8. Biztonságtechnikai rendszerek

Tóth Levente – Tóth Attila

A rendszerváltozást megelőző időszakban a tulajdontárgyak döntő többsége, a termelőeszközök nagy egésze az állam tulajdonában volt. Ebből kifolyólag az állam mint közhatalmi szervezet látta el az állami vagyonvédelem mellett a tulajdonosi és vagyonvédelmi feladatokat is. A rendszerváltást követően a gazdaság szerkezete átalakult. Az állami tulajdon mértéke jelentősen csökkent, míg a magántulajdon meghatározó tényezővé vált. Ebben a helyzetben viszont az állam a magántulajdonosokat – egészen szűk kivételtől eltekintve – már nem kötelezhette vagyonuk védelmére, mert ezzel indokolatlanul beavatkozott volna a tulajdonos jogaiba. „Nemzetközi tendencia a magánbiztonság térnyerése, expanziója, amelynek hátterében többek között a rendőrségek kapacitásainak jobb eloszlása és a költséghatékonyság áll. Az államok, kormányok rájöttek, hogy a rendészeti monopólium szigorú fenntartása mellett, bizonyos feladatok, különösen egyes háttértevékenységek privatizálhatók, kiszervezhetők."[1]A fent részletezett okok miatt hazánkban megváltozott a vagyonvédelem szabályozásának addigi koncepciója.

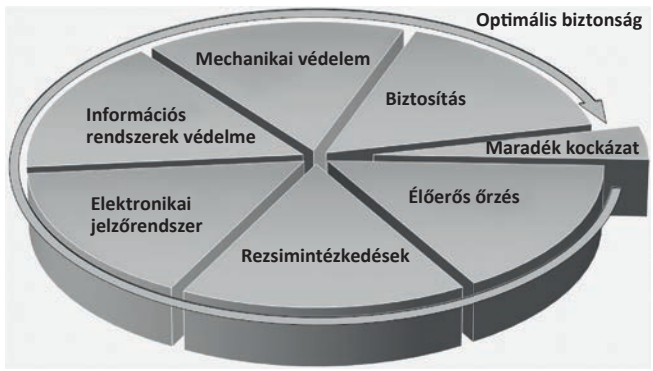
A tulajdonosok részére az állam már nem írt elő védelmi kötelezettséget, hanem a megalkotott és kihirdetett jogszabályok alapján lehetőséget biztosított vagyonuk megvédésére. A különböző társadalmi csoportok közötti vagyoni különbségek növekedése, az országhatárok megnyitása, a szervezett külföldi bűnszövetkezetek megjelenése, a hazai bűnszövetkezetek kialakulása és megerősödésének természetes következményeként a mindennapi élet során egyre inkább előtérbe került a közrend, a közbiztonság helyzete, a bűncselekmények során megsokszorozódott vagyon elleni bűncselekményekkel szembeni hatékony védelmi rendszerek kialakításának igénye. Magyarország – a korábbinál sokkal intenzívebb – nemzetközi katonai szerepvállalása, illetve az Európai Unióhoz (EU) való csatlakozása egy új veszélyforrást idézett elő, amely tovább növelte a hazánk ellen irányuló külső fenyegetettséget is, amely elsősorban a modern kori terrorizmusban ölt testet.

A felsorolt okok és indokok miatt egyre nagyobb igény jelentkezik a teljes körű vagyonvédelem kiépítésére, illetve a meglévő biztonságvédelmi rendszerek folyamatos fejlesztésére, bővítésére. E feladat megvalósításában kiemelkedő szerepet játszanak a komplex vagyonvédelmi rendszerek, azaz a mechanikai védelem, az elektronikai jelzőrendszerek, valamint az élőerős védelem és a különböző szervezeti intézkedések összessége. E tárgykörből manapság már nem hagyható figyelmen kívül az adott szervezet adatvagyonának védelme. Ennek okán a komplex védelem részét képezik az alkalmazott információs rendszerek védelmi megoldásai is. Ha a komplex védelmi rendszer valamely részét megerősítjük,

[1] Christián 2014a, 15–17.

https://doi.org/10.36250/00788_08

akkor más területeken csökkenthetünk a védelmen. (Például, ha több kamerát szerelünk fel az elektronikai jelzőrendszerbe, akkor kevesebb élőerő alkalmazásával is biztosítani tudjuk a védelmet.) A felsorolt tényezők egy esetleges kárkövetkezmény enyhítését szolgáló biztosítással együtt optimális biztonságot képesek nyújtani a felhasználóknak. Teljes körű, 100%-os védelem még így sem valósítható meg, ezért számolnunk kell egy maradék kockázattal, amely a magánszemély vagy egy gazdasági szervezet esetén a menedzsment tudatos kockázatvállalását jelenti azzal, hogy az egyes veszélyforrásokra nem vagy csak részben reagál védelmi megoldással. E kockázat egy káreseményt követően a visszaállítás során az egyénre vagy a gazdasági szervezetre háruló költségeket jelenti.



11. ábra

Az optimális biztonság fogalma

Forrás: a szerző saját szerkesztése

Az elektronikai jelzőrendszer, mint neve is mutatja, nem sorolható a klasszikus védelmi rendszerek közé. Ez a rendszer „csak" jelzi a behatolás tényét, illetve annak szándékát. Ezeknek a rendszereknek a feladata a különböző biztonságot veszélyeztető cselekmények vagy események detektálása, jelzése, a történések nyomon követése, rögzítése, az illetéktelen személyek belépésének vagy a gépjárművek behajtásának gátlása (mechanikus áteresztőszerkezetek vezérlésével), a különböző tárgyak, áruk, cikkek be- és kivitelének ellenőrzése, valamint különböző – általában – automatikus vezérlések végrehajtása. Ide soroljuk a behatolás- és támadásjelző, videomegfigyelő, tűzjelző, beléptető-, illetve árúvédelmi rendszereket. Ezek a rendszerek a mechanikai-fizikai védelemmel szemben nem adnak valós védelmet, hiszen nem tudják feltartóztatni a behatolót. Csupán jelzik az eseményt az élőerős védelemnek, amelynek feladata a bűncselekmény megakadályozása vagy az épületbe bejutott személy feltartóztatása, elfogása, vagyis a helyszíni intézkedés. Szintén azonnali beavatkozást igényel egy tűzjelző rendszer által adott riasztás, amikor a helyszínen tartózkodók menekítése mellett további feladat a vagyoni kár csökkentése, minimalizálása. A különböző események során végrehajtott intézkedések tervszerűséget, szervezettséget igényelnek. Ehhez szükséges az élőerős tevékenységet szabályzó úgynevezett rezsim- (szervezeti) intézkedések megléte.[2]

[2] A biztonsági szakmában használt technikai védelem kifejezés valóban pontatlan, de szinonim kifejezésként használatos az elektronikai jelzőrendszerre. *(A szerk.)*

A vagyonvédelem komplexitása, a védelmek közötti összefüggés úgy határozható meg, hogy az elektronikai védelemnek olyan előrejelzést kell biztosítania, hogy a mechanikai védelem képes legyen visszatartani a behatolni szándékozót az élőerős védelem kiérkezéséig. A védelmi rendszer kialakítása a védelem megfelelő ellátását szolgálja. A védelem folyamatos komplex tevékenység, amelynek célja, hogy biztosítsa a biztonság kívánatos szintjének elérését, illetve fenntartását.[3]

Az objektumok biztonsága olyan állapotot, helyzetet jelent, amelyben az ott tartózkodók életét, testi épségét, az anyagi javak és adatok létét, sértetlenségét, továbbá az objektum belső rendjét és működését sem külső, sem belső tényező nem sérti vagy veszélyezteti.

A biztonságot veszélyeztető tényezők lehetnek természeti (villámcsapás, vízbetörés stb.) vagy technológiai eredetűek (elektromos kontakthiba, rosszul működő őrlángérzékelő stb.), illetve emberi közreműködéssel végrehajtott cselekmények. Ez utóbbi lehet tudatos (szándékos jogellenes magatartás) vagy gondatlan (többnyire figyelmetlenségből, hanyagságból keletkező veszélyek). A biztonságot veszélyeztető, emberi közreműködéssel szándékosan végrehajtott cselekmények közé sorolhatjuk a betörést, a lopást, a rablást, de tágabb értelmezésben az informatikai rendszerünk ellen elkövetett feltörést és adathalászatot is.

A felsoroltakból is jól látszik, hogy számtalan tényező veszélyezteti a biztonságunkat. Ebből kifolyólag a védelmi rendszerek eszközválasztéka is rendkívül széles skálát képez, így számos megvalósítási lehetőség áll rendelkezésre az objektumok komplex vagyonvédelmének megtervezésére és kialakítására.

8.1. Tűzjelző rendszerek, beléptetőrendszerek, azok tervezése, kivitelezése és karbantartása

8.1.1. A tűzjelző rendszerek tervezése

A tűzjelző rendszerek létesítése az Országos Tűzvédelmi Szabályzat (OTSZ) mellékletében meghatározott építmények esetén kötelező.[4] Tűzjelző rendszer azonban létesíthető önkéntes alapon, illetve a jogszabályban meghatározott építményeken kívül, hatósági kötelezés alapján is, ahol a fennálló veszélyhelyzet vagy az építmény nemzetgazdasági, műemlékvédelmi stb. jellege azt indokolja.[5]

A tűzjelző rendszerek tervezése hatósági engedélyeztetési eljáráshoz kötött feladat. Az engedélyeztetési eljárást az I. fokú tűzvédelmi hatóság végzi, amely első körben megvizsgálja, hogy a dokumentáció megfelel-e a hatályos jogszabályi előírásoknak, az érvényben lévő szabványoknak, illetve, hogy a tervező rendelkezik-e a tervezéshez szükséges tűzvédelmi szakvizsgával és tervezői jogosultsággal.

Az automatikus tűzjelző rendszer tervezése felsőfokú műszaki végzettséggel, tűzjelző rendszerek tervezésére jogosító tűzvédelmiszakvizsga-bizonyítvánnyal, valamint a Magyar Mérnöki Kamaránál bejegyzett TUJ tervezői jogosultsággal végezhető.

---

[3] Berek Lajos – Berek Tamás – Berek László (2016): *Személy- és vagyonbiztonság.* Budapest, Óbudai Egyetem.

[4] Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 14. sz. melléklete tartalmazza a tűzjelző rendszer létesítésére kötelezett építményeket, rendeltetés szerinti csoportosításban.

[5] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról 154. § (1) *b)*

A tűzvédelmi szakvizsgára kötelezett foglalkozási ágakról, munkakörökről, a tűzvédelmi szakvizsgával összefüggő oktatásszervezésről és a tűzvédelmi szakvizsga részletes szabályairól szóló 45/2011. (XII. 7.) BM rendelet 1. számú mellékletében található a tűzvédelmi szakvizsgához kötött foglalkozási ágak és munkakörök jegyzéke. A jegyzék 10. pontjában szerepelnek a beépített tűzjelző berendezéseket tervezők, a kivitelezésért felelős műszaki vezetők, valamint az üzembe helyező mérnökök. A tűzvédelmiszakvizsgabizonyítványt különféle oktatásszervező cégeknél, felsőoktatási intézményeknél szervezett képzést követő sikeres szakvizsga letételével lehet megszerezni. A fenti BM-rendelet szabályozza a szakvizsgabizottság összetételét, valamint a szakvizsgáztatásra való jogosultág feltételeit is.

Az automatikus tűzjelző rendszerek tervezése rendkívül összetett feladat, széles körű eszközismeretet, tájékozottságot, tapasztalatot és precizitást igényel. A tűzjelző rendszer gondatlan tervezése, telepítése vagy üzemeltetése miatt a rendszer nem képes a keletkező tüzet idejében észlelni, a szükséges vezérléseket elvégezni, a kiürítést elindítani. Emiatt rendkívül nagy anyagi károk keletkezhetnek, legrosszabb esetben emberéleteket is követelhet a gondatlan tervezés.

A tervdokumentációk tartalmi és formai követelményeit a Magyar Mérnöki Kamara által kiadott *Tervdokumentációk Tartalmi és Formai Követelményeinek Szabályzata* tartalmazza. Ebben a szabályzatban találhatók a tűzjelző rendszerek esetében előforduló tervfajták is, amelyek a következők:

- Építtetői jóváhagyási terv;
- Ajánlati vagy tenderterv;
- Hatósági engedélyezési terv;
- Kiviteli terv;
- Megvalósulási terv.

8.1.2. A különféle tervdokumentációk tartalmi és formai követelményei

Tűzjelző berendezés építtetői jóváhagyási terve

Ez a tervdokumentáció hatósági engedélyeztetésre, kivitelezésre nem használható, a kivitelezési költségek becsléséhez készül, a hatályos jogszabályok és szabványi előírások figyelembevételével, az építészeti tervdokumentációk alapján. Tartalmazza a létesítés okát, a fontosabb követelményeket, a védendő építmény főbb építészeti, valamint tűzvédelmi jellemzőit és a benne található helyiségek rendeltetéseit. Ezenkívül a szükséges vezérléseket, a részegységek elvárt műszaki paramétereit (pontos típus nélkül), a tűzriasztás módját, a központ elhelyezését és az állandó felügyelet megoldását, illetve a telepítésre vonatkozó általánostól eltérő feladatokat.

Rajzmellékletként telepítési vázrajzokat kell csatolni a dokumentációhoz, konkrét kábelezés-bekötés nélkül.

Tűzjelző berendezés ajánlati- vagy tenderterve

Az ajánlati terv egy egyszerűsített kiviteli terv, amely azért készül, hogy a rendszer kivitelezésére ajánlatot adó pályázók egységes elvárásrendszer alapján készíthessék el ajánlataikat. Ha a pályázók mindegyike a tendertervben foglalt követelményeknek megfelelő ajánlatot tesz, akkor az ajánlatok kiértékelése elvégezhető akár a műszaki tartalmuk vizsgálata nélkül is. Emiatt nagyon fontos az ajánlati terv kellően részletes kidolgozottsága és pontossága.

Az ajánlati terv szakhatósági engedélyeztetésre nem használható. Nagyon fontos, hogy az ajánlati terv pontos típusmegjelöléseket nem tartalmazhat, csak a telepítendő rendszer elemeinek elvárt műszaki paraméterei szerepelhetnek benne. Hasonlóan az építtetői jóváhagyási tervhez, ebben is szerepelnek a vezérlések, az átjelzés és az állandó felügyelet módja, a tűzriasztás bemutatása stb. Mellékletként csatolni kell az egyes szintekre tervezett eszközök elhelyezési rajzait, az épület metszeti rajzait, valamint egy elvi összefüggési rajzot. Az árazatlan költségvetésben feltüntetett darabszámoknak egyezniük kell az eszközelhelyezési rajzokon összeszámolható eszközök számával. Ha mégsem egyezik, akkor ajánlatadáskor a rajzon szereplő eszközök száma a mérvadó.

Tűzjelző berendezés kivitelezési terve

A tűzjelző berendezés hatósági engedélyeztetéséhez engedélyezési, kivitelezési és – ha a kivitelezés során eltértek a kivitelezési tervtől, akkor – megvalósulási tervdokumentációt kell készíteni. A kivitelezési terv alapján is lehet engedélyeztetni a létesítést,[6] ebben az eseten létesítési engedélyezési és kivitelezési tervdokumentáció készül. A kivitelezési terv akkor megfelelő, ha az alapján a kivitelezést végző szakember a jogszabályoknak, szabványi előírásoknak és a tűzjelző berendezés műszaki specifikációjának megfelelően el tudja készíteni az automatikus tűzjelző rendszert.

A kivitelezési tervdokumentáció tartalmi elemei a következők:

- előlap;
- tervezői nyilatkozat az OTSZ-ben[7] meghatározott tartalommal;
- tartalomjegyzék;
- műszaki leírás (előzmények, a védendő építmény jellemzői, az építmény tűzvédelmi jellemzői, az épület rendeltetése, az ott folytatott tevékenység, tervezési alapelvek, különleges tervezési feladatok, a tűzjelző rendszer felépítése, az alkalmazott eszközök jellemzői, műszaki paraméterei, a tűzeseti vezérlések és jelzése fogadása, a tűzriasztás módja, az állandó felügyelet kialakítása (átjelzés), jelölések, telepítési követelmények, üzembe helyezés, karbantartás);
- mellékletek (egyeztetési jegyzőkönyvek, vezérlési mátrix,[8] nyilatkozatok stb.);

---

[6] 491/2017. (XII. 29.) Korm. rendelet a beépített tűzjelző, illetve tűzoltó berendezések létesítésének, használatbavételének és megszüntetésének engedélyezésére irányuló hatósági eljárás részletes szabályairól. Az 1. § (2) tartalmazza az engedély iránti kérelem kötelező tartalmi elemeit.

[7] OTSZ: Országos Tűzvédelmi Szabályzat [54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról].

[8] A vezérlési mátrix tartalmazza a tűzjelzőeszköz-csoportok és a vezérelt berendezések közötti kapcsolatokat.

- rajzmellékletek (helyszínrajz, elvi nyomvonalrajzok legfeljebb 1:200 léptékben, összefüggési rajz, metszeti rajz, bekötési rajzok, amennyiben a gyártói leírásban szereplőn felül többletinformáció szükséges a telepítéshez);
- a tűzjelző berendezés megvalósulási terve.

Megvalósulási tervet akkor kell készíteni, ha a kivitelezés során eltértek a kivitelezési tervdokumentációtól. A megvalósulási terv tartalma megegyezik a kivitelezési tervdokumentáció tartalmával, a műszaki leírás elegendő, ha csak a változásokat tartalmazza, azonban ebben az esetben a megvalósulási dokumentáció együtt kezelendő a kivitelezési tervvel.

8.1.3. Jelzőrendszerek átalakítása

A tűzjelző berendezésen végzett átalakításokat minden esetben dokumentálni kell a megvalósulási tervben, és az átalakítást követően el kell végezni az üzembehelyezési eljárást. Az átalakításokat előzetesen engedélyeztetni kell. Az engedélyeztetési eljárástól két esetben el lehet tekinteni, ha erről a hatóság írásban is nyilatkozik. Az OTSZ 154. § (2) a, c pontja alapján a tűzjelző rendszer átalakításának engedélyeztetésétől el lehet tekinteni, ha az érzékelők száma egy naptári évben legfeljebb összesen 10 darabbal nő, és a jelzési zóna határa nem változik, illetve ha csak a rendszer állandó felügyeletének helye vagy módja változik. Az érzékelők számának csökkentését minden esetben előzetesen engedélyeztetni kell!

8.1.4. A tűzjelző rendszerek megszüntetése

A tűzjelző rendszer csak hatósági engedély birtokában szüntethető meg. A megszüntetési engedély iránti kérelem tartalmát a 491/2017. (XII. 29.) Korm. rendelet 3. számú melléklete tartalmazza.[9]

- Az üzemeltetőnek nyilatkoznia kell az épület azon jellemzőiről, amely alapján a létesítést a létesítéskor hatályos jogszabály előírta.
- Az üzemeltetőnek nyilatkoznia kell a létesítési kötelezettséget megalapozó körülmény tűzvédelmi szempontból kedvező megváltozásáról.
- Be kell nyújtani egy tűzvédelmi dokumentációt, amely igazolja, hogy az épület a rendszer megszüntetését követően is megfelel a hatályos OTSZ követelményeinek.

A tűzjelző rendszer megszüntetésének előfeltételeit igazoló tűzvédelmi dokumentációt építésügyi tűzvédelmi tervező készíthet.[10] Építésügyi tűzvédelmi tervező lehet a tűzvédelmi mérnök, tűzvédelmi szakmérnök, építőmérnök, illetve építészmérnök tűz- és katasztrófavédelmi szakirányú végzettségű mérnök.

[9] A 491/2017. (XII. 29.) Korm. rendelet a beépített tűzjelző, illetve tűzoltó berendezések létesítésének, használatbavételének és megszüntetésének engedélyezésére irányuló hatósági eljárás részletes szabályairól.

[10] 375/2011. (XII. 31.) Korm. rendelet a tűzvédelmi tervezői tevékenység folytatásának szabályairól.

8.1.5. A Tűzvédelmi Műszaki Irányelvek (TVMI)

Az Országos Tűzvédelmi Szabályzat egy jogszabály, az ebben foglaltak betartása kötelező. Az OTSZ tartalmaz műszaki követelményeket, de a követelményeket teljesítő műszaki megoldásokat nem. A biztonságosan alkalmazható műszaki megoldások meghatározása a szabványok feladata. A jogszabály ezekre a szabványokra hivatkozhat. Egy új technológia bevezetésének, használatának nem szab gátat a jogszabály kötelező alkalmazása, mivel a szabványokban foglalt műszaki megoldásoktól el szabad térni, ha legalább azzal egyenértékű megoldást alkalmazunk.

Hazánkban a szabványok közzétételére, módosítására, visszavonására a Magyar Szabványügyi Testület (MSZT) jogosult.[11] A szabványokat az MSZT értékesíti, azokat nem lehet díjmentesen letölteni, a megvásárolt szabványt nem szabad közzétenni, lemásolni. A tűzvédelmi műszaki irányelvek, a szabványokkal összhangban készített műszaki követelmények, amelyek alkalmazása önkéntes, de ha a tervező és a kivitelező betartja a TVMI-ben foglaltakat, akkor a telepített rendszer meg fog felelni az OTSZ-ben foglalt műszaki követelményeknek.

A TVMI-ket időközönként felülvizsgálják, mindig az aktuálisan elérhető műszaki megoldásokat tartalmazzák. Jelenleg 12 darab TVMI érhető el, amelyeket a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatósága tesz közzé honlapján.[12] A beépített tűzjelző berendezés tervezésére és telepítésére az 5. számú TVMI vonatkozik.

8.1.6. A tűzjelző rendszerek kivitelezése

A tűzjelző berendezések kivitelezése tűzvédelmi szakvizsgához kötött tevékenység, amelyet a tervezéshez hasonlóan a 45/2011. (XII. 7.) BM rendelet 1. számú mellékletében szereplő foglalkozási ágak és munkakörök között találunk.[13] A tűzjelző rendszer kábelhálózatát, védőcsövezését elkészítheti a villanyszerelő is, de rendszerelemeit csak tűzvédelmi szakvizsgával rendelkező személy telepítheti, kötheti be, és a programozást, tesztelést is csak ő végezheti.

8.1.6.1. Az üzembehelyező mérnök és a felelős műszaki vezető

Az üzembehelyező mérnököt a megrendelő bízza meg a létesített automatikus tűzjelző rendszer teljes ellenőrzésére.[14] Az üzembehelyező mérnök felelős a rendszeren minden üzemi próba elvégzéséért, ellenőrzi, hogy a kivitelezett rendszer megfelel-e az engedélyezési tervdokumentációban leírtaknak, ellenőrzi a felhasznált anyagokat, valamint a szerelés szakszerűségét. Az üzembehelyező mérnök az üzembe helyezésről jegyzőkönyvet készít, majd írásban nyilatkozik az üzembe helyezés megtörténtéről. Üzembehelyező mérnöki

[11] A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény felhatalmazása alapján.

[12] Tűzvédelmi műszaki irányelvek. Forrás: www.katasztrofavedelem.hu/index2.php?pageid=tuzmegelozes_otsz_iranyelvek (A letöltés dátuma: 2018. 05. 15.)

[13] Beépített tűzjelző berendezések kivitelezését, karbantartását, javítását, telepítését, felülvizsgálatát végzők.

[14] Feladatait az Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 158. § tartalmazza.

feladatokat tűzjelző rendszerek tervezésére jogosító tűzvédelmiszakvizsga-bizonyítvánnyal lehet ellátni.

A felelős műszaki vezető (FMV) a kivitelező által megbízott személy, aki a szerelési munkát szervezi, irányítja és ellenőrzi.[15] Minden építési engedélyhez vagy az Étv. 33/A. §-a[16] szerinti egyszerű bejelentéshez kötött kivitelezési tevékenység esetén meg kell bízni felelős műszaki vezetőt a kivitelezés irányításával. A FMV közreműködik a használatbavételi engedélyezési eljárásban, az alvállalkozói teljesítéseket igazolja, vezeti az építési naplót (amennyiben erre a kivitelezőtől megbízást kapott). A felelős műszaki vezető a kivitelezés helyszínén betartatja az adott helyszínen érvényes munkavédelmi, egészségügyi, tűzvédelmi, környezetvédelmi stb. előírásokat.

A villamos területen tevékenykedő felelős műszaki vezetőket a 266/2013. (VII. 11.) Korm. rendelet alapján a Magyar Mérnöki Kamara tartja nyilván, a jogosultsági kérelmeket a kamara bírálja el.

8.1.6.2. A tűzjelző rendszerek üzemeltetési, karbantartási feladatai

A beépített tűzjelző berendezések üzemeltetésére, karbantartására vonatkozó követelményeket az OTSZ tartalmazza.[17] A tűzjelző berendezés üzemeltetéséről és karbantartásáról üzemeltetési naplót kell vezetni. Az üzemeltetési naplóban meg kell nevezni többek között a rendszer kezelésére oktatásban részesült személyeket, fel kell benne tüntetni a rendszer főbb adatait, a tűzátjelzés módját, az átjelzést fogadó szervezet adatait, az illetékes tűzoltóság adatait, valamint a rendszer karbantartását végző szervezet adatait. Az üzemeltetési naplót minden nap kell vezetni, és az utolsó bejegyzéstől számított öt évig meg kell őrizni. A napló napi, havi, negyedéves és féléves ellenőrzéseire vonatkozó követelményeket az OTSZ részletesen tartalmazza.

A napi ellenőrzést az üzemeltető végzi. Ennek során ellenőrizni kell, hogy a rendszer hibamentesen működik-e, ha hibát jelez a rendszer, akkor értesítették-e a karbantartót. Ha előző nap történt hibabeírás a naplóba, akkor ellenőrzi, hogy a hiba elhárítására történt-e megfelelő intézkedés. Végül ellenőrzi, hogy a központ minden állapotjelzője megfelelően működik-e. Ez az ellenőrzés általában egyetlen gombnyomással elvégezhető a tűzjelző központon. Az ellenőrzés tapasztalatait beírja az üzemeltetési naplóba, amely bejegyzést aláírásával hitelesíti.

A havi ellenőrzést szintén az üzemeltető végzi. A havi ellenőrzés során meg kell győződni arról, hogy a naplót az elmúlt hónapban folyamatosan vezették-e, hogy a rendszer felügyeletét ellátók részesültek-e oktatásban, illetve hogy a tűzjelző központ eseménynyomtatójához rendelkezésre állnak-e nyomtatási kellékek (papír, festékszalag, patron stb.).

A rendszer negyedéves ellenőrzését szintén az üzemeltető végzi. Ekkor ellenőriz mindent, amit a napi és havi ellenőrzés során szokott, ezenfelül pedig meggyőződik arról, hogy történtek-e az épületben olyan átalakítások, vagy változtak-e helyiségfunkciók oly módon, hogy azok a telepített automatikus érzékelők működőképességét hátrányosan befolyásolják.

---

[15] Feladatait a 191/2009. (IX. 15.) Korm. rendelet az építőipari kivitelezési tevékenységről 13. § tartalmazza.

[16] 1997. évi LXXVIII. törvény az épített környezet alakításáról és védelméről.

[17] Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 253. §

Meggyőződik arról is, hogy a kézi jelzésadók jól látható, elérhető helyen vannak-e, nem kerültek-e kitakarásra. Ellenőrzi, hogy a hangjelzőket nem burkolták-e le, hangjuk jól hallható-e. Végül ellenőrzi, hogy a jelzések helyének beazonosítását segítő táblázatok, rajzok rendelkezésre állnak-e, ha van grafikus megjelenítő, akkor az üzemképes-e.

A rendszer féléves ellenőrzését, karbantartását a tűzvédelmi szakvizsgával rendelkező szerződött karbantartó végzi. Ilyenkor az üzemeltető feladata, hogy biztosítsa a karbantartó munkáját, tegye lehetővé, hogy a szakember minden tűzjelző eszközhöz hozzáférjen. A karbantartás során meg kell győződni arról, hogy a naplóba az elmúlt fél évben történt hibabejegyzésekre történt-e megfelelő intézkedés, a hibákat elhárították-e, a rendszer üzemképes és hibamentes-e. A karbantartó feladata, hogy ha bármilyen nem megfelelőséget tapasztal, akkor tegyen javaslatot a rendszer helyreállítására, fejlesztésére. A karbantartónak minden jelzési zónában legalább egy kézi jelzésadót és egy automatikus érzékelőt működtetnie kell, és meg kell győződnie arról, hogy a jelzések pontosan megjelennek-e a tűzjelző központon, elindulnak-e a szükséges vezérlések, megszólalnak-e a hangjelzők, illetve, hogy átmegy-e az átjelzés a felügyeleti központba. Ellenőrzi továbbá az akkumulátorok működőképességét, ha szükséges, cseréjüket is elvégzi, és ellenőriz mindent, amit a gyártó, a telepítő vagy a rendszer forgalmazója előírt.

Az éves karbantartást szintén a szerződött szakvizsgával rendelkező karbantartó végzi. A karbantartó évente ellenőrzi az összes érzékelő működőképességét azok kivételével, amelyeket a féléves karbantartásnál már ellenőrzött. Ezenkívül pedig elvégez minden olyan feladatot, amit a féléves karbantartás során kell megtennie.

8.1.6.3. Rendkívüli felülvizsgálat

Rendkívüli felülvizsgálatot kell végrehajtani a tűzjelző rendszeren az alábbi esetekben:

Tűzeset után

Attól függetlenül el kell végezni, hogy a tűzjelző rendszer jelzett-e. Amennyiben jelzett, akkor meg kell vizsgálni, hogy kellő részletességgel jelenítette-e meg a jelzéseket, elvégezte-e szükséges vezérlési feladatait, küldött-e átjelzést a felügyeleti központba. Meg kell vizsgálni, hogy a tűz következtében nem károsodott-e a rendszer. Ha a rendszer javítása szükséges, akkor el kell végezni a javítást.

Téves riasztás esetén

Meg kell vizsgálni, hogy mi váltotta ki a tűzjelzést. Ha üzemszerű téves riasztás[18] keletkezett, akkor javaslatot kell tenni a téves riasztást okozó körülmény megszüntetésére. Ha nem szüntethető meg, akkor javaslatot kell tenni a téves riasztást produkáló érzékelők cseréjére

[18] Üzemszerű téves riasztásról beszélünk, amikor egy helyiségben olyan megtévesztő jelenség keletkezik (nem tűz), ami tűzjelzést okoz az automatikus tűzjelző rendszeren.

olyan érzékelő alkalmazásával, amelynél az időszakosan vagy folyamatosan fennálló megtévesztő jelenség nem okoz téves jelzést.

A rendszer meghibásodása esetén

Meg kell vizsgálni, hogy mi okozta a hibát, hogy a hiba milyen hatással volt a rendszer működésére, majd el kell végezni a meghibásodott elemek cseréjét-javítását.

A rendszer változtatása esetén

A megváltozott rendszerrészen az éves felülvizsgálatot kell elvégezni.

Hosszú üzemszünet[19] *után*

Az éves felülvizsgálatot kell elvégezni.

Új karbantartóval kötött szerződés után

Ellenőrizni kell a szükséges iratok meglétét, és az éves felülvizsgálatot kell elvégezni.

A felülvizsgálatokat minden esetben dokumentálni kell az üzemeltetési naplóban.

8.2. Tűzveszélyességi és kockázati osztályok meghatározása

Fontosabb fogalmak:

Tűzveszélyességi osztály

Az anyagra, keverékre vonatkozó besorolás, amely az anyag, keverék fizikai, kémiai tulajdonságát alapul véve, tűzvédelmi szempontból a viselkedését, veszélyességét jellemzi.

Kockázati osztály

A tűz esetén a veszélyeztetettséget, a bekövetkező kár, veszteség súlyosságát, a tűz következtében fellépő további veszélyek mértékét kifejező besorolás.

[19] Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 258. § (3) 30 napnál hosszabb teljes körű leállás.

Kockázati egység

Az építmény vagy annak tűzterjedésgátlás szempontjából körülhatárolt része, amelyen belül a kockázati osztályt meghatározó körülményeket a tervezés során azonos mértékben és módon veszik figyelembe.

Mértékadó kockázati osztály

Az építmény, az önálló épületrész egészére vonatkozó besorolás, amely megegyezik a kockázati egységek kockázati osztályai közül a legszigorúbbal.

8.2.1. Tűzveszélyességi osztály

Az anyagokat korábban öt tűzveszélyességi osztályba sorolták. Ez alapján megkülönböztettünk Fokozottan tűz- és robbanásveszélyes „A", Tűz- és robbanásveszélyes „B", Tűzveszélyes „C", Mérsékelten tűzveszélyes „D" és Nem tűzveszélyes „E" kategóriát. A hatályos OTSZ-ben viszont már csak három kategóriát különböztetünk meg.[20] Robbanásveszélyes osztályba tartozik minden anyag, amelyet korábban „A" vagy „B" tűzveszélyességi osztályba soroltak. Tűzveszélyes osztályba tartoznak a korábban „C" vagy „D" tűzveszélyességi osztályba sorolt anyagok. Nem tűzveszélyes osztályba tartozik minden korábban „E" tűzveszélyességi osztályba sorolt anyag.

8.2.2. Kockázati osztály

Az önálló épületekre, épületrészekre, speciális építményekre vonatkozó besorolás a kockázati osztályba sorolás. Az épület kockázati osztálya határozza meg a betartandó tűzvédelmi követelményeket. Négy kockázati osztályt különböztetünk meg. Ezek a nagyon alacsony kockázati osztály (NAK), az alacsony kockázati osztály (AK), a közepes kockázati osztály (KK), illetve a magas kockázati osztály (MK).

8.2.3. A kockázati osztályba sorolást befolyásoló tényezők

A tűzveszélyességi kockázatot alapvetően meghatározza az épület rendeltetése, az ott tárolt anyagok tűzveszélyességi besorolása és mennyisége, az építmény magassága vagy földfelszín alatti létesítmény esetén a föld alatti, legalsó szintjének szintmagassága, a benn tartózkodó személyek száma és menekülési képessége, illetve az épületben folyó tevékenység.

[20] Az anyagok tűzveszélyességi osztályba sorolását az Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 9. § részletesen tartalmazza.

Az épület magassága és befogadóképessége szintén befolyásolja a kockázati osztályba sorolást.[21]

A menekülési képesség alapján megkülönböztetünk önálló menekülésre képes, segítséggel menekülő, előkészítés nélkül menthető és előkészítéssel vagy azzal se menthető személyeket.[22]

- Az önállóan menekülésre képes emberek nagyon alacsony kockázatot (NAK) jelentenek.
- A segítséggel menekülők menekítése lassabb, nehézkesebb, alacsony kockázatba (AK) sorolandók.
- Az előkészítés nélkül menekíthető emberek közepes kockázatot jelentenek (KK).
- Az előkészítéssel vagy anélkül se menekíthetők tartózkodására szolgáló területek magas kockázati osztályba (MK) sorolandók.

8.3. A beléptetőrendszerek

A beléptetőrendszerekre vonatkozó követelményeket az MSZ EN 60839 szabványsorozat tartalmazza.

A beléptetőrendszer egy biztonságtechnikai rendszer, amelynek biztonságtechnikai tervező-szerelő igazolvánnyal[23] és mérnöki kamarai tervezői jogosultsággal rendelkező tervező tervezhet. Biztonságtechnikai tervező-szerelő igazolványt biztonságtechnikai, híradástechnikai, távközlési, mechanikai, illetve villamosmérnöki képzettséget adó egyetemi vagy főiskolai végzettséggel lehet kérni. Az igazolványt a tervező lakóhelye szerint illetékes rendőrhatóság állítja ki és tartja nyilván.

8.3.1. A beléptetőrendszerek tervezésének főbb lépései

A beléptetőrendszerek tervezésének első fázisában meg kell határozni a rendszer telepítésének célját. Egészen másképp kell hozzákezdeni a tervezéshez, ha egyszerűen csak illetéktelenek véletlenszerű belépését kell megakadályozni egyes helyiségekbe, vagy ha a dolgozók összes mozgását naplóznunk kell, és meg kell tudnunk határozni, hogy ki hol tartózkodik, vagy az egyes helyiségekben kik tartózkodnak. Ugyanilyen nagy különbséget jelent a rendszer kialakításában, ha a bérszámfejtés segítésére a dolgozók munkaidejének nyilvántartása a cél, vagy egy ipari objektumban a személy- és tehergépjármű-forgalom szabályozása, naplózása a feladat. Egyes telepítési helyszíneken a célt egyértelműen meghatározza az objektum rendeltetése. Egy uszodába uszodai rendszert kell tervezni, egy szállodába szállodai beléptetőrendszert. Ezeken a helyszíneken a rendszerrel szemben támasztott követelmények nagyjából azonosak.

Miután a rendszer célját meghatároztuk, megkezdhetjük a belépési pontok feltérképezését. Ehhez pontosan ismernünk kell a védendő objektumban működő szervezet folyama-

[21] Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 1. melléklet, 1. táblázat.
[22] Országos Tűzvédelmi Szabályzat 54/2014. (XII. 5.) BM rendelet 1. melléklet, 2. táblázat.
[23] 2005. évi CXXXIII. törvény 1. § (4)

tait, a dolgozók és gépjárműveik, valamint a vendégek várható mozgását, illetve a dolgozók, a vendégek és a behajtani szándékozó gépjárművek számát. Nagyon fontos, hogy a belépési pontokat úgy határozzuk meg, hogy azok megkerülhetetlenek legyenek. Véletlenül se fordulhasson elő, hogy egy védett területre más irányból kártyahasználat nélkül be lehet jutni.

Ha ismerjük a belépési pontok helyét, fel kell mérnünk, hogy az adott pontokon milyen elektromechanikus áteresztő szerkezetet (APAS)[24] alkalmazzunk. Első és legfontosabb, hogy szingularizált[25] beléptetést kell-e megvalósítani vagy sem. Szingularizált beléptetőpont például a forgóvillával kialakított beléptetőpont vagy gépjárműveknél a zsilipelt gépjármű-beléptetés. Ez után meg kell vizsgálnunk, hogy az adott belépési ponton fail safe[26] vagy fail secure[27] típusú áteresztőpontot kell kialakítani. A menekülési útvonalakon minden esetben fail safe beléptetőpontot kell alkalmazni, amely hiba vagy áramszünet esetén szabadon nyithatóvá válik. Vagyonvédelmi szempontból érzékeny területekre (például trezor, szervergépterem stb.) tervezhetünk fail secure beléptetőpontot, de ezeken a helyeken is lehetővé kell tenni belülről az azonosítás nélküli nyitást – tűz esetén a menekülés megkönnyítésére.[28] Áteresztőszerkezet személy beléptetése esetén például az elektromágneses ellenzárral szerelt közönséges ajtó vagy szingularizált beléptetés esetén a forgóvilla, gyorskapu. Gépjárműveknél a motoros kapu, a sorompó és a különféle útakadályok (blockerek) is, szingularizált gépjármű-beléptetés esetén ezek kombinációja zsiliprendszerben.

Miután megvannak a belépési pontok, meg kell tervezni a belépési pontokat összekötő kommunikációs hálózatot. A hálózatot a gyártói előírások betartásával kell kialakítani. Ez után a felhasználó segítségével meg kell határozni a beléptetőrendszer központi szerverének helyét, valamint a beléptetőrendszert kezelők körét. A kezelők részére munkaállomást kell biztosítani a megfelelő kliensszoftverekkel. A vendégkártyák kezelését megkönnyíthetjük vendégkártyakiadó terminálok telepítésével a kapun szolgálatot teljesítő őröknél vagy recepciósoknál,vendégkártyát elnyelő oszlopok alkalmazásával pedig automatizálhatjuk a vendégkártyák visszavételét is.

8.3.2. A beléptetőrendszerekre vonatkozó adatkezelési szabályok

A beléptetőrendszerekben kezelt személyes adatok esetén is érvényes a célhoz kötöttség elve. Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.[29] Ezenkívül fontos, hogy csak az érintett hozzájárulásával kezelhető,[30] tehát minden esetben tájékoztatni kell a belépőt arról, hogy mely személyes adatait kezeli a szervezet, milyen céllal, és azokat mennyi ideig tárolja. A dolgozókat a munkaszerződésükben is lehet tájékoztatni a vállalat adatkezelési szabályairól, amelyet a munkavállaló aláírásával elfogad. Látogatók esetén egy rövid adatkezelési tájékoztató aláíratásával megtehetjük ugyanezt.

---

[24] APAS: Access Point Actuators and Sensors. Jelentése: áthaladást szabályozó eszközök és érzékelők.
[25] Szingularizált beléptetés esetén egy azonosítás egy belépést jelent.
[26] Fail safe: életvédelmi szempontból biztonságos.
[27] Fail secure: vagyonvédelmi szempontból biztonságos.
[28] Vésznyitó gomb és/vagy kulcsdoboz telepítésével.
[29] 2011. évi CXII. törvény 4. § (2)
[30] 2011. évi CXII. törvény 5. § (1) *b)*

A személyek beazonosíthatósága érdekében a kiadott kártyaszámokhoz elegendő eltárolni a belépő nevét, illetve a beazonosítására szolgáló fényképes igazolvány típusát és számát. Dolgozói kártyák esetén a belépési jogosultságok kezelését segíti, ha szervezeti egységenként vagy munkakörönként is csoportosítjuk a munkavállalókat, ezért a dolgozói kártyákhoz ezeket az információkat is érdemes eltárolni. Vendégek számára kiadott kártyák esetében a fenti személyes adatokon kívül rögzíthető, hogy a vendég melyik szervezettől érkezett és kihez jött.

A rendszerben a dolgozói mozgásadatok megőrzésének idejét a munkáltató határozza meg, a megőrzési időről a dolgozókat tájékoztatni kell. A megőrzési idő meghatározásánál tekintettel kell lenni a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 4. § (2) bekezdésére, amely szerint „a személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető". Tehát a cég tevékenysége, illetve biztonsági folyamatai figyelembevételével azt a legrövidebb tárolási időt kell meghatározni, amelyre szükség lehet a szabálytalanságok észleléséhez. A rendszeres belépési jogosultság megszűnését követően a beléptetőrendszerben tárolt mozgásadatokat legkésőbb az adat keletkezésétől számított hat hónap elteltével meg kell semmisíteni.[31]

Vendégek esetén személyes adataikat a vagyonvédelmi törvény 32. § (2) bekezdés *b)* pontja alapján „alkalmi belépés esetén a távozástól számított huszonnégy óra elteltével meg kell semmisíteni".

8.3.3. A proximity kártyás beléptetés biztonsága

A beléptetőrendszerekben alkalmazott proximity kártyák úgynevezett contactless, vagyis érintésmentes kártyák, amelyek olvastatásakor a kártyát nem szükséges hozzáérinteni az olvasóhoz. Működési elve leegyszerűsítve a következő: a proximity kártya egy passzív eszköz, nem tartalmaz semmilyen áramforrást (csak egy induktív tekercs, egy kondenzátor és egy integrált áramkör van benne, az integrált áramkör tartalmazza a kártya számát). Az olvasó folyamatosan alacsony frekvenciás (125 kHz) rádiójelet sugároz. Amikor az olvasó által sugárzott elektromágneses erőtérbe belekerül a kártya, az abban lévő passzív elemek egy rezgőkört alkotva energiát nyernek ki a lekérdező olvasó erőteréből. Ezt követően a kinyert energia segítségével az integrált áramkörben tárolt kártyaszámot visszasugározzák az olvasóba. A kártya és az olvasó között a kommunikáció teljesen nyílt, semmilyen titkosítást nem tartalmaz.

Ezeket a kártyákat az olvasók – típustól függően – akár 50–60 cm távolságból is képesek olvasni. Az egyszerű működési elv és a viszonylag nagy olvasási távolság következménye, hogy ezek a rendszerek könnyen feltörhetők. A kártyaadatokat akár egy táskába rejtett nagy olvasási távolságú olvasóval be lehet gyűjteni, mivel bármilyen olvasó kérdezi, a kártya ellenőrzés nélkül elküldi a saját számát. A kereskedelemben kaphatók programozható proximity kártyák és kártyakódolók, amelyek segítségével különösebb szakértelem nélkül bárki le tud másolni egy proximity kártyát. Ráadásul a másoláshoz nem szükséges az eredeti kártya, elegendő annak számát tudni.

[31] 2005. évi CXXXIII. törvény 32. § (3) *a)*

Napjainkban a beléptetőrendszerek nagy része még ilyen olvasókkal és kártyákkal működik, pedig már léteznek sokkal biztonságosabb megoldások.

Az úgynevezett hozzáférés védett rendszerek esetén az olvasók kódolt jelet sugároznak és csak a hozzájuk rendelt kártyákkal kommunikálnak. Ugyanígy a kártyák is kizárólag annak az olvasónak küldenek információt, amelyhez hozzárendelték őket. Ezeknél a rendszereknél az adatcserét minden esetben megelőzi egy hétlépcsős azonosítási folyamat. Az azonosítást követően pedig a kommunikáció titkosított formában történik, amely titkosítási folyamatban használt titkosítási kulcs véletlenszerűen generálódik minden olvastatáskor. Ez az eljárás védelmet nyújt a lefigyelt kommunikáció ismétlésével szemben is.[32] Az egyik legelterjedtebb ilyen kriptográf védelmet biztosító megoldás a Mifare-rendszer.

A Mifare-család is folyamatosan fejlődik, egyre több szolgáltatással és egyre nagyobb biztonságot garantáló megoldásokkal jönnek ki a gyártók. (például Mifare Ultralight, Mifare Classic, Mifare Plus, Mifare DESFire és ezeken belül is például Mifare Plus S, Mifare Plus X stb.)

8.3.4. Az ujjnyomat-azonosítás megbízhatósága, alkalmazhatósága, FAR, FRR

A legelterjedtebb biometrikus azonosítási mód az ujjnyomat-azonosítás. Az ujjnyomat-azonosítás során, az ujjbegyen található bőrredők (fodorszálak) jellegzetes mintáit, pontjait és azok egymáshoz viszonyított helyzetét tárolja a rendszer. Nagyon fontos, hogy a letárolt adatokból az ujjnyomat nem reprodukálható, tehát nem személyes adatot tárol a rendszer. Az érzékenység és az azonosítás biztonsága annál nagyobb, minél több pont egyezése szükséges az azonosításhoz. Az ujjnyomatolvasóval működő beléptetés nem feltétlenül jelent biztonságosabb beléptetést. A biometrikus azonosítás megbízhatóságának leírására használt mutatók a FAR és az FRR.

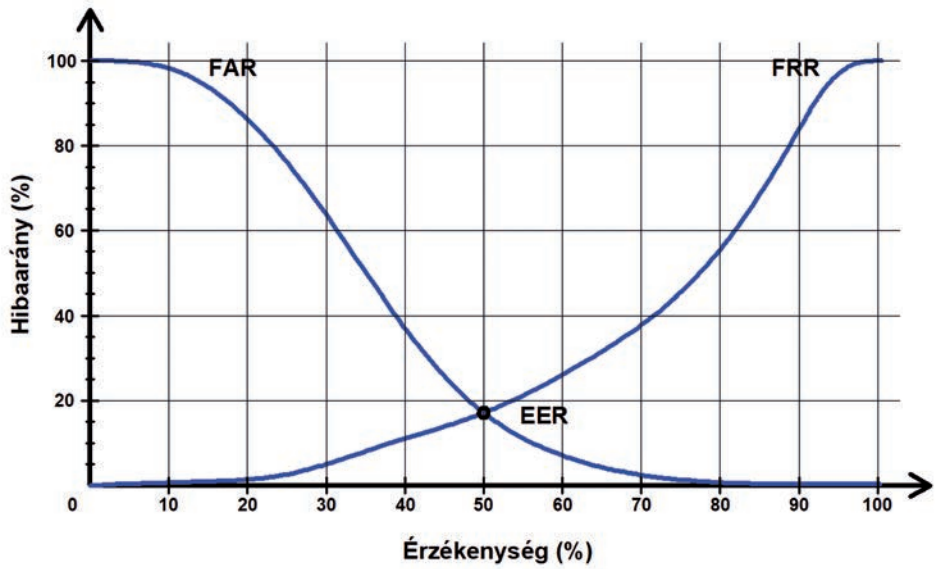
A FAR (False Acceptance Rate) téves elfogadási arányt jelent. Ez a tényező megmutatja, hogy a vizsgált biometrikus eszköz a belépésre nem jogosultak hány százalékát engedi be téves azonosítás miatt.

Az FRR (False Rejection Rate) téves elutasítási arányt jelent. A téves elutasítási arány azt mutatja meg, hogy a biometrikus azonosító a belépésre jogosultak hány százalékát utasítja el azért, mert hibásan azonosítja, vagy mert nem tudja azonosítani őket.

A téves elutasítás nem veszélyezteti a biztonságot, viszont kényelmetlenségeket okoz a rendszer használata során. A téves elfogadás azonban komoly biztonsági kockázatot rejt magában. Minél pontosabb azonosítást követelünk egy biometrikus azonosítótól, annál kisebb lesz a téves elfogadások valószínűsége, viszont annál többször fordulhat elő, hogy nem ismeri fel a belépésre jogosultat a rendszer. Másképpen fogalmazva, ha kényelmesebb beléptetést szeretnénk, akkor az érzékenységet kell csökkentenünk. A kényelmesebb beléptetés a FAR növekedését okozza, viszont ilyenkor csökken a kényelmetlenséget okozó FRR. Ha növeljük az érzékenységet, akkor biztonságosabb lesz a rendszer, de több lesz a téves elutasítások száma. Meg kell találni azt az egyensúlyi állapotot, ahol még elfogadható

[32] Filkorn József (é. n.): *Fokozott biztonsági követelményszintet teljesítő RFID rendszereszközök.* (Előadás)

mértékű a FAR és az FRR. Ezt a pontot nevezzük EER-nek (Equal Error Rate), egyenlő hibaaránynak.[33]



12. ábra

A hibaarány változása az érzékenység függvényében

Forrás: a szerző saját szerkesztése

Az ujjnyomatalapú azonosítás gyorsaságát és megbízhatóságát növelhetjük úgy, hogy az ujjnyomat-azonosítót kombináljuk kártyaalapú azonosítással. Ebben az esetben az azonosítandó ujjnyomatmintát a rendszernek nem az összes letárolt mintából kell kikeresnie (1:n alapú azonosítás), hanem elegendő az azonosított kártyához tartozó mintával összevetnie (1:1 megfeleltetés). A kettős azonosítás a beléptetés biztonságát is jelentősen növeli.

8.4. Behatolás- és támadásjelző, valamint videomegfigyelő rendszerek

A behatolás- és támadásjelző rendszerek egyik alapvető funkciója, hogy a lehető legkorábbi szakaszban érzékeljék a védett objektumba történő behatolási kísérletet. A rendszer felügyelete nemcsak az értékek tárgyiasult formájára terjed ki, hanem ide tartozik még a támadásnak kitett és jelzőeszközzel ellátott személyek kontrollálása is. Az érzékelésen és felügyeleten túl a rendszerek fontos része a riasztásjelzés és/vagy a távfelügyelet felé

[33] KOVÁCS Tibor – MILÁK István – OTTI Csaba (2012): A biztonságtudomány biometriai aspektusai. *Pécsi Határőr Tudományos Közlemények,* 13. kötet. 487.

történő átjelzés. A behatolás- és támadásjelző rendszerek hatékonyságát három fő tényező determinálja:

- megfelelő tervezés;
- megfelelő kivitelezés;
- megfelelő üzemeltetés.

A behatolás- és támadásjelző rendszerre vonatkozó követelményekhez az MSZ EN 50131-1:2006/A2:2017 szabvány tartalmazza. Ezenkívül a megfelelő tervezéshez és kivitelezéshez elengedhetetlen az MSZ CLC/TS 50131-7:2010 szabvány ismerete is. Az elektronikai rendszerek gyors fejlődése kihatással van a biztonságtechnikai piacra is. Számos, régebben mechanikai érzékelési elven működő berendezést mára már processzoros jelfeldolgozású szenzorok váltották fel (például üvegtörés és rezgésérzékelők). Különböző érzékelési technológiákat dolgoztak ki, amelyek tovább bővítették az objektumvédelem technikai eszköztárát. A megnövekedett eszközválaszték nagyobb szakismeretet, pontosabb tervezést, precízebb kivitelezést és karbantartást kíván a kivitelezőcégek részéről, míg gondosabb és felkészültebb üzemeltetési feladatokat támaszt a felhasználókkal szemben. A rendszerek nagyságával nő azok bonyolultsága, összetettsége, ezzel együtt a hibaforrások és a kezelési hibák száma.

8.4.1. Behatolás- és támadásjelző rendszerek tervezése

Egy adott objektum védelmi rendszerének tervezése igen nagy szakmai ismeretet igényel. Ismernünk kell a környezett bűnügyi fertőzöttségét, meg kell vizsgálni, hogy a vagyonellenes cselekmények közül milyen elkövetési módok fordulnak elő gyakrabban (lopás, betöréses lopás, rablás, rongálás stb.). A különböző biztonságot veszélyeztető veszélyforrásokat fel kell tudni ismerni, ezeket bekövetkezési valószínűség szerint sorba kell rendezni, és a védett értékhez igazított, költségoptimalizált védelmi rendszert kell megtervezni. A feladat végrehajtásához hatalmas eszközismeret szükséges, amit nehezít az a tény, hogy a technológiai gyártásfolyamat korszerűsödése, az újabbnál újabb innovációk egy folyamatosan fejlődő és megújuló termékkínálatot eredményeznek.

A megfelelő védelem kialakításához el kell végezni a védendő objektum szabvány szerinti 4 biztonsági fokozat valamelyikébe történő besorolását. A tervezés során ügyelni kell arra, hogy az alkalmazott eszközök mindegyike legalább a biztonsági fokozatnak megfelelő minősítéssel rendelkezzen.

A tervdokumentációval szemben támasztott követelmények vonatkozásában a tűzjelző rendszerekhez hasonlóan itt is célszerű figyelembe venni a Magyar Mérnöki Kamara által kiadott *Tervdokumentációk Tartalmi és Formai Követelményeinek Szabályzata*[34] című dokumentációt. A tervtípusok is megegyeznek A tűzjelző rendszerek tervezése fejezetben leírtakkal, valamint a már említett MSZ CLC/TS 50131-7:2010 szabványban foglaltakkal. Lényegi különbség azonban, hogy a behatolás- és támadásjelző, videomegfigyelő-

[34] *Tervdokumentációk Tartalmi és Formai Követelményeinek Szabályzata* (é. n.). Forrás: www.mmk.hu/tudastar/dokumentumtar/szabalyzatok/tervdokumentacio-tartalmi-es-formaikovetelmenyei-2017.05.09.pdf (A letöltés dátuma: 2018. 06. 11.)

és beléptetőrendszerek vonatkozásában nincs olyan felügyeleti szerv, ahol kezdeményezni kell a hatósági jóváhagyást.

A kivitelezési tervdokumentáció tartalmi elemei a következők:

- előlap;
- tervezői nyilatkozat;
- tartalomjegyzék;
- előzmények;
- a védendő objektum jellemzői;
- védelmi igény;
- védelmi koncepció;
- a megvalósítandó rendszer működési leírása;
- az alkalmazott eszközök műszaki paraméterei;
- telepítési és üzembehelyezési előírások;
- üzemeltetési és karbantartási utasítások;
- mellékletek (egyeztetési jegyzőkönyvek, nyilatkozatok stb.);
- rajzmellékletek (rajzjel magyarázata, helyszínrajz, elvi nyomvonal rajzai legfeljebb 1:200 léptékben, összefüggési rajz, bekötési rajzok, amennyiben a gyártói leírásban szereplőn felül többletinformáció szükséges a telepítéshez).

8.4.2. Behatolás- és támadásjelző rendszerek telepítése

A behatolás- és támadásjelző rendszer telepítését a 2005. évi CXXXIII. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységről szóló törvény szabályozza. Ennek értelmében a telepítést csak megfelelő szakképesítéssel és a rendőrség által kiállított, szerelési tevékenységre jogosító igazolvány birtokában lehet végezni. Ez alól kivétel lehet az elektronikai vagyonvédelmi rendszer telepítésére, szerelésére irányuló hálózatépítéssel összefüggő segédmunka, amennyiben a hálózatépítés helyszínén van olyan munkát irányító személy, aki rendelkezik a szerelésre jogosító igazolvánnyal. A rendszert a rendszertervnek megfelelően kell telepíteni. Amennyiben eltérésre van szükség, akkor azt a tervezővel egyeztetni kell. A tervtől való eltérés esetén megvalósulási tervdokumentációt kell készíteni.

A beüzemelés során minden egyes érzékelőt le kell tesztelni, és meg kell vizsgálni, hogy érzékelési tartománya kielégíti-e a tervben leírt védelmi igényeket. Külön figyelmet kell fordítani a mozgás- és rezgésérzékelőkre, amelyeknél szükség lehet az érzékenység vagy az érzékelési lefedettség beszabályozására. Ellenőrizni kell, hogy a kijelzések és az értesítések megfelelnek-e a rendszertervben foglaltaknak. Végezetül egy teljes működési tesztet kell végrehajtani, beleértve az összes figyelemfelhívó eszköz és riasztásátviteli berendezés működésbe hozását is. Ahol a riasztásátviteli berendezése része a rendszernek, ott ellenőrizni kell a riasztásfogadó központ felé történő sikeres jelzéstovábbítást is.

8.4.3. Behatolás- és támadásjelző rendszerek üzemeltetése

A behatolás- és támadásjelző rendszer megrendelőjének biztosítania kell, hogy a behatolás- és támadásjelző rendszert csak oktatott személyek kezelhessék, valamint a behatolás-

és támadásjelző rendszert a kezelési utasítások és az oktatáson elhangzottak szerint működtessék.

A rendszert célszerű rendszeresen tesztelni annak érdekében, hogy a behatolás- és támadásjelző rendszer teljesítőképessége a megkívánt szinten maradjon. A behatolás- és támadásjelző rendszer bármilyen meghibásodását haladéktalanul be kell jelenteni a hibaelhárításért felelős vagyonvédelmi cégnek. Figyelemmel kell kísérni a létesítmény használatával vagy kialakításával kapcsolatos bármilyen változást, amelyek károsan befolyásolhatják a behatolás- és támadásjelző rendszer teljesítőképességét, és amennyiben az eredeti állapot nem állítható vissza, akkor azt szintén jelezni kell a hibaelhárításért felelős vagyonvédelmi cégnek. Figyelmet kell fordítani az új belépők kezelési oktatására és a meglévők időszakos ismétlő képzésére. A működés megkezdésekor üzemeltetési naplót célszerű rendszeresíteni, amelyben nyomon követhetők a tesztelésekkel, karbantartásokkal és hibaelhárításokkal kapcsolatos tevékenységek adatai. A behatolás- és támadásjelző rendszer folyamatos és hibátlan működésének biztosítása érdekében a behatolás- és támadásjelző rendszert időszakonként karban kell tartani. A megrendelő felelőssége, hogy a behatolás- és támadásjelző rendszer megfelelően karbantartva és javíttatva legyen. E tevékenység elvégzésére a hibaelhárító/karbantartó céggel megállapodást kell kötni.

8.5. Videómegfigyelő rendszerek

Napjaink egyre divatosabb és gyakran használt kifejezése, a digitális technika jelen van a videómegfigyelő rendszerekben is. Digitalizálás során különböző, analóg jel formájában megjelenő (tárgyi) információt számítógéppel olvasható és értelmezhető, kódolt formába teszünk át. A hang vagy kép digitalizálásakor az analóg, azaz időben folyamatosan változó hang- vagy képi információt többnyire egy speciális eszközzel, hangkártyával vagy videokártyával alakítjuk számjegyekké. Ez a feladat komoly matematikai háttérrel és ennek megfelelő irodalommal rendelkezik, amelynek részletes ismertetését a könyv keretei nem teszik lehetővé.

A számítógépes képfeldolgozás során igen nagy adathalmazokkal kell műveleteket végezni. Az információt tömöríteni kell annak érdekében, hogy a képeket digitalizálás után minél kisebb méretben tudjuk tárolni vagy éppen az adott hálózaton továbbítani.

Bizonyos esetekben a tömörítést követően vissza kell nyerni az eredeti adatstruktúrát, nem engedhető meg az adat torzulása, elvesztése. Ilyen például a számítógépes fájlok tömörítése. Ezt a kis hatékonyságú tömörítési módszert nem használjuk a képek esetében. Figyelembe véve az emberi szem, illetve az agy érzékelési és képfeldolgozási korlátait, lehetőség van adatvesztéses tömörítési eljárást alkalmazni. Az adatvesztéses képtömörítésnél fontos, hogy a tömörítés során elveszett információ csak alig észrevehető változást okozhat a képben. Az elérhető kompresszió itt sokkal jobb az adatvesztés nélküli tömörítéshez képest. [35]

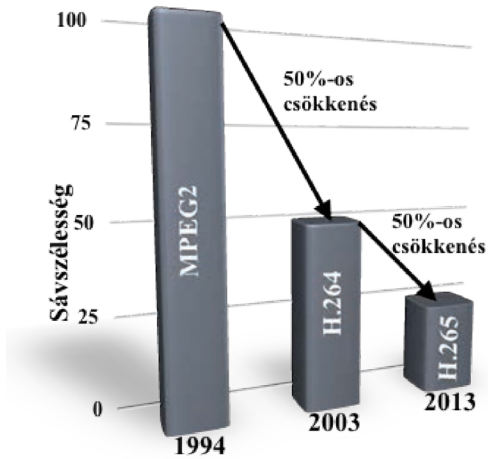
Hátránya viszont, hogy nehéz megtalálni az általánosan alkalmazható tömörítési arányt, és nem megfelelő adaptáció esetén a képtartalom jelentősen sérülhet. Az adatvesztéses tömörítés eredményessége képtartalomfüggő, így konkrét adatokkal csak a képi

[35] Tóth Levente (2004): *CCTV magyarul*. Budapest, BM Nyomda Kft. 209.

információ ismeretében lehet jellemezni. Tovább lehet fokozni a tömörítési rátát, ha nemcsak a mozgóképet alkotó állóképekben önmagában végezzük el a tömörítést, hanem vizsgáljuk a képkockák közötti változásokat is. Ebben az esetben sávszélességet és tárhelyet spórolhatunk, ha a változatlan, statikusan álló hátteret nem továbbítjuk minden egyes képkockánál. Ez a működési alapja a régi MPEG1, illetve a DVD-knél használt MPEG2, valamint ezek továbbfejlesztett, napjainkban is használatos MPEG4, H.264 és H.265 tömörítési algoritmusoknak. Általánosságban elmondható, hogy a tömörítési technológiai fejlődés és ezzel párhuzamosan a tömörítési ráta növekedési velejárója az egyre erősebb hardverigény, mind a kamera oldalán, mind pedig a képfeldolgozó (megjelenítő) végponton. A H.264 és az egyre inkább elterjedő H.265 algoritmus között akár 50%-os tömörítési hatásfokkülönbség is elérhető ugyanazon videóanyag esetén, de ennek velejárója a 10-szer nagyobb számolási igény.

Bár az ezredfordulón a szakemberek egybehangzó véleménye volt, hogy a digitális képtovábbítás néhány éven belül átveszi a vezető szerepet a biztonságtechnikai videómegfigyelő rendszerek terén, ez azonban mégsem így történt. Ennek több oka volt:

- A számítástechnikai hálózaton (továbbiakban IP-hálózaton) történő képtovábbítás megfelelő infrastruktúra kiépítést, az addig megszokott koaxiális kábeltől eltérő adatkábelezést és aktív elemeket, valamint informatikai jártasságot igényel.
- Az aktív elem és a videoeszköz közötti távolság, az úgynevezett szegmenshossz nem haladhatja meg a 100 métert (a Duplex 100Mb/s 5. kat. UTP esetén).
- Lehetőség van ugyan a már meglévő informatikai hálózatot megosztani, és a videó képi továbbítására is felhasználni, azonban ebben az esetben gondoskodni kell arról, hogy a hálózathoz egyébként hozzáférők, de a videomegfigyelő rendszer szempontjából jogosulatlan felhasználók a biztonságtechnikai adatfolyamhoz, illetve az ide tartozó eszközökhöz ne férjenek hozzá. Ilyenkor az informatikai rendszergazdának arra is kell figyelnie, hogy a folyamatos jó képminőség érdekében megfelelő sávszélességet allokáljon a videófolyam számára, viszont ez ne menjen az egyéb információs adat rovására.
- A kép digitalizálása, tömörítése, majd a megjelenítéskor a visszaalakítása, valamint a hálózati késleltetés (network latency) miatt a monitoron az események akár néhány másodperces késleltetéssel jelenhetnek meg.
- Az 1998-ban megjelenő SMPTE 292M HD-SDI szabvány, majd az ezt követően folyamatosan piacra kerülő szabvány szerinti eszközök lehetővé teszik a HD (high-definition, 1920 x 1080 pixel) felbontású digitális képek továbbítását koaxiális hálózaton keresztül. Ezekkel az eszközökkel lehetőség volt a régi, de jó minőségű analóg kamerahálózatot megtartva HD-felbontású rendszerre átállni.



13. ábra
Különböző tömörítési algoritmusok

Forrás: a szerző saját szerkesztése

Az IP-kamerák gyors előretörésének legnagyobb gátja az analóg HD CCTV- (Closed Circuit Television, azaz zárt láncú televíziós) rendszer piacra kerülése lett. 2012-ben a HD-TVI rendszer amerikai cég általi kifejlesztésére még abban az évben megjött a válasz egy kínai cégtől az általuk megjelentetett HD-CVI-rendszerrel. Egy évvel később egy koreai csipgyártó is beszállt a versenybe egy harmadik, AHD-formátummal. A három HD CCTV-rendszer elemei egymással nem kompatibilisek. Mindössze egy közös tulajdonsággal rendelkeznek. Mindhárom képes koaxiális hálózaton keresztül nagy felbontású képek analóg formában történő továbbítására. Mára mindhárom rendszer mögé igen nagy számban felsorakoztak azok a gyártók, amelyek piaci részesedést akartak a HD CCTV területén. Vannak olyan termékek (például képrögzítők), amelyek képesek mindhárom formátum feldolgozására. Mind a három rendszer tekintetében folyamatos a fejlesztés, amelynek köszönhetően már UHD (Ultra High Definition, 3840 × 2160 pixel, vagy más néven 4K-s) felbontású eszközök is elérhetők.

Ezekkel a rendszerekkel párhuzamosan az IP-kamerák eladása is folyamatosan növekszik. A Global Market Insights Inc. prognózisa szerint[36] 2024-re az IP-kamerák forgalma eléri a 20 milliárd dollárt. 2017 és 2024 között az átlagos éves növekedési ütem meghaladja a 25%-ot.

[36] *IP Camera Market to surpass $20bn by 2024: Global Market Insights, Inc* (2018). Forrás: https://globenewswire.com/news-release/2018/02/22/1379650/0/en/IP-Camera-Market-to-surpass-20bn-by-2024-Global-Market-Insights-Inc.html (A letöltés dátuma: 2018. 04. 15.)

8.5.1. Felbontás

A részletgazdag képalkotás alapvető igény a videómegfigyelő rendszereknél. Sokan azt gondolják, hogy ezt a célt a felbontás növelésével lehet elérni. Fontos azonban megjegyezni, hogy a nagy felbontás szükséges, de nem elégséges feltétele a részletgazdag képalkotásnak! A képminőséget befolyásoló tényezők:

- objektív minősége, határfelbontása;
- tömörítés;
- hőmérséklet;
- fényviszonyok.

Az objektív is rendelkezik határfelbontással. A határfelbontást meghaladó sűrűséggel elhelyezkedő fekete-fehér vonalakat az objektív már nem képes feketeként és fehérként leképezni. Helyette a fekete és fehér csíkok helyén is szürke „vonalakat" kapunk. Így a kamera képérzékelőjének egymás mellett lévő elemi pixelei ugyanazon információt kapják. Hiába a HD-felbontás, ha a képet alkotó pixelek között nincs információkülönbség.

A tömörítésénél fontos a megfelelő tömörítési algoritmus és a bitráta (másodpercenként feldolgozott egységnyi információ) kiválasztása. A környezeti hőmérséklet növekedésével a kamera (megfelelő hűtés/szellőztetés) hiányában egyre több zajt termel. Az így keletkező „mákos" kép apró részleteinek felismerését a zaj gátolja.

Hasonló a probléma az alacsony környezeti megvilágítás esetén. A kép részletgazdagsága és kontrasztossága akár felére is eshet a normál megvilágításhoz képest. Kis formátumú, de nagy (például 4K-s) felbontású biztonságtechnikai kameráknál ráadásul az extrém nagy megvilágítás (például nappali kültéri fényviszonyok) is a felbontás csökkenését okozhatja.[37]

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § (2) bekezdéséből levezethető, hogy a személyekről készített képfelvétel személyes adatnak, a (10) bekezdés alapján pedig a képfelvétel-készítés adatkezelésnek minősül. A törvény szerint személyes adatot csak meghatározott célból lehet gyűjteni. Ugyanerről a kérdésről az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) szintén előírja a kamerás felvételek jogalapjának meghatározását, amelyről az érintetteket tájékoztatni is kell. A biztonságvédelmi célból felszerelt kamerás megfigyelésre alkalmazandó jogalap a jogos érdek, amely a GDPR-rendelet 6. cikk (1) bekezdés *f)* pontjában található. Mindezeket figyelembe véve már a videómegfigyelő rendszer telepítése előtt, a felmérés időszakában a megrendelővel közösen kell tudni meghatározni a telepítendő kamera célját. Ez a „célhoz kötöttség elve" betartásának alapvető feltétele. A célok között szerepelhet a tömegfelügyelet, személyek vagy tárgyak mozgásának vagy egyéb események észlelése, megfigyelése, felismerése, azonosítása. Időnként szükség lehet olyan minőségű képekre is, amelyek a részletes kivizsgálást is segítik.

Az MSZ EN 62676-4:2015 szabvány részletesen foglalkozik a különböző feladatokhoz adaptált felbontásértékekkel. A felismerni kívánt személy, tárgy vagy cselekmény

[37] TÓTH Levente (2016): Limitation in the Application of High Resolution Image Sensors. *National Security Review,* 2. sz. 111–114.

vonatkozásában a különböző megfigyelési célokhoz rendelt minimum felbontási értékek a következők:

- áttekintés vagy tömegfelügyelet esetén 12,5 pixel/méter
- észlelés esetén 25 pixel/méter
- megfigyelés esetén 62,6 pixel/méter
- felismerés esetén 125 pixel/méter
- azonosítás esetén 250 pixel/méter
- kivizsgálás esetén 1000 pixel/méter.

Fontos azonban még egyszer megjegyezni, hogy önmagában a megadott méterenkénti pixelszám teljesülése kevés az adott megfigyelési cél elérésére. Mindenképp ügyelni kell arra, hogy az egymás melletti pixelek önálló, a valóságot reprezentáló információtartalommal rendelkezzenek.

8.5.2. Videóanalitikák

A videómegfigyelő rendszerek által hatalmas adatmennyiség keletkezik. Az IHS Markit piackutató cég felmérése szerint[38] 2015-ben az újonnan telepített HD-felbontású kamerák 566 petabájt adatot generáltak. Ez az adatmennyiség körülbelül 11,3 millió kétrétegű Blu-ray adathordozóra fér rá. A létrehozott hatalmas adatmennyiséget ki is kell értékelni. Sokszor ez Real-Time módon, operátorok által történik. Ez az igen megterhelő munka jól képzett és a monotonitást jól tűrő személyeket kíván. Sokszor azonban nem is a fáradtság vagy a figyelmetlenség miatt kerüli el az operátor figyelmét egy-egy inkriminált esemény, hanem a temérdek felügyeletére bízott kamera közül pont nem azokat a képeket figyeli, amelyeken a fontos esemény zajlik. A videóanalitikai szoftverek elvégzik az operátor helyett a kép kiértékelését, és a meghatározott kritériumok elérésekor riasztást adnak. Ezek a kritériumok lehetnek előre definiáltak, de legtöbbjüknél változtatható, illetve az adott helyszínhez adaptálható. Az egyszerűbb analitikák statikusak, míg a bonyolultabbak öntanulók, illetve dinamikusak. Az első csoportba tartozó, pixelváltozás alapján működő legegyszerűbb képkiértékelő algoritmusok közé tartozik a mozgásérzékelés. Itt adott mennyiségű pixelcsoport változása okoz riasztást. Ennél az egyszerű algoritmusnál tudjuk paraméterezni a pixelcsoport nagyságát, időbeni lefolyását és az érzékenységet. Mivel a képtartalmon belül a pixelcsoportok vektoriális elmozdulásának figyelése nem feladat, így sokszor a megvilágítási viszonyok megváltozása már (téves) riasztást okoz (például villámlás).

Adott pixelcsoportok képtartalmon belüli elmozdulásának figyelése már lényegesen fejlettebb technológia. Ennél a megoldásnál az elmozdult pixelcsoportot objektumként kezeljük. A sebességből és a vektorparaméterekből következtethetünk az elmozdulás irányára. Ez csökkentőleg hat a téves riasztásokra, valamint a valószínűtlen mozgási értékek abnormális mozgásra utalnak. Mára a különböző algoritmusok már képesek gépjárműveket

[38] Woodhouse, Josh (2016): Big, big, big data: higher and higher resolution video surveillance. *IHS Markit Technology,* 2016. 01. 26. Elérhető: https://technology.ihs.com/571026/big-big-big-data-higher-and-higher-resolution-video-surveillance (A letöltés dátuma: 2018. 05. 21.)

kategorizálni (kerékpár, személyautó, busz stb.), személyek nemét és hozzávetőleges életkorát felismerni.

Rögzített felvételeknél az esemény-visszakeresést gyorsítja, hogy a különböző eseményekről szóló információt kiszedjük a képből, és ezeket szöveges formátumban, úgynevezett metaadatként egy adatbázisban tároljuk. Az adatbázisban például egy vonalátlépés szóra történő találat sokkal gyorsabb, mintha a többórás videofelvételt analizálnánk újra.

Vannak gyártók, amelyek az analitikákat a kamerákba implementálják, és vannak szoftverfejlesztők, amelyek szerveroldali analitikákat fejlesztenek. Mindkét megoldásnak vannak előnyei és hátrányai. Kameraoldali analitika esetében rendelkezésre áll lokálisan a jó minőségű, kevésbé tömörített videokép. Így az analitika hatásfoka lényegesen jobb tud lenni. Lehetőség van eseménymentes időszakban kevésbé jó minőségű, ellenben kisméretű képek átvitelére, abban az esetben, ha a kamerába épített analitika eseményt érzékel, akkor a képek minősége is jobb lesz. Ezzel szemben a legtöbb gyártónál akkor is kifizetjük a kamerába épített képelemző szoftvert és persze a hozzá tartozó hardvert, ha nincs is rá szükségünk. Szerveroldali analitika esetében a szükséges darabszámú kameralicence vásárolható. A kamerákba épített tárterület, processzorsebesség és -típus limitálja az analitikák mennyiségét és fajtáját. Egy új fejlesztésű, erősebb hardverigényű képelemző algoritmus kamerába történő utólagos betöltése korlátokba ütközhet. Szerveroldalon a hardver bővítése, gyorsítása egyszerűen megoldható.

8.6. Kibervédelem az elektronikus védelmi rendszereknél

A különböző elektronikai jelzőrendszerek már nemcsak önmagukban, azaz a rendszer alkotóelemeivel kommunikálnak, hanem képesek más rendszereknek információt továbbítani, vagy onnan fogadni és értelmezni. Megjelentek a piacon az úgynevezett M2M-eszközök (Machine-to-Machine: azaz gépek közötti adatkommunikációs technológia), amelyek intelligens módon képesek a keletkező adatokat feldolgozni és továbbítani más gépekhez vagy a felhasználóhoz. Mára már a rendszerek egymásba ágyazása, integrálása is sokkal mélyebben (szoftveres úton) történhet meg, szemben a tíz évvel ezelőtti relés kimenetek és bemenetek (hardveres) összekapcsolásával. Az IP-kamerák megjelenése magával hozta a kamera távoli elérésének igényét. A piaci pozíciók stabilizálása érdekében a gyártók felgyorsított fejlesztési, gyártási és tesztelési fázisokat alkalmaznak, amelynek következtében nemcsak a minőség, a tartósság szenved csorbát, hanem kevesebb figyelem jut az eszközök kiberbűnözéssel szembeni védelmére is. Ez utóbbi pedig közvetlenül vagy közvetve is súlyos kockázatot hordoz egy biztonsági rendszer tekintetében. A gyártó által véletlenül (vagy szándékosan) nyitva hagyott rejtett hozzáférés (backdoor) közvetlen lehetőséget biztosít a teljes kontroll átvételére az adott eszköz felett. Közvetve pedig – e bejáratot kihasználva – megnyílik a lehetőség más, szintén az adott belső hálózatra csatlakozó eszközök elérésére is. A cseh Biztonsági Információs Szolgálat (BIS) már a 2014-es évi jelentésében az alábbiakat írta: „Az elmúlt évekhez hasonlóan a BIS olyan készülékek és technológiák felderítésére összpontosított, amely a biztonságot fenyegető potenciális veszélyt rejt magában. 2014-ben a BIS vizsgálata kiterjedt többek között az IP-kamerákra is (hálózatos kamerákra, webkamerákra). A BIS-hez eljutott információkat megerősítették a saját megállapításaik is, amely szerint egy IP-kamerában olyan firmware-t találtak, amely

nem dokumentált rendszergazdafiókot (backdoor) is tartalmazott. A hálózatra történő csatlakozást követően a kamera kommunikálni próbált egy előre beállított domainszerverrel, ami valószínűleg egy nagyobb felhőtároló része lehetett. Hackerek a böngészőbe beírt lekérdezési karakterlánc segítségével a fent említett backdooron keresztül elérhetik a kamerát."[39]

A szolgálatok által közzétett észrevétel nem egyedi. Az interneten több olyan esettel is találkozhatunk, ahol – többnyire kínai – gyártókat támadnak azzal, hogy adathalászás vagy kémkedés céljára fenntartott backdoorokat[40] tartalmaz az eszközt működtető firmware-jük.[41]

Amennyiben a szándékosságot kizárjuk, akkor feltételezhetnénk azt is, hogy a biztonságtechnikaieszköz-gyártók szoftverfejlesztői biztonságvédelmi szempontból kevésbé hozzáértők a szoftverírásban, vagy hanyagság, időhiány miatt nem írják meg megfelelő biztonsági szinten a programot. Bár találhatunk erre is példát (amikor a hozzáférési jelszót titkosítás nélkül, sima szövegként tárolják, vagy webes hozzáférés esetén egyes aloldalak autentikáció nélkül is elérhetők), mégsem csak erről van szó. 2016 nyarán került napvilágra, hogy a világ 67 országában jelen lévő informatikai nagyvállalat eszközeiben szoftveres biztonsági rést találtak, amely több mint 120 különböző típusú berendezést, köztük biztonságtechnikai eszközöket és kamerákat is érint.[42] A gyártó a honlapján elismerte a hibát,[43] és körülbelül másfél hónap alatt megszüntette a biztonsági rést. Ekkora cégnél, ilyen fejlesztői háttérrel nem beszélhetünk hozzá nem értésről. Ebben az esetben egy beépített kényelmi szolgáltatás (az eszközök távoli elérése a cég szerverén keresztül) okozta az alapproblémát. A túl sok eszközhöz rendelt funkció, a beállítási lehetőségek széles skálája és persze a gyors piaci megjelenés miatt valószínűleg nem történt mindenre kiterjedő, alapos sérülékenységi vizsgálat. Az utólagos szoftverjavítás üdvözítő, azonban van egy nagy problémája. Nagyon sok magánfelhasználó, de még komoly cégek is úgy próbálnak üzemeltetési költségeket megtakarítani, hogy nem kötnek karbantartási szerződéseket. Így viszont elmaradnak a szoftverfrissítések, olyan patch-ek, upgrade-ek telepítése, amellyel a gyártó a biztonsági réseket próbálja befoltozni.

Az eddigiekből látható, hogy a technológiai fejlődésnek vannak árnyoldalai is. Egyrészt az új, korszerű berendezések nem csak a védelem, az elhárítás oldalán jelennek meg, másrészt pedig pont a kifelé zajló kommunikáció teremtett egy rést a kívülről jövő támadhatóságban. Szintén a fejlődésnek tudható be, hogy igen nagy mértékben megnövekedett az informatikai úton előálló adathalmaz, amelyben lehetnek személyes, minősített vagy éppen ipari kémkedésnek kitett adatok is. Ebből fakad, hogy a védendő materiális értékek,

---

[39] Annual report of the Security Information Service for 2014. *BIS*. Forrás: www.bis.cz/vyrocni-zpravaEN6c8d.html?ArticleID=1096#_Toc383177470 (A letöltés dátuma: 2018. 06. 02.)

[40] Yu, Xiao (2016): Is the World's Biggest Surveillance Camera Maker Sending Footage to China? *Voa News,* 2016. 11. 21. Forrás: www.voanews.com/a/hikvision-surveillance-cameras-us-embassy-kabuk/3605715.html (A letöltés dátuma: 2018. 07. 21.)

[41] Reynolds, Jake (2013): Dahua DVR Authentication Bypass – CVE-2013-6117. *Depth Security,* 2013. 11. 13. Forrás: https://depthsecurity.com/blog/dahua-dvr-authentication-bypass-cve-2013-6117 (A letöltés dátuma: 2018. 05. 15.)

[42] Kovacs, Eduard (2016): Serious Vulnerability Affects Over 120 D-Link Products. *Security week,* 2016. 07. 07. Forrás: www.securityweek.com/serious-vulnerability-affects-over-120-d-link-products (A letöltés dátuma: 2018. 05. 20.)

[43] Regarding Senr.io Vulnerability Affecting Many D-Link Products. *D-link*. Forrás: www.dlink.com/uk/en/support/support-news/2016/july/15/senrio-vulnerability (A letöltés dátuma: 2018. 05. 07.)

javak egyre inkább kiegészülnek kevésbé kézzel fogható, de egyes esetekben igen nagy értéket képviselő információkkal, adatokkal is. Mindezekből következik, hogy tágabb értelmezésben a komplex objektumvédelem kialakításánál nemcsak a fizikai úton, erőszakos módon történt anyagi javak megszerzése ellen kell védekeznünk, hanem ugyanilyen fontos az alkalmazott információs rendszerek védelme is, amelynek fontos részhalmaza a kiberbűnözés elleni védekezés. A kibertámadások célja többféle lehet. Lehet cél egy rendszer működésének gátlása, megzavarása, illetve irányulhat a rendszer adatainak megszerzésére vagy módosítására. A támadások többségét politikai és vallási aktivisták, gazdasági-bűnözői csoportok, terroristaszervezetek, illetve egyes államok titkosszolgálatai követik el. Azonban nem csak a külső támadásoktól kell félnünk. A Symantec által megjelentetett *Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders* című tanulmányban[44] nemzetközi kutatásokra alapozva vizsgálta azokat az adatvesztéseket, amelyeket belső munkavállalók okoztak. A nemzetközi kutatásba összesen hat ország (Anglia, Egyesült Államok, Kanada, Magyarország, Lengyelország és Dél-afrikai Köztársaság) 3250 irodai dolgozóját vonták be. A megkérdezettek közel fele (48%-a) dolgozik távoli elérést is használva. Közülük 37,5 % használ nem biztonságos hozzáférést. A dolgozók közel háromnegyede (71%) küld bizalmas anyagot a privát e-mail-címére, hogy a vállalaton kívül is dolgozhasson vele. A megkérdezett munkavállalók kétötöde (42%-a) másolta kódolás vagy egyéb védelem nélküli USB-re az irodai munkáját, és vitte haza további munkavégzés céljából. Az esetek 90%-ban a vállalatok rendelkeztek IT-biztonsági szabályzattal, de ez nem akadályozta meg a munkavállalókat a fentiek elkövetésében. E problémák megoldása történhet átfogó, mindenre kiterjedő informatikai szabályozással és a munkatársak megfelelő képzésével, tudatosságuk növelésével. Mindkét megoldás célja, hogy védjük és megőrizzük emberi és technológiai erőforrásainkat.

8.7. Új típusú eszközök a magánbiztonságban

A 21. század új, biztonságvédelem szempontú kihívása a pilóta nélküli repülőgép (UAV, Unmanned Aerial Vehicle), vagy más néven drón. Bár katonai repülésre már az 1960-as évek elejétől alkalmazzák, polgári elterjedése csak néhány éve számottevő. Magyarországon polgári védelem, katasztrófavédelem, közbiztonság, közrendvédelem céljára több mint 10 éve használják.[45] Az eszköz segítséget nyújt(hat) a zöldhatár figyelése során, az árvízi védekezésben, az erdőtüzek felderítésében, a közlekedési helyzet ellenőrzésében, az elfogások, rajtaütések tervezésében és ezek távoli megfigyelésében, valamint a tömegrendezvények biztosításában.[46]

---

[44] WALL, David S. (é. n.) *Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders.* Forrás: www.symantec.com/content/de/de/about/downloads/press/WP_Organizational_Security_and_the_InsiderThreat_Malicious_Negligent_and_Well-Meaning_FINAL.pdf (A letöltés dátuma: 2018. 06. 02.)

[45] VRÁNICS Dávid – ÜVEGES András (2015): Pilóta nélküli légi járművek fejlődése. *Felderítő Szemle,* 14. évf. 2. sz. 130.

[46] PETRÉTEI Dávid (2015): A drónok kriminál technikai és rendészeti felhasználása. *Magyar Bűnüldöző,* 6. évf. 1–3. sz. 71–72.

Az eszköz hazai magánbiztonsági felhasználása még nem számottevő, pedig ezen a területen is számos feladatra bevethető. Hatékonyan és jól képes támogatni a nagy kiterjedésű objektumok kerítésvédelmi rendszerét. A rendszer jelzése esetén a célra repülve, gyorsan kiszűrhetjük a téves riasztásokat, illetve rögzíthetjük és nyomon követhetjük az eseményeket. Az őrzési szolgáltatás minőségének javítása érdekében használhatjuk őrjárat ellenőrzésére vagy éppen ennek kiváltására, azaz kültéri járőrözés végrehajtására.

Fontos kiemelni, hogy a drónok nem csak védelmi berendezésként használhatók. Napjainkban sokkal nagyobb kihívást jelent az ellenük történő védekezés. A könyv írásának időpontjában történik az egységes európai rendelet megalkotása. Az Európai Tanács elfogadta[47] az aktualizált repülésbiztonsági szabályokat. A rendeletben többek között módosítják az Európai Repülésbiztonsági Ügynökség (EASA) megbízását, illetve most először uniós szintű szabályokat tartalmaznak a bármilyen méretű, polgári célokra használt drónokra vonatkozóan.

Az új szabályok meghatározzák azokat az alapelveket, amelyekkel szavatolható a biztonság, a védelem, a magánélet és a személyes adatok védelme, emellett pedig csökkentik a bürokráciát és ösztönzik az innovációt.

Független a törvényalkotás miként jétől, annak megjelenése csak a „jó szándékú" reptetést szabályozza, és nem gátja a különböző bűncselekmények végrehajtására bevetett drónoknak.

Jelenleg a kereskedelemben kapható drónok sebessége már eléri a 290 km/h-t. A jelenlegi megfizethető áru drónészlelési technológiák (radar, termokamera, hang) maximum egy-két kilométeres hatótávolságot tesznek lehetővé. Ez azt jelenti, hogy ilyen sebesség mellett körülbelül 12–25 másodperc áll rendelkezésre az észleléstől a megsemmisítésig. Ez még kevesebb is lehet, ha a drón már olyan területre ért, amely felett nem lehet lelőni (például tömegrendezvény).

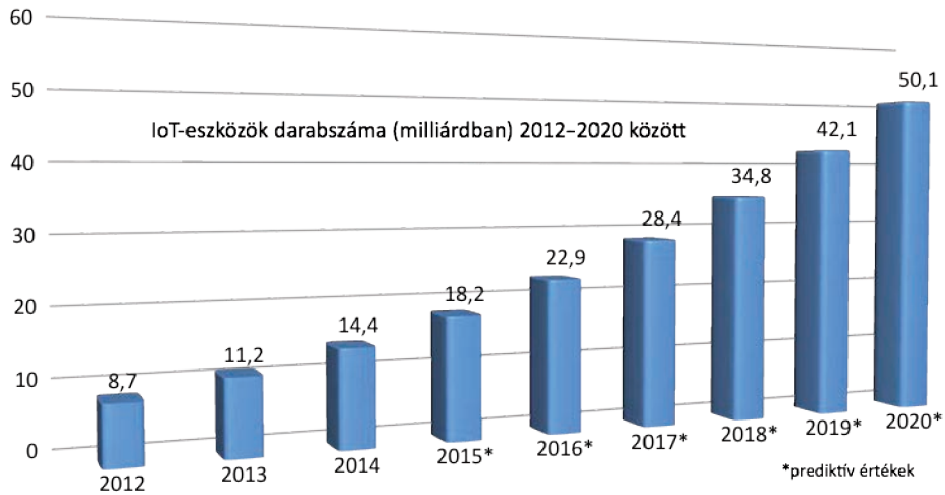
A technológiai fejlődés másik nagy kockázata biztonsági szempontból az egyre nagyobb számban megjelenő IoT (Internet of Things, a Dolgok Internete, de használatos még az „Internet ott tárgyak" kifejezés is), azaz az interneten keresztül elérhető eszközök. A Cisco Internet Business Solutions Group (IBSG) tanulmánya 2020-ra 50 milliárd IoT-eszközt prognosztizál.[48] Ezzel egyetértésben, de ezen is túlmutat a Strategy Meets Action (SMA) 2014-es kutatása, amely 2035-re 1000 milliárdra prognosztizálja az IoT-eszközök darabszámát.[49]

---

[47] *Drones: reform of EU aviation safety* (é. n.). Forrás: www.consilium.europa.eu/en/policies/drones/ (A letöltés dátuma: 2018. 05. 05.)

[48] Evans, Dave (2011): *The Internet of Things.* Forrás: www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (A letöltés dátuma: 2018. 03. 20.)

[49] *SMA, The Internet of Things: Creating a Connected World.* Forrás: https://strategymeetsaction.com/about-sma/ (A letöltés dátuma: 2018. 04. 16.)



14. ábra

IoT-eszközök darabszáma (milliárdban) 2012 és 2020 között

Forrás: a szerző saját szerkesztése

Az eszközök választéka már jelenleg is széles körű. A már szinte hétköznapinak számító okostévén túl találhatunk okos hűtőszekrényt, mosógépet, kazánt, de még kávéfőzőt is. Egyre népszerűbbek az „intelligens ház" (smart home) kialakítások, amelyeknek szerves részét képezik az IoT-eszközök. Egy ilyen rendszernél interneten keresztül mobiltelefon vagy táblagép segítségével vezérelhetjük a különböző otthoni berendezéseinket, vagy felügyelhetjük a fűtést/hűtést, a világítást, a kamerát vagy a behatolás- és támadásjelző rendszereinket. Ezek a funkciók nagyon kényelmesek, viszont számos veszélyt hordoznak magukban. Mobiltelefonunk ebben a szerepkörben egy teljesen új értelmezést nyert. Ebbe az eszközbe integrálódik a teljes biztonságunk, amelyen keresztül elérhetjük otthoni és céges levelezéseinket, hálózati tárolónkat, fizethetünk vele vagy felügyelhetjük a kameráinkat, ki- és bekapcsolhatjuk a riasztónkat, illetve használhatjuk beléptetőrendszerben kártya helyett, de vezérelhetjük vele a bejárati ajtónk zárját is. Egyes gépkocsiknál már lehetőség van a telefonon keresztüli nyitásra, illetve zárásra. Mindezen funkciókhoz hozzáférhetünk egy kifigyelhető jelkód vagy a születési évünkre beállított jelszó birtokában.