a véna-szkennelés alapja, hogy a kézben vagy az ujjban lévő egyedi vénás mintázatokat megvilágítja infravörös fény segítségével. A vérben található hemoglobin elnyeli az infravörös sugarakat, így a vénák sötétként, a környező szövetek pedig világosként jelennek meg a képen. A tenyér esetében akár 5 millió azonosítási pontot is meg tud különböztetni. A technológia további előnye, hogy még 70%-os fizikai roncsolódás esetén is képes megbízhatóan azonosítani a tulajdonost, mivel a bőr felszíni változásai, sérülések vagy szennyeződések nem befolyásolják az azonosítási folyamatot.

Nagy biztonságú beléptető rendszerekben is használható a magas azonosítási pontok száma miatt. A megtéveszthetősége szinte lehetetlen. A felhasználói elfogadottsága magas, minimális és rövid ideig tartó kontaktust igényel. Hátránya a magasabb eszköz költség. [68 pp. 78-81]

Írisz alapú azonosítás

Az írisz (szivárványhártya) a pupillát körülvevő, jól látható, színes gyűrű. Az írisz mérhető, bonyolult részletekből, úgynevezett csíkokból, gödrökből és barázdákból áll. Nincs két egyforma írisz; még az ember két írisze is teljesen más. Az egyetlen íriszben mérhető egyedi információ mennyisége sokkal nagyobb, mint az ujjlenyomatokban. Az azonosítás során infravörös világítják meg az íriszt és egy monokróm fényképet készítenek róla. Ezt a szegmentációs folyamat követi, ahol elkülönítésre, kiemelésre kerül az írisz a képből, majd egy poláris koordinátarendszer segítségével meghatározza az azonosításhoz szükséges zónákat (képrészleteket). A kódolási folyamat során a zóna adatokat (kép adatokat) összetett matematikai kifejezésekké, vektorokká alakítja át az algoritmus. Ezek a vektorok határozzák meg az alkép „mit” és „hol” részét.

Az íriszfelismeréshez a felhasználó aktív közreműködése szükséges, egy pillanatra mozdulatlanul a kamerába kell néznie. A rendkívül pontos és nagybiztonságú kontaktmentes (10-180cm) azonosítás miatt a bűnüldöző szervezetek (FBI) is rendszeresítették. Az azonosítás sikertelenségét a különböző szembetegségek (ernyedt szemhéj, szürkehályog), valamint a szemüveg viselése okozza.

Hangazonosítás

Az ilyen rendszerek a felhasználók egyedi hangmintájának analízisére épülnek, és ezeket használják az azonosításhoz. A rendszer során a felhasználók meghatározott

(jelszómondat) vagy szabad formájú hangmintát adnak, amelyet a rendszer rögzít és analizál. A hangminta elemzése a beszéd jellemzőinek, például a beszédritmusnak, a hangerőnek, a hangszínnek, valamint a beszédhangok és a beszédhangok közötti időközöknek a vizsgálatán alapul.
A hangazonosítás nem alkalmas önállóan magas biztonsági szintű azonosításra, azonban alacsonyabb biztonsági szinteken kombinálva másik biometrikus azonosítási folyamattal alkalmazható. Hátrányai közé sorolhatjuk a nagy fájl méretű hangsablonok tárolásának nehézkes körülményeit, az azonosítás relatív hosszú idejét (2-10mp), valamint az életkor változásával összefüggő hangszínváltozásokat.

Járás alapú azonosítás

A járásfelismerés során az egyén egyedi járásának mintázatát használja az azonosításhoz. A rendszer érzékelők segítségével, például kamerákkal, rögzíti a személy mozgását. Ezt követően a mozgási mintákat analizálja és összehasonlítja egy adatbázisban tárolt mintákkal. Ez a technológia lehetővé teszi a távoli és tömeges azonosítást, nem igényel közvetlen interakciót a felhasználóval, és a járás személyre szabott jellemzőinek köszönhetően nehéz hamisítani. Azonban a járásminták sok tényezőtől függenek, mint például a ruházat, a járófelület típusa, vagy a felhasználó egészségi állapota. Emiatt önálló biometrikus azonosításként nem használják, csak multimodális, vagy több faktoros azonosítás részeként.

Összefoglalás

Ebben a szakaszban a beléptető rendszerekhez kapcsolódó azonosítási eljárásokat jártam körül, feltárva a tudás-, tárgy- és biometriai alapú azonosítási módszerek lehetőségeit, előnyeit és hátrányait. A kiválasztott azonosítási módszerek és annak alkalmazásai alapvetően határozzák meg a beléptető rendszerek struktúráját és működését. Ugyanakkor nem szabad megfeledkeznünk arról, hogy a rendszerek hatékonyságát az irányadó szabványok és jogszabályok is befolyásolhatják (pl.: adatvédelmi jogszabályok).

4.4 Szabványok, ajánlások és jogszabályok Magyarországon

Ebben a fejezetben a beléptető rendszerek magyarországi szabályozási kérdését vizsgálom meg. Elsőként a honosított nemzetközi szabványokat és a hazai ajánlásokat helyezem a fókuszba, amelyek iránymutatást adhatnak a beléptető rendszerek kialakításában.

A fejezet második részében azokkal a magyarországi jogszabályokkal foglalkozom, amelyek hivatkoznak a beléptető rendszerekre. A jogi keretek ismerete elengedhetetlen ahhoz, hogy megértsük a beléptető rendszerek hazai alkalmazásának feltételeit és korlátait.

4.4.1 Hazai és nemzetközi szabványok és ajánlások

Az beléptető rendszerekkel kapcsolatban két nagy nemzetközi szabványcsomag került kiadásra. Elsőként az EN 5013x, majd ennek kiváltásaként az EN 60839. Magyarországon az EN 5013x szabványcsomag részben magyar nyelvű fordításban jelent meg, azonban az EN 60839 csak angol nyelven, esetenként magyar nyelvű előlappal került bevezetésre. Időrendi sorrendben az alábbi szabványok jelentek meg az elektronikus beléptető rendszerekkel kapcsolatban Magyarországon:

- 2000.12.01. **MSZ EN 50133-1:2000** - Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények [105]
- 2000.12.01. **MSZ EN 50133-7:2000** – Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek [106]
- 2001.05.01. **MSZ EN 50133-2-1:2001** - Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 2-1. rész: Részegységek általános követelményei [107]
- 2003.04.01. **MSZ EN 50133-1:1996/A1:2003** - Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények [108]
- 2006.09.01. **MSZ EN 50133-1:2006** - Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények [109]
- 2011.11.01. **MSZ EN 50130-4:2011** - Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsalád-szabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós

megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei [110]

- 2013.09.01. **MSZ EN 60839-11-1:2013** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-1. rész: Elektronikus beléptető rendszerek. A berendezésekre és készülékekre vonatkozó követelmények (IEC 60839-11-1:2013) [111]
- 2015.03.01. **MSZ EN 50130-4:2011/A1:2015** - Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsaládszabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei [112]
- 2015.08.01. **MSZ EN 60839-11-2:2015** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek (IEC 60839-11-2:2014) [113]
- 2017.07.01. **MSZ EN 60839-11-31:2017** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-31. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló alaprendszer interoperabilitási protokollja (IEC 60839-11-31:2016) [114]
- 2017.07.01. **MSZ EN 60839-11-32:2017** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-32. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló beléptetés monitorozása (IEC 60839-11-32:2016) [115]
- 2021.01.01. **MSZ EN IEC 60839-11-5:2021** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-5. rész: Elektronikus beléptetőrendszerek. Nyílt felügyelt eszközprotokoll (OSDP) (IEC 60839-11-5:2020) [116]
- 2022.02.01. **MSZ EN IEC 60839-11-33:2022** - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-33. rész: Elektronikus beléptetőrendszerek. A webszolgáltatásokon alapuló beléptetés konfigurálása (IEC 60839-11-33:2021) [117]

A fenti felsorolásból az MSZ EN 50133-X magyar nyelvű szabványsorozat visszavonásra került, helyét az MSZ EN IEC 60839-X angol szabványsorozat vette át. az **MSZ EN 60839-11-1:2013** szabvány a beléptető rendszerekre és azok komponenseire vonatkozó minimális funkcionalitást, teljesítménykövetelményeket és tesztelési módszereket

határozza meg a fizikai hozzáférés (be- és kilépés) szabályozására épületekben és védett területeken. Ez a szabvány azokra az elektronikus beléptető rendszerekre és komponensekre vonatkozik, amelyeket biztonsági alkalmazásokban (vagyonvédelmi rendszerekben) használnak a beléptetés (hozzáférés) engedélyezésére. A szabvány tartalmazza a naplózási, az azonosítási és az információk kezelésével kapcsolatos követelményeket. [111]

Az ebben a szabványban található előírások egy részét implementálta a Magyar Biztosítók Szövetsége Vagyonvédelmi és Kármegelőzési Bizottság (MABISZ VKB) által kiadott „Betöréses lopás- és rablásbiztosítás technikai feltételei" című ajánlás C/II. fejezete.

A fejezetben a következőképpen kerül meghivatkozásra a szabvány: *„A jelen ajánlásban vizsgált beléptető rendszer és elemei az MSZ EN 60839-11-1 szabvány biztonsági fokozatainak (security grade, G1-G4) figyelembevételével kerülnek besorolásra."* Ezt követően a szabvány négy osztályozási fokozatából hármat generál úgy mint: *„A alacsony biztonsági szintű, K közepes biztonsági szintű, M magas biztonsági szintű beléptető rendszer eleme"*.

4.4.2 Beléptető rendszerek megjelenése a magyar jogszabályokban

A magyar szűkebb jogszabályi környezetben (törvények és rendeletek) az elektronikus beléptető rendszerekkel kapcsolatos megemlítések a legtöbb esetben csak a beléptető rendszer használata során keletkező adatok kezelését szabályozza. Néhány jogszabályban a beléptető rendszerek valamely tágabb fogalom meghatározásának részeként jelennek meg. Például az 2005. évi CXXXIII. törvényben az elektronikus vagyonvédelmi rendszer részeként, a 2013. évi L. törvényben a fizikai védelem részeként szerepel a beléptető rendszer. [118 74.§ 6.][119 1.§ (1) 20.]

A 169/2010. (V. 11.) Kormány rendelet a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről című jogszabály 40/A.§ (4) pontjának b) alpontja alapján *„**kritikus elektronikus információnak vagy rendszernek minősíti** az utasoktól különböző személyek által használt **beléptető rendszereket** beleértve az elektronikus kapukat és egyéb ajtókat"*.

Azonban nagyobb számban olyan jogszabályokat találtam, amelyek előírják a beléptető rendszerek használatát, de nem határozzák meg annak követelményeit. [120]

A **53/2015. (IX. 24.) BM rendelet** az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges

kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről kiadott rendelet, a megszemélyesítés műszaki, technológiai, informatikai és biztonsági követelményei fejezetének 5. pontjában a megszemélyesítő tevékenység végzésének biztonsági feltételeinél előírja *„a megszemélyesítésben használt helyiségeket biztonsági kamerával, beléptető rendszerrel, riasztóval, tűzjelző berendezéssel”* történő felszerelését. [121]

A **33/2021. (IX. 15.) MNB rendelet** a fizetési rendszer működtetése tevékenységre vonatkozó részletes szabályokról című jogszabály a fizikai biztonsági feltételeit tartalmazó rész **23.§** (3) pontjában úgy fogalmaz, hogy „*A védendő helyiségek körére a rendszerüzemeltető a* ***kockázatokkal arányos védelmet biztosító beléptető rendszerrel rendelkezik****, amely biztosítja a személyek mozgásának visszakereshetőségét és egyértelmű azonosítását, ellenőrizhetőségét.*” Ebben a rendeletben az elektronikus vagyonvédelmi rendszer fogalom meghatározásában a következőképpen szerepel a beléptető rendszer: *„belépési jogok automatizált kezelését biztosító elektronikus berendezés”*. [122 2.§ 8.] Szakmailag elfogadható, lehet párhuzamot vonni a jogszabályon belüli két megjelenítési forma között. A kockázattal arányosságot az üzemeltetőknek kell meghatározniuk kockázatértékelést követően ez biztosítja számukra a különböző védelmi fokozatok kialakítását.

A **78/2015. (XII. 23.) BM rendelet** az arcképelemző rendszer működtetésének részletes szabályairól 11.§ (4) pontja alapján *„Az arcképelemző rendszer elhelyezésére szolgáló helyiségekbe történő beléptetés tekintetében a központi szerv* ***köteles elkülönített elektronikus beléptető rendszert működtetni,*** *továbbá köteles gondoskodni az objektumvédelemről.”* [123] Az *„elkülönített elektronikus beléptető rendszer”* kifejezés biztonságszakmai szempontból a beléptető rendszer szigetszerű kiépítését jelenti, valamint utal arra, hogy a helyiség kiemelten védelemmel rendelkezik. A „*Kiemelten védendő helyiségek esetében a biometrikus azonosítás, illetve a bizottsági típusú - legalább két személy együttes jelenlétét – megkövetelő megoldások alkalmazását is mérlegelni kell.*” [89 p. 119]

A **62/2009. (XII. 17.) IRM rendelet** a Közjegyzői Levéltár tevékenységével összefüggő szakmai követelményekről jogszabály, a levéltári anyag tárolásával összefüggő követelmények fejezetében a 26.§ (1) pontjában úgy fogalmaz, hogy *„****Megfelelő riasztó- és beléptető rendszerrel*** *kell biztosítani, hogy a levéltárba és a raktárhelyiségbe csak az arra feljogosított személyek léphessenek be.”* Jelen paragrafus (2) pontja alapján a levéltár a saját ügyrendjében szükséges, hogy meghatározza a „*a raktárhelyiségbe történő belépés*

feltételeit és a belépési jogosultságot". A jogszabályban szereplő „megfelelő" kifejezést biztonságszakmai szempontból nem tudom egzakt módon értelmezni, a védelmi cél és az eszköztár ismerete nélkül. [124]

A hazai törvények és rendeletek vizsgálata során összesen kettő olyan hatályos és nyilvános kormányrendeletet találtam, amelyekben **különböző védelmi szintekhez, különböző biztonsági szintű beléptető rendszert rendelt** hozzá.

A 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről kiadott, valamint a 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről kiadott jogszabályt.

A **90/2010. (III. 26.) Kormányrendelet** 26. § (1) előírja, hogy a biztonsági terület határán, valamint a Nyilvántartó és a Kezelőpont helyiségébe történő be- és kilépésre beléptető rendszert kell alkalmazni, ugyanakkor ennek a fogalomnak a definiálást nem végezték el a jogszabályban.[81] Ezen rendelet 1-4. kategorizálja a beléptető rendszereket (védelmi) tulajdonságait, ahol a 1. szint a leggyengébb, a 4. kategória a legerősebb védelmet jeleni.

Az 1. kategóriájú beléptető rendszernek felelti meg a kulccsal bezárt ajtót a ki és belépések adatainak manuális rögzítésével.

A 2. kategóriájú beléptető rendszerek esetén az ellenőrzés őrség vagy recepciósok alkalmazása által valósul meg. A belépés igazolvány felmutatása, a ki- és belépések manuális regisztrálása mellett történik.

A 3. kategória esetén a területre történő belépés **elektronikus kártyával vagy más ezzel egyenértékű eszközzel vagy PIN kód használatával** működik. A ki- és belépések regisztrálása elektronikusan történik.

A 4. kategóriájú beléptető rendszerről akkor beszélhetünk, ha teljesen automatikus, **elektronikus kártyával vagy más, ezzel egyenértékű eszközzel és PIN kód vagy biometrikus azonosító** használatával működik. Az áthaladás mechanikus sorompó vagy őrség által ellenőrzött, mely egyszerre egy személy áthaladását teszi lehetővé. A ki- és belépések regisztrálása elektronikusan történik.

Biztonságszakmai szempontból, csak a 3. és 4. kategóriában megfogalmazott előírások esetén beszélhetünk (elektronikus) beléptető rendszerekről. Az 1. kategóriában a rendelet se áttörésgátlási fokozatot, se biztonsági zárat nem ír elő. A 2. kategóriánál 5 perces áttörésgátlással rendelkező ajtót ír elő, azonban a zárszerkezetről nem rendelkezik a rendelet. Szakmai véleményem szerint a jogszabály ezen pontjának kiegészítése,

megerősítése szükséges a zárszerkezet, kategória szerinti védelmi fokozatának megjelölésével.

A **190/2011. (IX. 19.) Kormány rendelet** az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről kiadott jogszabályban a fizikai védelem részeként, detektálási funkcióval szerepelnek a beléptető rendszerek. Ebből a rendeletből is kimaradt a beléptető rendszerek definíciója.[3] A jogszabály ebben az esetben is négy fokozatot állapított meg egyes védelmi szinteknek (A-D) megfelelően, ahol az A fokozat a legerősebb, a D pedig a leggyengébb fizikai védelmi szintet jelöli.

Az A szintű fizikai védelem esetén a jogszabály [1] előírja a beléptető rendszerek tekintetében a biometrikus azonosítást, az olvasó-ellenőrző egységeket és az áteresztési pontokat. Azonban rendelet a beléptető rendszer elemként sorolja fel a különböző biztonsági átvizsgáló eszközöket is, a csomagvizsgálót, a robbanóanyag detektort, a fémdetektort és a sugárkaput.

A B és C szintű fizikai védelem esetén csak olvasó-ellenőrző egységek, személyazonosító elemek és áteresztési pontok szerepelnek a jogszabályban.

A D szintű fizikai védelem esetén a beléptető rendszer zárható ajtóból, valamint a belépési jogosultságok korlátozásból áll.

Ahogy az előző jogszabálynál, itt is észlelhető egy kis fogalomzavar a beléptető rendszerek tekintetében. Az A fizikai védelmi szintnél szerepelő, a biztonsági átvizsgálást megvalósítását végző eszközök nem tartoznak a beléptető rendszerekhez, azonban a beléptetéssel kapcsolatos eljárás részeként elfogadhatók. A D szintű védelemnél a jogszabály egy másik része előírja a minimum 3 perces betörésállóságot. Ezen kifejezés helyett inkább az áthatolási, vagy az áttörési ellenállási kifejezés használatát javasolnám. Összehasonlítva (6. számú ábra) az előző két jogszabályban szereplő kategorizálási rendszert, több ponton egyezőséget, megfeleltethetőséget találtam.

5. ábra Védelmi kategóriák összehasonlítása, a szerző saját szerkesztése

A magyar jogrendszerben további mélyebb kutatást folytattam, a hivatalos rendeletek és törvények mellett más forrásokat is áttekintettem. Meglepő módon csak egyetlen további helyen találkoztam a beléptető rendszerrel szembeni követelmények meghatározásával, mégpedig a 8/2021. (XI. 18.) OBH[39] utasítás a bírósági épületek fizikai védelmi rendszereinek feltételeiről címmel megjelent utasításának III. fejezetének 6. pontjában. Azonban beléptető rendszerekkel szembeni követelmények biztonságszakmailag hiányosan kerültek megfogalmazásra. [125]

4.5 Következtetések

Értekezésem ebben a fejezetében alaposan bemutattam az elektronikus beléptető rendszerek fogalmát és felépítését, amit az azonosítási eljárások részletes ismertetése - tudásalapú, tárgyalapú és biometria alapú - követett. Emellett részleteztem a nemzetközi és hazai szabványokat, valamint a magyar jogrendszerben érvényes beléptető rendszerekkel kapcsolatos jogszabályokat. A kutatásom során kiderült, hogy a magyar jogalkotás sajnálatos módon nem rendelkezik pontos vagy helyes definícióval a beléptető rendszerek fogalmát illetően, ami komoly problémákat okoz az iparágban.

[39] Országos Bírósági Hivatal

A hiányzó vagy téves definíciók következtében nem sikerül meghatározni a beléptető rendszerek fizikai és logikai követelményrendszerét. Ennek negatív hatásai jól érzékelhetőek lehetnek például a kritikus infrastruktúrák beléptető rendszereinek tervezése és működtetése során, ahol az egyértelmű szabályok és definíciók nélkülözhetetlenek a biztonság és hatékonyság szempontjából.

A kutatás során elemzett jogszabályok azt mutatják, hogy sürgős szükség van egy olyan tanulmány elkészítésére, amely célzottan foglalkozik az elektronikus beléptető rendszerek definíciójával és jogi keretrendszerével Magyarországon. A jövőbeni tanulmány feladata lesz az aktuális nemzetközi és technológiai trendek figyelembevételével egyértelmű és alkalmazható definíciók kidolgozása, amelyek hozzájárulnak a rendszerek hatékonyságának, biztonságának és rugalmas ellenállóképességének javításához. [126] Ezenkívül a tanulmány a jogalkotók és a szakemberek számára iránymutatást nyújthat a jogi keretrendszer aktualizálásához, és lehetővé teszi a jogszabályi háttér és definíciók rendszeres felülvizsgálatának elvégzését az újonnan felmerülő veszélyforrások és biztonsági kihívások kezelése érdekében.

Értekezésem következő fejezetében a kritikus infrastruktúrák korábban meghatározott védelmi zónáinak fizikai és elektronikai védelmi rendszereinek alapkövetelményeit mutatom be.

5 VÉDELMI ZÓNÁK ALAPKÖVETELMÉNYEINEK MEGHATÁROZÁSA

Ebben a fejezetben részletesen vizsgálom az egyes védelmi zónák fizikai, elektronikai és személyi feltételeit a védelmi funkciók szemszögéből. A védelmi zónák kialakítása és megfelelő működtetése elengedhetetlen a kritikus infrastruktúrák hatékony védelme érdekében. [127][128][129]

Először is, a fizikai feltételek elemzésével foglalkozom, amelyek a védelmi zónák fizikai kialakításához és struktúrájához kapcsolódnak. Ez magában foglalja az épületek és helyiségek megfelelő tervezését, a bejárati pontok biztosítását, az akadályok és korlátok elhelyezését, valamint a vészkiutasítási útvonalak és tűzvédelmi intézkedések biztosítását.[130][131]

Másodszor, az elektronikai feltételek vizsgálata során a különböző elektronikus eszközök és rendszerek szerepét és jelentőségét tárgyalom a védelmi zónákban. Ide tartoznak az elektronikus beléptető rendszerek, riasztórendszerek, kamera- és megfigyelőrendszerek, valamint a tűzjelző és tűzoltó rendszerek. Ezek az eszközök hozzájárulnak a zónák hatékony működéséhez és a veszélyek korai észleléséhez.[132]

Harmadszor, a személyi feltételek elemzése során a személyi erőforrásokat és képzést veszem figyelembe a védelmi zónákban. Ez magában foglalja a biztonsági személyzet, a vészhelyzeti csapatok és más munkavállalók képzését, valamint a megfelelő kommunikációs és koordinációs folyamatok kialakítását. A személyi erőforrások és a megfelelő képzés biztosítása kulcsfontosságú a zónák hatékony működéséhez és a váratlan helyzetek kezeléséhez.[61]

Végül, a védelmi funkciók szemszögéből értékelem az egyes védelmi zónákban alkalmazott intézkedéseket és eljárásokat. Ide tartozik a beléptetési és kijutási eljárások szabályozása, a hozzáférés-ellenőrzés és az azonosítás, a rendszeres ellenőrzések és auditok, valamint a vészhelyzeti tervek kidolgozása. Ezek a funkciók biztosítják a zónák hatékonyságát és a fenyegetésekkel szembeni védelmi képességet.[78]

Ezen elemzések és vizsgálatok alapján lehetőség nyílik a védelmi zónák megfelelő kiépítésére és működtetésére a kritikus infrastruktúrák védelme érdekében. A fejezet célja, hogy átfogó képet nyújtson a védelmi zónák fizikai, elektronikai és személyi feltételeiről a védelmi funkciók szemszögéből, és segítse a szakembereket a hatékony és megbízható védelmi rendszerek kialakításában és fenntartásában. [94][127]

5.1 0. védelmi zóna

A 0. védelmi zóna a kritikus infrastruktúra külső régiójában helyezkedik el, és fő célja a külső kerítés és az üzem/iroda épületek közötti terület védelmének biztosítása fizikai és elektronikus védelmi megoldásokkal, valamint biztonsági szolgálattal, amelyet a következőkben részletesebben ismertetek.

A kerítést a telekhatáron vagy a zárt terület határán kell elhelyezni, és legalább 2 méter magasnak kell lennie. A kerítést erős anyagból, például acélból vagy műanyag dróthálóból, az oszlopfelépítményeket szögacélból vagy betonból kell elkészíteni úgy, hogy legalább 5 másodperc legyen a szerkezet leküzdési ideje[40].

A főkapukat úgy kell kialakítani, hogy nyitott állapotban ellenőrzött módon biztosítsák a létesítmény személy- és gépjárműforgalmát. Ezeknek a kapuknak erős acélból kell készülniük, amely anyagban erősebb a kerítés anyagánál, így védelmet nyújtva a gépjárművel történő behatolással szemben. Emellett a kapuk magasságának legalább el kell érnie a kerítés magasságát. Fontos, hogy a kapuk távirányíthatóak legyenek, és motoros nyitószerkezettel legyenek ellátva.

A kerítés egyéb pontjain található kapuknak biztosítaniuk kell a tartalék behajtási lehetőséget, és segíteniük kell a karbantartási feladatok ellátását. Ezeknek a kapuknak anyagjukban egyenértékűnek kell lenniük a kerítés anyagával.

Az épületek falazatának meg kell felelnie a MABISZ (Magyar Biztosítók Szövetsége) által előírt teljeskörű mechanikai védelem követelményeinek. Ez magában foglalja legalább 3 perces áttörésgátlási képességet az ajtóknál, az RC2[41] védelmi szint elérését a zárszerkezeteknél, valamint a P4A[42] dobásálló védelmi fokozat alkalmazását az üvegfelületeknél. Ezek az előírások biztosítják a megfelelő fizikai védelmet és ellenállást a potenciális támadásokkal szemben a védelmi zónában.

Az elektronikus vagyonvédelmi rendszerek közül a kerítésvédelmi jelzőrendszer, a behatolásjelző rendszer és a videómegfigyelő rendszer kiemelt szerepet kap a védelmi zóna biztosításában. Ezek a rendszerek folyamatosan figyelik és detektálják a védelmi zónában történő eseményeket, beleértve a potenciális behatolási kísérleteket is. A kerítésvédelmi jelzőrendszer segítségével azonnal értesítés történik, ha valaki megpróbálja megszegni a terület határait.

---

[40] Leküzdési idő, azt az időtartamot értjük ez alatt, amely ahhoz szükséges, hogy a behatoló átjusson a kerítésen. Ezt az időtartamot lehet növelni például, úgynevezett mászásgátló kerítésszerkezetekkel.

[41] MSZ EN 1627:2021 alapján [133]

[42] MSZ EN 356:2000 alapján [134]

A zóna határán található bejáratoknál a személyforgalom ellenőrzésére azonosító rendszert kell telepíteni, amely lehetőséget nyújt az egyéni PIN-kód, proximity kártya vagy biometrikus azonosítás használatára. Ezek az azonosítási módszerek biztosítják, hogy csak az engedélyezett személyek léphessenek be a zónába, és segítik a pontos nyomon követést és az esetleges bejutási próbálkozások rögzítését. A lehetséges kültéri használat, valamint első vonalbeli beléptetési pont védelme érdekében, az azonosítást végző eszköz és a kontroller tokozatának/burkolatának IP6X[43] és IK10[44] védelmi fokozattal szükséges rendelkeznie.

Az érkező vendégek bejutását a recepcióra a védelmi zóna bejáratainál történő személyazonosítás követően a biztonsági szolgálat személyesen, vagy technikai eszközökkel biztosítja. Ez biztosítja, hogy csak azonosított és az engedélyekkel rendelkező vendégek léphessenek be a területre, és segíti a biztonsági szolgálatot a vendégek mozgásának és tartózkodásának nyomon követésében.

Ezenkívül, a biztonsági személyzet hatékonyabb feladatellátása érdekében ajánlott URH rádiós kommunikációs rendszer telepítése, amelyek lehetővé teszik a gyors és megbízható kommunikációt az őrséggel és a központi vezérlőközponttal.

Ezek a technikai megoldások komoly előnyöket nyújtanak a védelmi zóna szempontjából. Az események rögzítése és folyamatos ellenőrzése lehetővé teszi a gyors reagálást és a potenciális veszélyforrások azonosítását.

A kritikus infrastruktúra védelmével kapcsolatos intézkedéseket a biztonsági szabályzatban szükséges részletesen és átfogóan rögzíteni. Ez a dokumentum meghatározza a biztonsági folyamatok és eljárások, valamint a védelmi intézkedések részleteit a kritikus infrastruktúra területén. A biztonsági szabályzat célja a munkavállalók és vendégek biztonságának garantálása, valamint a kritikus infrastruktúra hatékony védelme és a fenyegetések időben történő felismerése és kezelése.

A szabályzatban kiemelt figyelmet kell fordítani a munkavállalók és vendégek belépésével és bent tartózkodásával kapcsolatos szabályokra és protokollokra. Ez magában foglalja az azonosítási eljárásokat, a belépési jogosultságkezelési eljárásokat, valamint a belépési ellenőrzőpontok kialakítását és működtetését. Amennyiben a 0. védelmi zónában parkolási lehetőség került kialakításra, akkor a behajtásra és a parkolásra vonatkozó részletszabályokat is szabályozni szükséges a kritikus infrastruktúra védelme érdekében.

[43] MSZ EN 60529:2015 alapján [135]
[44] MSZ IEC 62262:2023 alapján [136]

A biztonsági szabályzatnak részletesen ki kell térnie az őrszolgálati utasításra is. Ez az utasítás meghatározza az őrszolgálat feladatait, kötelességeit és tevékenységeit a kritikus infrastruktúra területén. Ide tartoznak a járőrözési kötelezettségek, a jelentési eljárások, az esetleges vészhelyzetekre való reagálás, valamint az információátadás folyamata. Az őrszolgálati utasítás biztosítja a folyamatos és strukturált őrzést az infrastruktúra területén, ami elengedhetetlen a potenciális fenyegetések időben történő észleléséhez és a gyors reakcióképesség biztosításához.

5.2 1. védelmi zóna

Az 1. védelmi zóna a kritikus infrastruktúra perifériás területén található, innen nyílik lehetőség a belső zónákba történő bejutásra. A zóna elsődleges védelmi funkciója a belső zónákba belépni szándékozó személyek, valamint a vendégek azonosítása és kontrolálása.

A fizikai védelem a falazatoknál a MABISZ szerinti teljeskörű mechanikai védelemnek megfelelő kialakítást, az ajtóknál pedig legalább 5 perces áttörésgátlási időt kell biztosítani. A zárszerkezeteknek az RC3[45] védelmi szintnek kell megfelelniük. Az ablakok esetében a P6B[46] áttörésbiztos fokozatot vagy legalább 6 mm vastagságú üvegezést kell alkalmazni, amelyet kívülről nem szerelhető fix vagy nyitható belső rácsszerkezet egészít ki. Ez a rácsszerkezet körbe hegesztett rácsból kell, hogy álljon, 140×140 mm-es kiosztású és 10 mm átmérőjű köracélból.

A recepciós helyiségnél további specifikus fizikai védelemre van szükség. Az üvegfelületeknél az átlövésgátló BR2NS[47] fokozatot kell alkalmazni, míg az ajtónak legalább az FB2[48] védelmi fokozatnak kell megfelelnie. A recepció falazatának is ezzel az egyenértékű védelmet kell nyújtania.

Az elektronikai védelem terén a videómegfigyelő rendszernek nem csak áttekintő képeket kell rögzítenie, hanem olyan felvételeket kell készítenie, amelyek alkalmasak a személyazonosításra. Emellett behatolásjelző rendszert szükséges kiépíteni nyitásérzékelőkkel, üvegtörésérzékelőkkel, falbontásérzékelőkkel, mozgásérzékelőkkel és támadásjelzővel. Javasolt továbbá automatikus tűzjelző rendszer kiépítése is a teljes körű biztonság fenntartása érdekében.

[45] MSZ EN 1627:2021 alapján [133]
[46] MSZ EN 356:2000 alapján [134]
[47] MSZ EN 356:2000 alapján [134]
[48] EN 1522:1998 alapján [137]

A recepciónál elhelyezett beléptető pontnál a személyek azonosítása beléptető kártya vagy biometrikus azonosítás segítségével történjen. A beléptető pontot fizikai kialakítását úgy kell megvalósítani, hogy csak egy személy belépését engedje, így kizárva a besurranás (tailgaiting) lehetőséget. Ehhez forgóvilla, forgókapu, gyorskapu vagy zsilip alkalmazható. [138] A beléptető rendszereknél alkalmazott anti-passback funkciók közül kötelezően a soft, „lágy" visszajelzés beállítása kötelező. A funkció ellenőrzi az áteresztési ponton áthaladók irányát és összehasonlítja az adatbázisában tárolt eseményekkel. Amennyiben a tárolt események között az adott személyre vonatkozóan az utolsó áthaladási adat azonos a vizsgált áthaladási iránnyal, akkor hang- és fényjelzést generál.

A recepciónál elhelyezett áteresztő ellenőrző pontnál telepített fémdetektor kapu és csomagröntgen biztosítja a belső zónákba irányuló személyek és csomagok átvizsgálását, megakadályozva a tiltott tárgyak, például fegyverek, szúró-vágó eszközök és adathordozók be- és kivitelét.

Az 1. védelmi zónában célszerű kialakítani a vendégek fogadására szolgáló tárgyalókat annak érdekében, hogy ne legyen szükség beléptetni őket a kritikus infrastruktúra belső zónáiba. Fontos megjegyezni, hogy a teljes 1. zónában tilos olyan hálózati végpontokat kialakítani, amelyek az irodai vagy üzemi hálózathoz csatlakoznak, ezzel minimalizálva az informatikai hálózat kompromittálódásának lehetőségét.

Az 1. védelmi zónában folyamatosan jelen kell lennie a biztonsági szolgálatnak. A biztonsági személyzet feladata a belépő személyek biztonságérzetének növelése, a beléptetéssel kapcsolatos feladatok ellátása, valamint a személy- és csomagátvizsgáló berendezések kezelése.

Az 1. védelmi zónához kapcsolódóan szükséges további szabályzatokat ki kell adni, amelyek részletesen meghatározzák a csomag- és személyátvizsgáló berendezések használatát, a vendégek fogadását és regisztrálását, valamint a biometrikus adatok kezelését.

5.3 2. védelmi zóna

A 2. védelmi zóna a kritikus infrastruktúra belső perifériás területén helyezkedik el, és magában foglalja az adminisztrációs irodákat, mérőlaboratóriumokat, műszaki helyiségeket és irattárakat.

A fizikai védelem terén az ajtóknál legalább 10 perces áttörésgátlási időt kell biztosítani, és a zárszerkezeteknek az RC4[49] védelmi szintnek kell megfelelniük. Az ablakok esetében a P7B[50] áttörésbiztos fokozatot vagy legalább 6 mm vastagságú üvegezést kell alkalmazni, amelyet kívülről nem szerelhető fix vagy nyitható belső rácsszerkezet egészít ki. Ez a rácsszerkezet körbe hegesztett rácsból kell, hogy álljon, 90×90 mm-es kiosztású és 10 mm átmérőjű köracélból.

Amennyiben nemzeti és külföldi "Szigorúan titkos" minősítésű adatokat kezelnek és tárolnak az irattárban, további mechanikai megerősítésre van szükség. Ebben az esetben az ajtónak és a zárszerkezetnek legalább 15 perces áttörésgátlást kell biztosítania. Az irattár falazatán található ablakokon, nyílásokon és áttöréseken fixen rögzített vagy a helyiségen belülről felszerelt, számkombinációs zárral kiegészített nyitható rácsszerkezetet kell telepíteni. A rácsoknak 70×70 mm-es kiosztásúaknak kell lenniük, és legalább 10 mm átmérőjű köracélból vagy legalább 10 mm oldalhosszúságú négyzetacélból kell állniuk, rácspontokon körbe hegesztett rácsszerkezetként.[51]

Az elektronikus vagyonvédelmi rendszereknek meg kell felelniük a MABISZ által előírt teljeskörű elektronikai jelzőrendszerekre vonatkozó követelményeknek. A mérőlaborok esetében javasolt a behatolásjelző rendszer kiegészítése vegyianyag-érzékelőkkel. A laboratóriumokban és az irattárban javasolt automatikus oltórendszerek kiépítése a személyek, tárolt anyagok és infrastruktúra védelme érdekében. A közműveket fogadó műszaki helyiségekben pedig javasolt speciális érzékelők, például gáz- vagy vízérzékelők, hozzáadása a behatolásjelző rendszerhez.

A beléptetési pontoknál azonosítókártya és PIN-kód, vagy legalább két faktoros biometrikus azonosítás szükséges. [139]

A 2. védelmi zónában javasolt véletlenszerű, maximum 2 óránkénti járőrszolgálatot szervezni a biztonsági szolgálat részéről. Amennyiben nincs kialakítva technikai

[49] MSZ EN 1627:2021 alapján [133]
[50] MSZ EN 356:2000 alapján [134]
[51] 90/2010 (III.26.) Kormány rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről alapján [81]

megoldás a MAK irattárba történő belépés ellenőrzésére, szükséges egy őrszolgálati pont felállítása.

A zónában található műszaki helyiségekbe, mérőlaborokba, dokumentációs és a MAK irattárakba történő belépési protokollokat külön-külön kell szabályozni. A laboratóriumokban előforduló heves vegyi reakciókat kiváltó anyagok hozzáférhetőségét és kezelését pedig külön laboratóriumi utasításokban javasolt szabályozni.

5.4 3. védelmi zóna

A 3. védelmi zóna, a kritikus infrastruktúra központi zónájának része, amely csak a 2. védelmi zónán belül alakítható ki. Ide tartozik az őrségközpont (biztonsági központ), a szerverszoba, a kommunikációs központ és az infrastruktúrák működését szabályozó részfolyamatok vezérlőtermei.

A fizikai védelem terén az ajtóknál legalább 15 perces áttörésgátlási időt kell biztosítani, és a zárszerkezeteknek az RC5[52] védelmi szintnek kell megfelelniük. Az ablakok, üvegfelületek és falazatok esetén a BR2NS védelmi fokozatnak megfelelő védelmet kell kialakítani. A nehezen hozzáférhető üvegfelületek tekintetében elfogadható az ajtóknál meghatározott 15 perces áttörési fokozat biztosítása, illetve olyan fixen rögzített vagy a helyiségen belülről felszerelt, számkombinációs zárral kiegészített nyitható rácsszerkezet, amely 70×70 mm-es kiosztású és legalább 10 mm átmérőjű köracélból vagy legalább 10 mm oldalhosszúságú négyzetacélból áll rácspontokon körbe hegesztett rácsszerkezetként.

Az őrségközpont üvegfelületeinek BR7NS[53], a bejárati ajtóinak FB7[54] védelmi fokozat kell biztosítania. Az őrségközpont falazatát az FB7 védelmi fokozattal egyenértékűen kell kialakítani. A helyiségbe történő belépésnél zsilipes beléptetést kell megvalósítani, amelyet rendkívüli esemény bekövetkeztekor egy veszélyhelyzeti kapcsolóval felül lehet írni a gyorsabb reagálás érdekében. A belső térből nyíló biztonságtechnikai szerverszobát EMC[55] védelemmel szükséges ellátni annak érdekében, hogy a szerverek és más elektronikus berendezések zavartalanul működjenek anélkül, hogy az elektromágneses interferencia negatív hatással lenne rájuk. Az EMC védelem növeli a biztonsági

[52] MSZ EN 1627:2021 alapján [133]
[53] MSZ EN 356:2000 alapján [134]
[54] EN 1522:1998 alapján [137]
[55] Az EMC védelem olyan intézkedések és tervezési megoldások összessége, amelyek az elektronikai berendezések és rendszerek érzékenységét csökkentik az elektromágneses interferencia (EMI) hatásaira, biztosítva ezzel a zavartalan működést és az adatintegritást.

rendszerek megbízhatóságát, csökkenti a kieséseket és hibákat, biztosítva az adatintegritás, a stabil és folyamatos működést.

A szerverszobába történő beléptetést személyi zsilippel szükséges megvalósítani, amely biztosítja a helyiségbe belépők egyenkénti azonosítását. A rendszer kiegészíthető súlyellenőrzéssel, vagy fémkeresővel is. A szerverszobát és a kommunikációs központot is EMC védetten szükséges kialakítani.

Az informatikai hálózat tekintetében az 0-2. zónákban kiépített irodai hálózat nincs összeköttetésben a 3-4. zónákban található üzemi hálózattal. A 0-4. zónákban kiépített biztonsági hálózat az egyetlen, amely átfogja a teljes kritikus infrastruktúrát, ezért erre a hálózatra kizárólag megfelelő azonosítást követően lehet felcsatlakoztatni eszközöket. Kiemelten fontos a hálózati végpontok logikai és fizikai védelme is.

A szerverszobába, a kommunikációs központba és a vezérlőtermekbe történő belépési jogosultságok szigorú szabályozása megkövetelt, kitérve a rendszeres jogosultságfelülvizsgálatra. Amennyiben szükséges külsős munkavállaló, vagy vendég belépésének biztosítása, azt beléptető rendszer vendég kísérési funkciójával lehet megvalósítani.

5.5 4. védelmi zóna

A 4. védelmi zóna, a kritikus infrastruktúra központi zónája. Úgy kell kialakítani, hogy kizárólag a 3. védelmi zónán belülről legyen megközelíthető. Ebbe a zónába került besorolásra a kritikus infrastruktúra központi vezérlőhelyiségei. Ilyen helyiségek például az erőművek vezérlői, a nemzetközi repülőterek irányítótornyai, katonai létesítmények irányító központjai, vagy biológiai/virológiai laboratóriumok. Az a közös ezekben a helyiségekben, hogy az illetéktelen bejutás olyan károkat okozhat az infrastruktúrákban, amelyeknek jelentős, közvetlen hatással lehetnek a társadalomra vagy a gazdaságra.

A fizikai védelemi rendszereket alapját a MABISZ szerinti 20 perces áttörésgátlású ajtó RC6[56] védelmi fokozatú zárszerkezettel és FB7[57] átlövésgátló kialakításban, továbbá BR7NS[58] védelmi fokozatú üvegfelületek, valamint ezzel egyenértékű védelemmel rendelkező falfelületek alkotják.

[56] MSZ EN 1627:2021 alapján [133]
[57] EN 1522:1998 alapján [137]
[58] MSZ EN 356:2000 alapján [134]

A beléptetési pontot zsilip-szerűen kell kialakítani biztosítva az egyszemélyi belépést. A zsilipben további biztonsági megoldásokat lehet alkalmazni, mint a súlyérzékelés, fémdetektor, vagy akár sugárzó anyag detektálás. A 4. zónába történő beléptetéshez több faktoros biometrikus azonosítás és belépőkártya szükséges azzal a beállítással, hogy több személynek kell egy adott időintervallumon belül azonosítania és engedélyeznie a belépni szándékozó személyt. Szintén az elektronikus beléptető rendszerben szükséges beállítani a bent tartózkodók számának figyelését, meg kell határozni egy minimum és egy maximum értéket, amely alatt és felett riasztás generálódik.

Az őrszolgálatnak ellenőrző pontokat kell kialakítania a 4. zóna összes bejáratánál. Részt kell venniük a belépő személyek belépési jogosultságainak ellenőrzésében, valamint folyamatosan figyelemmel kell kísérniük a zónán belülről érkező biztonságtechnikai jelzéseket és a videómegfigyelő rendszer által biztosított kameraképeket.

Meg kell határozni a beléptetéssel kapcsolatos különleges szabályokat, valamint a veszélyhelyzeti forgatókönyveket, azaz ki, mikor és hogyan léphet be a zónába rendkívüli eseménykor. A rendkívüli eseményekkel kapcsolatban szükséges kiépíteni olyan ellenőrzött és naplózott technikai megoldást, amely segítségével az egyszemélyes zsilipes beléptetési funkció felülírható és biztosítható a gyors reakció.

5.6 Segédlet

A kritikus infrastruktúrák beléptető rendszereinek tervezése és kialakítása során nem elegendő a logikai felépítés, és a zónatulajdonságok elvi meghatározása. Annak érdekében, hogy működőképes és hatékony biztonsági rendszer tudjunk létrehozni, létrehoztam egy konkrét útmutatót, egy olyan segédletet, amely lehetőség szerint minden lehetséges helyszín és körülmény esetére részletes, továbbá az alkalmazandó megoldást egyértelműen megjelölő, de egyben komplex megoldási javaslattal szolgál. [135]

A következőkben bemutatásra kerül követelmény csoportokra osztva, az egyes védelmi zónák fizikai és beléptetési követelményeit tartalmazó segédlet táblázatos formában.

A táblázatokban rögzített információk a kutatásom eredményeként került rögzítésre.

	Védelmi zóna száma				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Fizikai biztonsági követelmények					
Belépési pont áttörési/áthatolási ellenállóképessége MABISZ szerint (perc)	3	5	10 15[59]	15	20
Zárszerkezet védelmi szintje MSZ EN 1627:2021 alapján	RC2	RC3	RC4	RC5	RC6
Üvegfelület védelmi szintje MSZ EN 356:2000 alapján	P4A	P5A, BR2NS[60]	P7B	BR2NS, BR7NS[61]	BR7NS
Ajtó lövedékállósági fokozata EN 1522:1998 alapján		FB2[62]		FB7[63]	FB7
Falazat védelmi fokozata	MABISZ szerinti teljeskörű	MABISZ szerinti teljeskörű, FB2-vel egyenértékű [64]	MABISZ szerinti teljeskörű	MABISZ szerinti teljeskörű, FB7-tel egyenértékű [65]	FB7-tel egyenértékű
Rácskiosztás mérete		140x140mm	90x90, 70x70mm[66]	70x70	70x70
Azonosítási követelmények					
Azonosítási módszer típusa	tudás **vagy** tárgy **vagy** biometrikus	tárgy **vagy** biometrikus	tárgy **és** biometrikus vagy tárgy **és** tudás	tárgy **és** biometrikus	tárgy **és** biometrikus
Azonosítási faktor száma	1	1	2	2	3

4. táblázat Fizikai és azonosítási követelmények összefoglalása, a táblázatot a szerző szerkesztette

[59] Nemzetközi, vagy nemzeti „Szigorúan titkos!” minősítésű iratok kezelése és tárolása esetén.
[60] Recepciós helyiségnél
[61] Biztonsági/védelmi központnál
[62] Recepciós helyiségnél
[63] Biztonsági/védelmi központnál
[64] Recepció helyiségnél
[65] Biztonsági/védelmi központnál
[66] Nemzetközi, vagy nemzeti „Szigorúan titkos!” minősítésű iratok kezelése és tárolása esetén.

Jelmagyarázat:

K: kötelező követelmény,

O: opcionális, választható követelmény,

T: tiltott követelmény,

-: nem értelmezhető követelmény.

	Védelmi zónák				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Logikai követelmények					
Azonosítási faktor száma	1	1	2	2	3
A védelmi zónába történő belépéshez jogosultság szabályozást kell meghatározni	K	K	K	K	K
A védelmi zónából történő kilépéshez jogosultság szabályozást kell meghatározni	O	K	K	K	K
Hard anti-passback	O	O	K	K	K
Soft anti-passback	O	K	T	T	T
Global anti-passback	O	O	O	K	K
Anti-passback felülbírálása/letiltása	O	K	K	K	K
Időzített anti-passback	O	O	O	K	K
A belépési jogosultság érvényességi időhöz kötött	K	K	K	K	K
A belépési jogosultság érvényességi időjénél meghatározható az év, a hónap, a nap, az óra és a perc	O	O	K	K	K
A beléptető rendszer rendszernek képesnek kell lennie több konfigurálható nap kezelésére (pl. törvényi ünnepnapok, speciális munkanapok és nem munkanapok)	H	K	K	K	K
Vendég/látogató kísérési jogosultság	O	K	K	K	K
Több vendég egyidejű felügyelt beengedése	O	O	T	T	T
Tailgating, piggybacking tiltása	O	K	K	K	K
Lift/lépcsőház használati jogosultság	O	O	O	O	O
Kizárólag tudás alapú azonosítás	O	-	-	-	-
Tárgy alapú azonosítás	O	O	K	K	K
Biometria alapú azonosítás	O	O	O	K	K
A tárgya alapú azonosítás kombinálása tudás, vagy biometria alapú azonosítással	O	-	K	-	-

Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Minimum 6 numerikus, vagy alfanumerikus karakter a tudás alapú azonosításnál	K	-	K	-	-
A tudás alapú kódoknál nem megengedett az egymást közvetlenül követő számjegy-, vagy betűsorozatok használata	K	-	K	-	-
Két jogosult személy egyidejű belépésének alkalmazása (Dual access)	-	-	O	O	K
Adott zónán belüli egyedi jogosultság biztosítása felhasználóként	O	K	K	K	K
Konfigurálható beléptetési időszakok minimális száma.	4	4	8	8	8
Valós idejű időszinkronizálás a szerver és vezérlő egységek között 24 óránként	K	K	K	K	K
A szerver órájának szinkronizálása valós idővel (pl.: GPS) minimum 24 óránként	K	K	K	K	K
A hozzáférést meg kell tagadni minden egyes, érvénytelen memorizált információval rendelkező érvényes kártya használatával történő hozzáférési kísérlet után, és előre meghatározott számú sikertelen próbálkozás után az adott kártya hozzáférési jogosultságait előre beállított időtartamra felfüggesztik. A próbálkozások száma konfigurálható. Ahol nem konfigurálható, a próbálkozások számát 5-re kell korlátozni	O	-	K	-	-
Hamis elfogadás maximális aránya	1%	1%	0,30%	0,30%	0,10%
A teljes áramkimaradást követően a beléptető rendszer automatikus újraindítása szükséges az elsődleges áramforrás helyreállításakor	K	K	K	K	K
Ha az automatikus újraindítást követően a beléptető egység teljes működőképessége nem állítható vissza (az adatok megsérültek vagy elvesztek), akkor hibaállapotot kell közölni	K	K	K	K	K

5. táblázat: Logikai követelmények meghatározása, a táblázatot a szerző szerkesztette

	Védelmi zónák				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Azonosító eszköz / olvasó / billentyűzet					
Az áthaladás engedélyezésekor vizuális és/vagy hangjelzés szükséges	K	K	K	K	K
Az áthaladás megtagadásakor vizuális és/vagy hangjelzés szükséges	K	K	K	K	K
Az áthaladási pont zárolt állapotának vizuális és/vagy hangjelzése a hozzáférés engedélyezéséig	K	K	K	K	K
Az előre definiált nyitvatartási idő lejártát követően hang- és fényjelzés	O	K	K	K	K
Az azonosítást végző eszköz tokozatának minimálisan meg kell felelnie az előírt IP besorolásnak	IP6X	IP4X	IP4X	IP5X	IP5X
Az azonosítást végző eszköz tokozatának minimálisan meg kell felelnie az előírt IK besorolásnak	IK10	IK04	IK06	IK08	IK10
Az azonosítást végző eszköz tokozatának megbontását hang- és fényjelzéssel kell helyben és a felügyeleti központban jelezni	K	K	K	K	K
A PIN-kód beviteli billentyűzet minden gombjának lenyomása azonos hang- és fényjelzést kell adnia	K	-	K	-	-
Az azonosító eszközökben eltárolt információkat védeni kell a jogosulatlan módosítás vagy a másolás ellen	K	K	K	K	K
Normál üzemmódban a rendszer tárgy alapú azonosító összes információt (létesítménykód és kártyaszám vagy egyedi kártyaszám) használja a felismeréshez.	K	K	K	K	K
Több létesítménykód támogatása, ha a rendszer létesítménykódolást használ	K	K	K	K	K
A szabad szemmel látható kódrendszerű tárgy alapú azonosítókat nem szabad használni	K	K	K	K	K
A tárgyalapú azonosító eszközön olvasható azonosító szám nem tartalmazza a teljes egyedi azonosítót	K	K	K	K	K

6. táblázat Azonosítással kapcsolatos követelmények, a táblázatot a szerző szerkesztette

	Védelmi zónák				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Kontroller / vezérlő egység					
A nyithatósági időtartam a kontroller által definiált	O	K	K	K	K
A nyithatósági időtartam belépési pontonként külön definiálható	O	K	K	K	K
A nyithatósági időtartam belépési jogosultságonként külön definiálható (pl. mozgássérült, szállítás)	O	O	O	O	O
A belépési pont nyitott állapotának megengedett időtartamát a kontroller határozza meg	O	T	T	T	T
A belépési pont nyitott állapotának megengedett időtartama áthaladási pontonként konfigurálható	O	K	K	K	K
A belépési pontnál többféle nyitvatartási idő konfigurálható a belépési jogosultságoknak megfelelően.	O	O	O	O	O
Az azonosítási eseményeket naplózni szükséges	K	K	K	K	K
Hang- és fényjelzés, valamint naplózás szükséges a kényszernyitáskor	K	K	K	K	K
A kontroller belső elemeihez való hozzáféréshez speciális eszközt kell használni	O	K	K	K	K
A kontroller eltávolítása a felszerelési helyéről, vagy a tokozásának megbontása szabotázsjelzést generál a felügyeleti központban	K	K	K	K	K
A kontroller eszköz tokozatának meg kell felelnie az előírt IP besorolásnak	IP6X	IP4X	IP4X	IP5X	IP5X
A kontroller eszköz tokozatának meg kell felelnie az előírt IK besorolásnak	IK10	IK04	IK06	IK08	IK10
A vezérlőegység(ek) és a központi szerver közötti kommunikáció megszakadása esetén a vezérlőegység által tárolandó események minimális száma áthaladási pontonként	1000	1000	1000	1000	1000
A kontroller automatikus nyitást biztosít a tűzjelző rendszertől érkező jelzésre	K	K	K	O	O

Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Vagyonvédelmi rendszerű (fail-secure) zárás biztosítása áramkimaradás esetén	O	O	O	K	K
Az áteresztési pont egyszeri távoli nyithatósága	O	O	O	O	T
A rendszer összes áteresztési pontjának egyszeri távoli nyithatósága	O	O	O	O	T
Nyithatóság biztosítása a további rendszerparancsig, egyetlen vagy több áthaladási pont esetében	O	O	O	O	T
Áthaladási pont blokkolása további rendszerparancsig, egyetlen vagy több áthaladási pont esetében	O	O	O	O	O
Egyetlen vagy több áthaladási pont ütemezett/időzített blokkolása	O	O	O	O	O

7. táblázat: Vezérlő egységgel kapcsolatos követelmények, a táblázatot a szerző szerkesztette

Védelmi zónák

Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Kommunikáció					
Titkosítás szükséges az elektronikus beléptető rendszer összetevői között (szerver, kontroller, azonosító eszköz, kliens)	O	K	K	K	K
A kontroller és a szerver közötti kommunikáció meghibásodása vagy helyreállása nem eredményezheti az áteresztési pont nyitását	K	K	K	K	K
A központi szerverrel való kommunikáció meghibásodása nem szakíthatja meg a hozzáférési döntési folyamatot	K	K	K	K	K
A kommunikáció meghibásodásának hang- és fényjelzése, valamint naplózása a felügyeleti központban	O	K	K	K	K
A használati utasításnak tartalmaznia kell az olvasók és a beléptető egység közötti kommunikációs vezetékekhez való hozzáférést korlátozó mechanikai védelem telepítési követelményeinek részleteit.	O	K	K	K	K

8. táblázat: Kommunikációval kapcsolatos követelmények, a táblázatot a szerző szerkesztette

	Védelmi zónák				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Energiaellátás					
Sem az elsődleges áramforrás elvesztése, sem a helyreállítás nem befolyásolhatja hátrányosan a rendszer normál működését.	O	K	K	K	K
A teljes áteresztési pont működési ideje az elsődleges áramforrás kiesése esetén készenléti áramforrásról (óra)	1	2	2	4	4
Elsődleges tápellátás hiba jelzése és naplózása	K	K	K	K	K
Készenléti tápellátási hiba jelzése és naplózása (alacsony akkumulátorfeszültség és nincs akkumulátor)	O	K	K	K	K
Elsődleges tápellátás helyreállásának jelzése és naplózása	K	K	K	K	K

9. táblázat: Energiaellátással kapcsolatos követelmények, a táblázatot a szerző szerkesztette

	Védelmi zónák				
Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Rendszerfelügyelet					
A beléptetési pontot felügyelete	O	K	K	K	K
Bent tartózkodók számlálása	O	K	K	K	K
Felhasználó követése	O	K	K	K	K
Vizuális jelzés, riasztás és naplózás szükséges a hozzáférés megtagadásához egy lejárt érvényességű tárgy alapú azonosító használatának kísérlete miatt	K	K	K	K	K
Vizuális jelzés, riasztás és naplózás szükséges a hozzáférés megtagadásakor érvénytelen PIN kód miatt	K	-	K	-	-
A belépési pontok riasztásainak vizuális jelzése a grafikus felügyeleti állomáson	K	K	K	K	K
Ütemezett portálállapot-módosítás (nyitás, blokkolás)	O	O	O	O	O
Kézi portálállapot-módosítás (nyitás, blokkolás), naplózás szükséges	O	O	K	K	K
A konfigurációs módba történő be- és kilépés naplózása, megjelenítése	O	K	K	K	K

Követelmények	**0. zóna**	**1. zóna**	**2. zóna**	**3. zóna**	**4. zóna**
Minden eseményt típus, hely, időpont és időpont szerint azonosítani kell	O	K	K	K	K
A riasztásoknak tartalmazniuk kell az adott prioritási szintjük jelzését, ha a rendszer lehetővé teszi ilyen prioritási szintek kijelölését	K	K	K	K	K
Az egyidejűleg kapott riasztásokat prioritási sorrendben kell megjeleníteni, ha a rendszer lehetővé teszi ilyen prioritási szintek hozzárendelését	K	K	K	K	K
Az áthaladási pont kényszerített nyitásának hang- és fényjelzése	K	K	K	K	K
Az olvasó állapotának jelzése (on/off-line) a felügyeleti központban	K	K	K	K	K
A naplófálj maximális kapacitásának 90%-os elérése esetén jelzés generálása a felügyeleti központban	K	K	K	K	K
Hang- és fényjelzés, valamint naplózás szükséges, ha a bent tartózkodok létszáma nincs a kritériumon belül	-	-	-	O	K
A beléptető rendszerben történő operátori beavatkozást rögzíteni kell a típussal, az operátorazonosítóval, az esemény időpontjával és dátumával	K	K	K	K	K
A riasztásokhoz fűzött operátori megjegyzéseket az operátori azonosítóval, a megjegyzés beírásának időpontjával és dátumával együtt kell naplózni.	O	K	K	K	K
A naplózott információkhoz való hozzáférést az események lekéréséhez (pl. megjelenítése, nyomtatása, exportálása) az operátori azonosítóval, az esemény időpontjával és dátumával kell naplózni.	K	K	K	K	K
A felügyeleti állomás felhasználói hozzáférési szintjeinek minimális száma	1	2	2	4	4
A rendszeradminisztrációhoz, beleértve a konfigurációt is, csak érvényes hitelesítő adatok használatával lehet logikailag hozzáférni.	K	K	K	K	K

Követelmények	0. zóna	1. zóna	2. zóna	3. zóna	4. zóna
Logikai hozzáférési hitelesítő adatokat csak a rendszergazda rendelhet hozzá	K	K	K	K	K
A gyártó által a logikai hozzáféréshez előre beállított értékek felülírhatók	K	K	K	K	K

10. táblázat: Rendszerfelügyelettel kapcsolatos követelmények, a táblázatot a szerző szerkesztette

5.7 Összefoglalás

A biztonsági kockázatok csökkentése érdekében elengedhetetlen a kritikus infrastruktúrák védelmével összefüggő jogi szabályozás hiányosságaiból adódó problémák megoldása. Ennek alapját – a kritikus infrastruktúrák eltérő jellege miatt – a hasonlóságok felkutatása, és az egyes hasonlóságokhoz külön-külön kapcsolható, egységes biztonsági megközelítés alkalmazása képezi, amely leghatékonyabban a kritikus infrastruktúrák védelmi zónarendszerének kialakításával érhető el.

A zónarendszer alkalmas a védelem egyéb összetevőinek hatékony kialakítására is, de kutatásom célja kiemelten a beléptető rendszerek – mint a szándékos károkozó tevékenységek megelőzésére szolgáló, elsőszámú védelem-technikai megoldás – alkalmazásával összefüggő egységes szemlélet, és gyakorlati megoldás kidolgozása.

A beléptető rendszerek kialakításához a védelmi zónák és azok jellemzőinek meghatározása nyilvánvalóan csak az egyes zónákhoz tartozó követelmények, azaz az ott alkalmazandó beléptető rendszerek műszaki-technikai és biztonsági feltételeinek teljesülése mellett adnak valós segítséget, ezért a jelen fejezetben, kidolgoztam a kritikus infrastruktúrák egyes védelmi zónáihoz kapcsolódó, a hazai és a nemzetközi szabályozás, illetve a gyakorlati tapasztalatok alapján meghatározott minimális, tárgyi és szervezési feltételeket is tartalmazó beléptetési követelményrendszer logikai és fizikai egységét.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kritikus infrastruktúrák védelmének és biztonságának fenntartása, azaz az ilyen létesítmények biztonsági kockázatainak csökkentése érdekében elengedhetetlen a védelmükkel összefüggő jogi szabályozás hiányosságaiból adódó problémák megoldása. Ennek alapját – a kritikus infrastruktúrák eltérő jellege miatt – a hasonlóságok felkutatása, és az egyes hasonlóságokhoz külön-külön kapcsolható, egységes biztonsági megközelítés alkalmazása képezi, amely leghatékonyabban a kritikus infrastruktúrák védelmi zónarendszerének kialakításával érhető el.

A védelmi zónák tulajdonságaihoz, nevesítéséhez kapcsolódnia kell a hazai és a nemzetközi szabályozás, illetve a gyakorlati tapasztalatok alapján meghatározott minimális, tárgyi és szervezési feltételeket is tartalmazó beléptetési követelményrendszer logikai és fizikai egységéhez.

Bár a zónarendszer önmagában is segítséget nyújt a védelem egyéb összetevőinek hatékony kialakítására, de a megfelelően kialakított beléptető rendszer a szándékos károkozó tevékenységek megelőzésére szolgáló olyan elsőszámú védelem-technikai megoldásként kezelendő, amely egységes biztonságszakmai szemléleten alapuló, részletes gyakorlati útmutató szerint épül fel.

A fenti feltételek teljesülése és alkalmazása mellett létrehozható bármilyen típusú kritikus infrastruktúra megfelelő védelmi stratégiája és hatékony beléptető rendszere, amely a megfelelő jogszabályi keretrendszer kialakítása és fenntartása mellett elősegíti a kritikus infrastruktúrák hosszú távú stabil és biztonságos működését.

A kutatómunka összegzése

A kezdeti kutatási szakaszban végzett munkám keretében mélyinterjúkat készítettem hazai és nemzetközi biztonsági vezetőkkel, valamint biztonsági szakértőkkel, a kritikus infrastruktúrák fizikai és digitális védelmi rendszereinek szabályozási környezetére vonatkozóan.

Az átfogó jogi keret megértése érdekében áttekintettem és összegyűjtöttem a releváns európai uniós és magyarországi jogszabályokat, amelyek a kritikus infrastruktúrákat szabályozzák.

Az interjúk és a jogszabályi környezet értékelése után arra a következtetésre jutottam, hogy több országban, beleértve Magyarországot is, hiányosságok tapasztalhatók a kritikus infrastruktúrák védelmi előírásainak definiálásában. A hazai jogszabályok között a jogalkotó egyedül az atomenergia alkalmazási körében fogalmaz meg konkrét fizikai védelmi előírásokat.[3]

Az összegyűjtött információk és az azokból levont szükségletek alapján sikerült kialakítanom egy olyan módszertant, amely lehetővé teszi a kritikus infrastruktúrák védelmi zónáinak definícióját. A kijelölt védelmi zónákhoz társított minimális fizikai és elektronikus védelmi követelményeket is meghatároztam, amelyek elősegítik a tervezési, kivitelezési és auditálási folyamatokat.

Új tudományos eredmények

Tézis1: **Meghatároztam a kritikus infrastruktúrák védelmi zónáit, amely kulcsfontosságú a potenciális incidensek hatásainak kezelése során.** A zónák szerinti osztályozás lehetővé teszi a védelmi erőforrások hatékony allokációját, maximalizálva ezzel a rendszer ellenállóképességére gyakorolt hatásukat. Ezen túlmenően, a zónák szerinti osztályozás lehetővé teszi a kockázatkezelési stratégiák finomítását, figyelembe véve az egyes zónákban lehetséges legsúlyosabb eseményeket és azok hatását a kritikus infrastruktúra működésére.

Korábban a jogszabályi környezet csak a sugárzó anyagok kezelésével kapcsolatos védelmi zónák meghatározását tartalmazta, azonban ez a rendszer nem volt átfogó és nem volt minden esetre alkalmazható, mivel nem vette figyelembe a kritikus infrastruktúrák sokféleségét és a velük járó különböző kockázatokat.

A hipotézis alapján létrehozott új rendszer azonban átfogó, minden kritikus infrastruktúra esetében alkalmazható védelmi zóna-besorolási rendszer, amely figyelembe veszi mind a fizikai, mind az elektronikus védelmi követelményeket. Ez lehetővé teszi a modern társadalmakban a kibertámadások és más elektronikus fenyegetések növekvő jelentőségének megfelelő kezelését. Az új rendszerrel a különböző területek hatékonyabban oszthatók be zónákba és kezelhetők, ezáltal növelve a kritikus infrastruktúrák rugalmas ellenállóképességét.

Tézis2: **A disszertációmban bizonyítottam, hogy meghatározhatók a kritikus infrastruktúrák beléptető rendszereihez társított alapkövetelmények**, figyelembe véve a korábban általam definiált védelmi zónákat. A megközelítésem integráltan

vizsgálja a nemzetközi és hazai szabályozásokat, valamint a gyakorlati tapasztalatokat, így egyedülálló lehetőséget kínál a beléptető rendszerek követelményrendszerének továbbfejlesztésére.
A kritikus infrastruktúrák közös jellemzői, mint a magas biztonsági szint, a folyamatos működési követelmények, az üzemzavarok minimalizálása és a szigorú adatvédelmi előírások, alapjául szolgálnak a beléptető rendszerek alapkövetelményeinek. Ezek a rendszerek képeseknek kell lenniük az adekvát felhasználóazonosításra, a belépő személyazonosságának ellenőrzésére, és az adatok biztonságos kezelésére. Az új rendszer figyelembe veszi a kritikus infrastruktúrák általános alapelveit, reagál a legújabb technológiai trendekre, és értékeli a védelmi zónák jelentőségét.

Tézis3: **A disszertációmban bizonyítottam, hogy az általam meghatározott alapkövetelmények alapján megalkotható egy olyan segédlet, amely komplex támogatást nyújt a kritikus infrastruktúrák beléptető rendszereinek tervezéséhez és kialakításához**. Ez a segédlet átfogó, univerzális eszköznek bizonyulhat, amely a tervezők, kivitelezők, megrendelők, üzemeltetők, és auditálók számára is hasznos iránymutatást ad a beléptető rendszerek kialakításának és működtetésének minden szakaszában.
A segédlet használatával az érintett felek képesek lesznek optimálisan kiválasztani a beléptető rendszert, mely figyelembe veszi a különböző jogszabályi előírásokat, a technológiai fejlődést, és a kritikus infrastruktúrák egyedi igényeit. Az általam létrehozott segédlet hozzájárulhat a kritikus infrastruktúrák védelmének erősítéséhez és elősegítheti a hatékony és biztonságos beléptető rendszerek kiválasztását és alkalmazását.

Javaslat a kutatómunka folytatására

A disszertációm során végzett kutatások és megállapítások alapján megfogalmaztam javaslatokat, melyeket fontosnak tartok a kritikus infrastruktúrák biztonságának további erősítéséhez.

Először is, szükségesnek látom a beléptető rendszerek fogalmának egységesítését a magyarországi jogszabályi környezetben. Megfigyeléseim alapján úgy találom, hogy a jelenlegi definíciók hiányosak vagy pontatlanok, ami akadályozza a kritikus infrastruktúrák védelmének optimális kialakítását.

Másodsorban, kiemelten fontosnak tartom, hogy a disszertációmban meghatározott védelmi zóna besorolási rendszert vegyék figyelembe a 2022/2557 irányelv magyarországi implementálásával kapcsolatos jogszabályok megalkotásánál. A védelmi zónák hatékony besorolása kulcsfontosságú a kritikus infrastruktúrák védelmében, és a szóban forgó irányelv helyi alkalmazása ideális lehetőséget biztosít erre.

Harmadsorban, felhívom a figyelmet a védelmi zónák követelményeit tartalmazó segédlet hasznosságára. Ajánlom ennek bemutatását és bevezetését a kritikus infrastruktúrákkal foglalkozó biztonsági szakértők részére, hogy támogatást nyújtson számukra a hatékony és biztonságos beléptető rendszerek kialakításában és működtetésében.

FELHASZNÁLT IRODALOM

[1] A Tanács 2008/114/EK Irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. (2008.12.23.) Az Európai Unió Hivatalos Lapja

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[3] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

[4] Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

[5] Böröcz, M. Gy. (2022) Az Európai Unió biztonságpolitikája szerepének vizsgálata a kritikus infrastruktúrák védelmében Doktori (PhD) értekezés; Óbudai Egyetem

[6] Bonnyai, T. (2011). A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása.

[7] Bonnyai, T. (2012). Kritikus infrastruktúra védelem az Európai Unióban – a kezdetektől napjainkig. Magyar rendészet, 12(1), 132–137.

[8] COM/2004/0702, A Bizottság közleménye a Tanács és az Európai Parlament részére, A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben

[9] COM/2005/0576, Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról

[10] COM/2006/0786, A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról

[11] COM/2006/0787, Javaslat A Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

[12] COM/2008/0676, Javaslat A Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN)

[13] Elavult Bizottsági javaslatok visszavonása. (2012.06.02) Az Európai Unió Hivatalos Lapja. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012XC0602(03)&qid=1683633307411 (Letöltve 2023.05.02.)

[14] COM/2020/829, Javaslat Az Európai Parlament és e Tanács irányelve a kritikus fontosságú szervezetek rezilienciájáról. (2020.12.16.)

[15] COM/2022/551, Javaslat A Tanács ajánlása a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről. (2022.10.18.

[16] ST/15623/2022/INIT. A Tanács ajánlása a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről (2022.12.9.)

[17] Bognár, B. (2014). A létfontosságú rendszerek és létesítmények védelmének nemzeti szabályozása. In A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése: Nemzetközi tudományos-szakmai konferencia (pp. 46–50).

[18] Károlyi L. (2007) A kritikus infrastruktúrák védelme és az operatív erők tevékenységirányítása a honi katasztrófavédelemben, különös tekintettel az EU konformitásra Doktori (PhD) Értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Katonai Műszaki Doktori Iskola

[19] 2112/2004. (V. 7.) Kormány határozat a terrorizmus elleni küzdelem aktuális feladatairól

[20] A Kormányzati Koordinációs Bizottság 1/2007. (III. 29.) számú határozata a katasztrófavédelemmel összefüggő 2007. évi feladatokról. https://jogkodex.hu/doc/6808616 (Letöltés ideje 2023.05.02.)

[21] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[22] 1249/2010. (XI. 19.) Kormány határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

[23] 295/2010. (XII. 22.) Kormány rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

[24] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról1

[25] Bognár, B., Bonnyai, T., Görög, K., Katai-Urban, L. & Vass, Gy. (2015). Létfontosságú rendszerek és létesítmények védelme Kézikönyv a katasztrófavédelmi feladatok ellátására. Nemzeti Közszolgálati Egyetem. ISBN 978-615-5057-50-2.

[26] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[27] 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól

[28] 65/2013. (III. 8.) Kormány rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

[29] Ciekanowski, Z., Żurawski, S., & Wyrębek, H. (2023). Critical infrastructure threats. In Studia Administracji i Bezpieczeństwa (Köt. 13, Issue 13, o. 263–272). Index Copernicus. https://doi.org/10.5604/01.3001.0016.2902

[30] Bonnyai, T. (2014). A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében Doktori (PhD) Értekezés. Nemzeti Közszolgálati Egyetem

[31] Bonnyai, T. (2013). Létfontosságú rendszerek és rendszerelemek katasztrófa-érzékenysége. Műszaki katonai közlöny, 23(1), 204–223.

[32] NIPP 2013, Partnering for Critical Infrastructure Security and Resilience. (2013). U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (letöltés ideje: 2023.05.02.)

[33] National Risk Register. (2020). HM Goverment. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf (letöltés ideje: 2023.05.02.)

[34] Risk Management Guide for Critical Infrastructure Sectors. (2010). Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf (letöltés ideje: 2023.05.02.)

[35] Pallagi, A., Pető, R., & Hronyecz, E. (2023). Increasing the resilience of critical infrastructures with defense zone system. In SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (pp. 549–554).

[36] McMillan, D. (2014) Disruption at Gatwick Airport. https://www.gatwickairport.com/globalassets/publicationfiles/business_and_community/all_public_publications/2014/mcmillan_report_feb14.pdf (letöltve: 2023.05.02.)

[37] Mufson, S. (2012) 3 nuclear power reactors shut down during Hurricane Sandy. Washington Post. https://www.washingtonpost.com/business/economy/3-nuclear-power-reactors-shut-down-during-sandy/2012/10/30/7ddd3a94-22b6-11e2-8448-81b1ce7d6978_story.html (leöltve: 2023.05.02.)

[38] DesRoches, R., Comerio, M., Eberhard, M., Mooney, W., & Rix, G. J. (2011). Overview of the 2010 Haiti Earthquake. In Earthquake Spectra (Köt. 27, Issue 1_suppl1, o. 1–21). SAGE Publications. https://doi.org/10.1193/1.3630129

[39] Fukushima accident summary. (2011). https://www.britannica.com/summary/Fukushima-accident (letöltve:2023.05.02.)

[40] 2023 Turkey-Syria Earthquake. (2023). https://disasterphilanthropy.org/disasters/2023-turkey-syria-earthquake/?gclid=Cj0KCQjwmtGjBhDhARIsAEqfDEfgjdIwtJJ4yPNZdAAU5vpJ2k4GKewg7BJjLERYgpDQWEbyeByRcQgaAhEYEALw_wcB (letöltve: 2023.05.02.)

[41] 2011. Report on Eyjafjallajokull (Iceland). In R. Wunderman (Szerk.), Bulletin of the Global Volcanism Network (Köt. 36, Issue 4). Smithsonian Institution. https://doi.org/10.5479/si.gvp.bgvn201104-372020

[42] Soma, S. (1975). In Journal of Geography (Chigaku Zasshi) (Köt. 84, Issue 4, o. 204–217). Tokyo Geographical Society. https://doi.org/10.5026/jgeography.84.4_204

[43] Tarik, M. (2022). The worst solar storms in history. https://www.space.com/12584-worst-solar-storms-sun-flares-history.html#section-2022-a-very-expensive-storm (letöltve: 2023.05.02.)

[44] Case Study: St. Francis Dam (California, 1928) https://damfailures.org/case-study/st-francis-dam-california-1928/ (letöltve: 2023.05.02.)

[45] Chernobyl Accident 1986. https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx (letöltve: 2023.05.02.)

[46] How the Ohio Train Derailment and Its Aftermath Unfolded. (2023). The New York Times. https://www.nytimes.com/article/ohio-train-derailment-timeline.html (letöltve: 2023.05.02.)

[47] Byers, M., Wright, E., Boley, A., & Byers, C. (2022). Unnecessary risks created by uncontrolled rocket reentries. In Nature Astronomy (Köt. 6, Issue 9, o. 1093–1097). Springer Science and Business Media LLC. https://doi.org/10.1038/s41550-022-01718-8

[48] Nagy, R. (2010). A klímaváltozás hatása a kritikus infrastruktúrák védelmére. NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE, 3(2), 35–44.

[49] Krista, C. (2021) Uttarakhand flood was caused by rare rock and glacier avalanche. https://www.newscientist.com/article/2280645-uttarakhand-flood-was-caused-by-rare-rock-and-glacier-avalanche/ (letöltve: 2023.05.02.)

[50] Tomalska, A. (2022). Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic. In Security and Defence Quarterly. War Studies University. https://doi.org/10.35467/sdq/146603

[51] European Commmossion. (2022). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/statistics-migration-europe_en (letöltve: 2023.05.02.)

[52] A tervezett üzemidő lejártát követő üzemeltetés engedélyezése a paksi atomerőmű 4. Számú blokkján (2017). Országos Atomenergetikai Hivatal. https://www.haea.gov.hu/web/v3/oahportal.nsf/96CD56566A00C7D9C12581230024CB74/$File/OAH_k%C3%B6z%C3%A9rthet%C5%91_%C3%B6sszefoglal%C3%B3%204.bl_05.08_v%C3%A9gl.pdf (letöltve: 2023.05.02.)

[53] Nagy, R. (2016). A kritikus infrastruktúrák elleni lehetséges radiológiai terrortámadások. MAGYAR RENDÉSZET, 16(6), 145–153.

[54] Nagy R. (2011) A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Hadmérnöki Doktori Iskola, Budapest

[55] Palicz, T., Sas, T., Tisóczki, J., Bencsik, B., & Joó, T. (2020). „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben. In Orvosi Hetilap (Köt. 161, Issue 36, o. 1498–1505). Akademiai Kiado Zrt. https://doi.org/10.1556/650.2020.31788

[56] Nguyen, H. P. D., Ruiz, L., & Rajnai, Z. (2021). Industrial Control System (ICS): The General Overview of the Security Issues and Countermeasures. In Informatics and Cybernetics in Intelligent Systems (o. 412–419). Springer International Publishing. https://doi.org/10.1007/978-3-030-77448-6_39

[57] Miranda, B. (2023) Key details behind Nord Stream pipeline blasts revealed by scientists https://www.theguardian.com/business/2023/sep/26/nord-stream-pipeline-blasts-key-details-revealed-by-scientists (letöltve 2023.10.01.)

[58] Pocskai, Á. (2012) Gondolatok a kritikus infrastruktúrák terrortámadással szembeni védelmének szabályozásáról. Terrorelhárítási Központ. https://www.epa.oszk.hu/02900/02932/00001/pdf/EPA02932_terror_elharitas_2012_1_02.pdf (letöltve: 2023.05.02.)

[59] Terror Profile Hungary. (2021). Council of Eupean Committee on Counter-terrorism. https://rm.coe.int/profile-hungary-may-2021-2767-7286-2979-v-2/1680a2b116 (letöltés ideje: 2023.05.02.)

[60] Global Terrorism Index 2023. (2023). Institute for Economics & Peace. https://www.economicsandpeace.org/wp-content/uploads/2023/03/GTI-2023-web.pdf (letöltve: 2023.05.02.)

[61] Szabo, A., & Rajnai, Z. (2017). The review of the external risk factors during the operation training plan of the security guards. In 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY). IEEE. https://doi.org/10.1109/sisy.2017.8080583

[62] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról.

[63] Bederna, Z., Rajnai, Z., & Szadeczky, T. (2020). Attacks against energy, water and other critical infrastructure in the EU. In 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE). IEEE. https://doi.org/10.1109/cando-epe51100.2020.9337751

[64] List of conflicts in Europe. Wikipedia. https://en.wikipedia.org/wiki/List_of_conflicts_in_Europe (letöltés ideje: 2023.05.02.)

[65] Beckvard, H. P. (2022). Protecting critical infrastructure and critical information infrastructure. In contemporary military challenges (Köt. 2022, Issue 2, o. 15–28). Walter de Gruyter GmbH. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.1

[66] Muha, L. (2007). A Magyar Köztársaság kritikus információs infrastruktúráinak védelme Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem

[67] Haig, Zs. & Kovács, L. (2012) Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány. Nemzeti Közszolgálati Egyetem. https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (letöltés ideje: 2023.05.02.)

[68] Őszi, A. (2019). A biometrikus azonosítás helye és szerepe az e-kereskedelemben PhD (Disszertáció), Óbudai Egyetem

[69] Nyikes, Z., & Rajnai, Z. (2015). Big data, as part of the critical infrastructure. In 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY). IEEE. https://doi.org/10.1109/sisy.2015.7325383

[70] James, F. B. & Eugene, T. (2012). Risk Analysis and the Security Survey Fourth Edition. Elseiver Inc. ISBN 978-0-12-382233-8

[71] Rehak, D., Markuci, J., Hromada, M., & Barcova, K. (2016). Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. In International Journal of Critical Infrastructure Protection (Köt. 14, o. 3–17). Elsevier BV. https://doi.org/10.1016/j.ijcip.2016.06.002

[72] Pataki, J. (2020). A terrorizmus, mint biztonsági probléma, a kritikus infrastruktúra védelmi szabályai tükrében Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola

[73] Muha, L., & Tóth, G. N. (2011). A bankbiztonság vizsgálata kockázatelemzéssel. HADMÉRNÖK, 6(4), 204–215. http://www.hadmernok.hu/2011_4_muha_toth.pdf (letöltve: 2023.05.02.)

[74] Rajnai, Z., & Fregan, B. (2016). Kritikus infrastruktúrák védelme (jogi szabályozás). In Műszaki Tudományos Közlemények (Köt. 5, o. 349–352). Muszaki Tudomanyos Kozlemenyek. https://doi.org/10.33895/mtk-2016.05.78

[75] Nagy, R. (2006). A kritikus infrastruktúravédelme és annak katasztrófavédelmi aspektusai a terrorizmus tükrében. Kard És Toll: Válogatás A Hadtudomány Doktoranduszainak Tanulmányaiból, (3), 56–64.

[76] Marina, M., Toni, M. & Robert, M. (2019). Critical infrastructure: Concept and security challenges. Friedrich Ebert Foundation, office Skopje. ISBN 978-9989-109-93-5

[77] Nunes-Vaz, R., & Lord, S. (2014). Designing physical security for complex infrastructures. In International Journal of Critical Infrastructure Protection (Köt. 7, Issue 3, o. 178–192). Elsevier BV. https://doi.org/10.1016/j.ijcip.2014.06.003

[78] Pallagi, A., & Kovács, T. (2019). Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására. In Hadmérnök (Köt. 14, Issue 4, o. 35–45). Hadmérnök. https://doi.org/10.32567/hm.2019.4.2

[79] Pető, R. (2017). Protection of Borders and Installation against vehicle-based. ÓBUDA UNIVERSITY E-BULLETIN.

[80] Ronyecz, L., Bognár, B., & Révai, R. (2018). A létfontosságú rendszerelemek közötti interdependencia kockázatainak elemzése, különös tekintettel az egészségügyi ágazat rendszerelemeire és létesítményeire. Hadmérnök, 13(1), 133–142.

[81] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[82] Bognár, B., Bonnyai. T. & Vámosi, Z. (2019). Kritikus infrastruktúrák védelme I.. Dialóg Campus Kiadó. ISBN 978-615-5945-28-1

[83] Chen, X. (2023). Risk-based Access Control Model for Hospital Information Systems. In Frontiers in Computing and Intelligent Systems (Köt. 2, Issue 3, o. 82–84). Darcy & Roy Press Co. Ltd. https://doi.org/10.54097/fcis.v2i3.5315

[84] Biringer, B., & Danneels, J. J. (2001). Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures. In Risk-Based Decisionmaking in Water Resources IX. Ninth United Engineering Foundation Conference on Risk-Based Decisionmaking in Water Resources. American Society of Civil Engineers. https://doi.org/10.1061/40577(306)4

[85] Garcia, M. L.. (2007) Design and Evaluation of Physical Protection Systems, 2nd Edition. Butterworth-Heinemann. ISBN: 9780080554280

[86] Horváth-Kálmán, E., & Elek, B. (2023). Risks and the management of construction in the environment of nuclear facilities. ACTA TECHNICA JAURINENSIS, 0–8. http://doi.org/10.14513/actatechjaur.00707

[87] Chouinard, P., & Giddings, J. (2023). A Systems Approach to Critical Infrastructure Resilience. In Safety and Security Science and Technology (o. 37–52). Springer International Publishing. https://doi.org/10.1007/978-3-031-21530-8_3

[88] Filkorn, J. (2009). Beléptető rendszerek. Seawing Kft. https://doksi.hu/get.php?lid=6516 (Letöltve: 2023.05.10.)

[89] Berek, L., Berek, T. & Berek, L.. (2016). Személy- és vagyonbiztonság. Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. ISBN 978-615-5460-94-4

[90] Berek, L.. (2014). Biztonságtechnika. Nemzeti Közszolgálati Egyetem.

[91] Lukács, Gy., Gábor, L. (2002.). Új Vagyonvédelmi Nagykönyv. CEDIT 2000 Kft.. ISBN: 963-8180-39-0

[92] Ferraiolo, H., Mehta, K., Ghadiali, N., Mohler, J., Johnson, V., & Brady, S. (2018). Guidelines for the use of PIV credentials in facility access. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-116r1

[93] Electronic Access Control. (2017). Elsevier. https://doi.org/10.1016/c2015-0-04450-1

[94] András, P., & Éva, B. (2019). Plan and design of complex security systems for critical infrastructures, with particular regard to the use of access control systems. In Kiberbiztonság – Cybersecurity 2. (Vol. 2, pp. 240–246).

[95] Dan M. Bowers. (1988) Access Control and Personal Identification Systems. Elsevier. https://doi.org/10.1016/c2013-0-04278-8

[96] The evolution of credential technologies. (2021). HID Global Corporation. https://www.hidglobal.com/doclib/files/resource_files/pacs-card-evolution-ig-en.pdf (letöltés ideje:2023.01.02.)

[97] Camilla, A. (2023) The history of door access control systems. https://www.2n.com/en_US/blog/the-history-of-door-access-control-systems (letöltés ideje: 2023.05.05.)

[98] Wang, X., Wang, X., Yan, Y., Liu, J., & Zhao, Z. (2022). RF-Access: Barrier-Free Access Control Systems with UHF RFID. In Applied Sciences (Köt. 12, Issue 22, o. 11592). MDPI AG. https://doi.org/10.3390/app122211592

[99] Abid, A., Cheikhrouhou, S., Kallel, S., Tari, Z., & Jmaiel, M. (2022). A Smart Contract-Based Access Control Framework For Smart Healthcare Systems. In The Computer Journal. Oxford University Press (OUP). https://doi.org/10.1093/comjnl/bxac183

[100] Pallagi, A. & Persely, A. (2023). Methodological and Health Reasons for Unsuccessful Biometric Identification. Interdisciplinary Description of Complex Systems, 21 (2), 206-213. https://doi.org/10.7906/indecs.21.2.10

[101] Fialka, G., & Kovács, T. (2016). The vulnerability of biometric methods and devices. Annals of faculty of engineering hunedoara: international journal of engineering, 14(3), 45–48.

[102] Ikponmwosa, O., S., O., Jeffrey Okieke, U., E. E., E., B. P., D., D. I., A., U.G., A., A. O., O., A.O., O., O.J., E., G. I., E., … K. U, O. (2023). Face recognition system for automatic door access control. In Engineering and Technology Journal (Köt. 08, Issue 02, o. 1981–1985). Everant Journals. https://doi.org/10.47191/etj/v8i2.03

[103] Shi, W., Li, G., Li, X., & Mitrouchev, P. (2023). Intelligent Access Control System Base on Face Recognition. In Advanced Manufacturing and Automation XII (o. 399–405). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-9338-1_49

[104] Tóth, A., & Tóth, L.. (2014) Biztonságtechnika. Nemzeti Közszolgálati Egyetem. ISBN 978-615-5305-56-6

[105] MSZ EN 50133-1:2000 Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények.

[106] MSZ EN 50133-7:2000 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek

[107] MSZ EN 50133-2-1:2001 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 2-1. rész: Részegységek általános követelményei

[108] MSZ EN 50133-1:1996/A1:2003 Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények

[109] MSZ EN 50133-1:2006 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények

[110] MSZ EN 50130-4:2011 Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsalád-szabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei

[111] MSZ EN 60839-11-1:2013 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-1. rész: Elektronikus beléptető rendszerek. A berendezésekre és készülékekre vonatkozó követelmények (IEC 60839-11-1:2013)

[112] MSZ EN 50130-4:2011/A1:2015 Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsaládszabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei

[113] MSZ EN 60839-11-2:2015 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek (IEC 60839-11-2:2014)

[114] MSZ EN 60839-11-31:2017 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-31. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló alaprendszer interoperabilitási protokollja (IEC 60839-11-31:2016)

[115] MSZ EN 60839-11-32:2017 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-32. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló beléptetés monitorozása (IEC 60839-11-32:2016)

[116] MSZ EN IEC 60839-11-5:2021 - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-5. rész: Elektronikus beléptetőrendszerek. Nyílt felügyelt eszközprotokoll (OSDP) (IEC 60839-11-5:2020)

[117] MSZ EN IEC 60839-11-33:2022 - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-33. rész: Elektronikus beléptetőrendszerek. A webszolgáltatásokon alapuló beléptetés konfigurálása (IEC 60839-11-33:2021)

[118] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

[119] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[120] 169/2010. (V. 11.) Korm. rendelet a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről

[121] 53/2015. (IX. 24.) BM rendelet az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről

[122] 33/2021. (IX. 15.) MNB rendelet a fizetési rendszer működtetése tevékenységre vonatkozó részletes szabályokról

[123] 78/2015. (XII. 23.) BM rendelet az arcképelemző rendszer működtetésének részletes szabályairól

[124] 62/2009. (XII. 17.) IRM rendelet a Közjegyzői Levéltár tevékenységével összefüggő szakmai követelményekről

[125] 8/2021. (XI. 18.) OBH utasítás a bírósági épületek fizikai védelmi rendszereinek feltételeiről

[126] Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. In International Journal of Disaster Risk Reduction (Köt. 60, o. 102316). Elsevier BV. https://doi.org/10.1016/j.ijdrr.2021.102316

[127] Pallagi, A., & Kovács, T. (2019). Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására. In Hadmérnök (Köt. 14, Issue 4, o. 35–45). Hadmérnök. https://doi.org/10.32567/hm.2019.4.2

[128] Pallagi, A., Pető, R., & Hronyecz, E. (2023). The fundamental requirements of the defense zones of critical infrastructures. In ICCECIP 2023 5th International Conference on Central European Critical Infrastructure Protection

[129] Puskas, B., & Rajnai, Z. (2015). Requirements of the Installation of the Critical Informational Infrastructure and Its Management. In Interdisciplinary Description of Complex Systems (Köt. 13, Issue 1, o. 48–56). Croatian Interdisciplinary Society. https://doi.org/10.7906/indecs.13.1.7

[130] Bruce, S.. Schneier a biztonságról. (2008). HVG Könyvek. ISBN: 978-963-304-026-3

[131] Lee, B., & Amanda, B. (2017). Defensive Security Handbook. O'Reilly Media Inc.. ISBN: 9781491960332

[132] Berek, L., & Hódosi, V. (2019). Veszélyes objektumok biztonsági rendszereinek ellenőrzése. In Hadmérnök (Köt. 14, Issue 3, o. 5–11). Hadmernok. https://doi.org/10.32567/hm.2019.3.1

[133] MSZ EN 1627:2021 Bejárati ajtók, ablakok, függönyfalak, rácsok és redőnyök. Betörésállóság. Követelmények és osztályba sorolás

[134] MSZ EN 356:2000 Építési üveg. Biztonsági üvegezés. Kézi támadással szembeni ellenálló képesség vizsgálata és osztályozása

[135] MSZ EN 60529:2015 Villamos gyártmányok burkolatai által nyújtott védettségi fokozatok (IP-kód) (IEC 60529:1989)

[136] MSZ IEC 62262:2023 Villamos gyártmányok burkolatai által nyújtott védettségi fokozatok külső mechanikai hatások ellen (IK-kód)

[137] EN 1522:1998 Ablakok, ajtók, redőnyök és árnyékolók - Lövedékállósága - Követelmények és besorolás

[138] Pandey, S. K. &, Mustafa, K. (2012). Access Control and Rights related Risk Assessment. International Journal of Engineering Research and Applications (IJERA). pp.1174-1178. https://www.ijera.com/papers/Vol2_issue1/GG2111741178.pdf (letöltve: 2023.01.04.)

[139] Krishna Khanth, N., Jain, S., & Madan, S. (2023). Sentinel: An Enhanced Multimodal Biometric Access Control System. In Big Data Analytics in Astronomy, Science, and Engineering (o. 95–109). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28350-5_8

RÖVIDÍTÉSJEGYZÉK

Rövidítés	angol nyelvű kifejezés	magyar nyelvű kifejezés
BM		Belügyminisztérium
CCD	Charge-coupled Device	töltés-csatolt eszköz. Fényérzékeny alkatrésszel, fotodiódával kombinálva a fényt elektronikus jelekké alakító eszköz.
CCTV	Closed-circuit television	Zárt láncú televízió, videómegfigyelő rendszer
CER	Crossover Error Rate	keresztezési hibaarány
CIP	Critical Infrastructure Protection	létfontosságú infrastruktúrák védelme
CIWIN	Critical Infrastructure Warning Information Network	létfontosságú infrastruktúrák figyelmeztető információs hálózata
DDos	Distributed Denial of Service	elosztott szolgáltatásmegtagadással járó támadás
DLP	Data Leak Protection	adatszivárgás elleni védelem
ECI	European Critical Infrastructure	európai kritikus infrastruktúra
EMC	Electromagnetic compatibility	Elektromágneses kompatibilitás
EPCIP	European Programme for Critical Infrastructure Protection	létfontosságú infrastruktúrák védelmére vonatkozó európai program
EüM		Egészségügyi Minisztérium
FAR	False Acceptance Rate	téves elfogadási arány
FBI	Federal Bureau of Investigation	Szövetségi Nyomozó Iroda
FER	Failure to Enroll Rate	bevonhatósági hiba valószínűsége
FRR	False Rejection Rate	téves elutasítási arány

FVM		Földművelésügyi és Vidékfejlesztési Minisztérium
GKM		Gazdasági és Közlekedési Minisztérium
HM		Honvédelmi Minisztérium
IK	Impact protection	Fizikai behatás elleni védettség osztálya az EN62262 alapján
IP	International Protection Marking / Ingress Protection	Nemzetközi védettségjelölés
IRM		Igazságügyi és Rendészeti Minisztérium
IRM		Igazságügyi és Rendészeti Minisztérium
KHEM		Közlekedési, Hírközlési és Energiaügyi Minisztérium
KI		kritikus infrastruktúra
KüM		Külügyminisztérium
KvVM		Környezetvédelmi és Vízügyi Minisztérium
MABISZ		Magyar Biztosítók Szövetsége
MAK		Minősített Adatok Kezelése
MeH		Miniszterelnöki Hivatal
Meh EKK		Miniszterelnöki Hivatal Elektronikus Kormányzati Központ
NCI	National Critical Infrastructures	létfontosságú nemzeti infrastruktúrák
NFC	Near Field Communication	rövid távú kommunikációs szabvány
NFGM		Nemzeti Fejlesztési és Gazdasági Minisztérium
OAH		Országos Atomenergetikai Hivatal
OBH		Országos Bírósági Hivatal
OKF		Országos Katasztrófavédelmi Főigazgatóság

OSP	Operator Security Plan	üzemeltetői biztonsági terv
ÖM		Önkormányzati és Területfejlesztési Minisztérium
ÖTM		Önkormányzati és Területfejlesztési Minisztérium
PIN	Personal Identification Number	személyi azonosító szám, PIN-kód
PM		Pénzügyminisztérium
RFID	Radio Frequency Identification	rádió frekvenciás azonosítás, automatikus azonosításhoz használt technológia

11. táblázat Rövidítések, a táblázatot a szerző szerkesztette

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

A doktori tanulmányaimat 2017 és 2023 között az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában végeztem, melynek keretében mélyreható kutatást folytathattam. Kivételes hálával és tisztelettel emlékszem mentoromra és barátomra, Prof. Dr. Kovács Tiborra, aki állandó ösztönzéssel és támogatással indított el a kutatásom kibontakozásában. Nagy tisztelettel mondok köszönetet témavezetőmnek Prof. Dr. Rajnai Zoltán tanár úrnak, a Biztonságtudományi Doktori Iskola vezetőjének a sok segítségért és iránymutatásért.

Hálás köszönettel tartozom Dr. Szűcs Endrének és Dr. Pető Richárdnak a baráti segítségért és szakmai tanácsokért. Hálásan gondolok a Doktori Iskola adminisztrációs hölgyeire, Farkasné Hronyecz Erikára és Lévay Katalinra, akik az adminisztratív feladatokban nyújtott segítségükkel hozzájárultak tanulmányaim zökkenőmentes lebonyolításához.

Utolsónak, de nem utolsósorban, tisztelettel köszönetemet fejezem ki a Doktori Iskola professzorainak, tanárainak és doktorandusz társaimnak, akik szakmai támogatásukkal és tanácsaikkal hozzájárultak kutatásaim és tanulmányaim sikeres végrehajtásához.

Végezetül, hatalmas elismeréssel és hálával fordulok családomhoz, barátaimhoz és vezetőimhez, akik ebben a meghatározó és intenzív időszakban mellettem álltak és szilárd támogatást nyújtottak. A sikeres disszertáció elkészítése végső soron az ő segítségüknek és hittel teli támogatásuknak köszönhető.