



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet



OE-BGK
2025.

Hallgató neve: Márfi Ákos Gábor
Hallgató törzskönyvi száma: T012280/FI12904/B



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Márfi Ákos Gábor

Szakedolgozat száma: [REDACTED]

Törzskönyvi száma: T012280/FI12904/B

Neptun kódja: [REDACTED]

Szak: biztonságtechnikai mérnöki

Specializáció: biztonságtechnikai mérnöki - biztonságtechnikai

A dolgozat címe: Beléptetőrendszerek és zárrendszerek fejlődése, típusai és integrált alkalmazásuk a modern biztonságtechnikában

A dolgozat címe angolul: Development, Types, and Integrated Application of Access Control and Locking Systems in Modern Security Technology

A feladat részletezése:

1. A biztonságtechnika fejlődéstörténete.
2. Korszerű beléptetőrendszerek típusai, működési elvei.
3. Zárrendszerek típusai és technológiai fejlődése.
4. Integrált beléptető- és zárrendszerek alkalmazása különböző környezetekben.
5. Irányzatok, kockázatok és jövőbeli fejlődési lehetőségek.

Intézményi konzulens neve: Dr. Hell Péter Miksa

A kiadott téma elévülési határideje: 2027. 12. 15.

Beadási határidő: 2025. 12. 15.

A szakedolgozat: Nem titkos.

Kiadva: Budapest, 2025. 10. 27.



[Signature]
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom. 2025. 12. 15.

[Signature]
belső konzulens

.....
külső konzulens



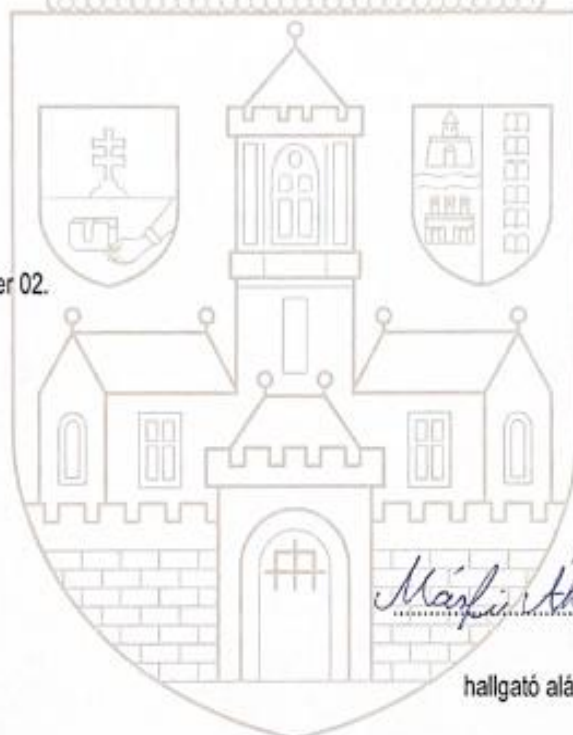
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet

HALLGATÓI NYILATKOZAT

Alulírott Márfi Ákos Gábor [REDACTED] hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára terítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2025. december 02.



Márfi Ákos Gábor

hallgató aláírása

BELÉPTETŐRENDSZEREK ÉS ZÁRRENDSZEREK
FEJLŐDÉSE, TÍPUSAI ÉS INTEGRÁLT ALKALMAZÁSUK A
MODERN BIZTONSÁGTECHNIKÁBAN

TARTALOMJEGYZÉK

BEVEZETÉS	7
1. A BIZTONSÁGTECHNIKA FEJLŐDÉSTÖRTÉNETE	9
1.1. Őskor.....	11
1.2. Ókor	13
1.3. Középkor.....	17
1.4. Újkor	20
1.5. Az első riasztó.....	21
1.6. További fontos mérföldkövek	24
2. KORSZERŰ BELÉPTETŐRENDSZEREK TÍPUSAI, MŰKÖDÉSI ELVEI	26
2.1. A beléptetőrendszerek alapjai és azonosítási módok	26
2.2. Beléptetőrendszerek csoportosítása	28
2.3. Azonosítási módok	29
2.4. Belépőkártyák típusai	31
2.5. Példák beléptetőrendszer eszközökre	33
2.6. A holnap belépőkártyája	35
2.7. Tervezés és kivitelezés	36
3. ZÁRRENDSZEREK TÍPUSAI ÉS TECHNOLÓGIAI FEJLŐDÉSE	38
3.1. Zárak technológiai fejlődése	38
3.2. Zárak fogalma, típusai	41
3.3. Zárbetétek biztonsági szintjei	46
3.4. Zárrendszerek.....	47
3.5. Kulcsok működése és típusai.....	50
3.5.1. Működés.....	50
3.5.2. Legismertebb kulcstípusok	51
4. INTEGRÁLT BELÉPTETŐ- ÉS ZÁRRENDSZEREK ALKALMAZÁSA KÜLÖNBÖZŐ KÖRNYEZETEKBE	52
4.1. Integrált vagyonvédelem.....	52
4.2. Integrált beléptetőrendszerek különböző környezetekben.....	53
4.2.1. Vállalati környezet.....	53
4.2.2. Kórházi környezet.....	55
4.2.3. Könyvtári környezet	56

4.2.4.	Szoftverek	57
4.3.	Integrált zárrendszerek.....	58
5.	IRÁNYZATOK, KOCKÁZATOK ÉS JÖVŐBELI FEJLŐDÉSI LEHETŐSÉGEK.....	60
5.1.	Irányzatok a biztonságtechnikában.....	60
5.1.1.	Digitalizáció.....	60
5.1.2.	IoT – Internet of Things (Dolgok Internete)	61
5.1.3.	Biometrikus azonosítás elterjedése	61
5.1.4.	A mesterséges intelligencia megjelenése a biztonságtechnikában	63
5.2.	Kockázatok	63
5.2.1.	Kiberbiztonsági kockázatok.....	63
5.2.2.	Biometrikus adatok kockázata	65
5.3.	Emberi kockázat	66
5.3.1.	Felhasználói kockázatok	67
5.3.2.	Operátori kockázatok	67
5.3.3.	Oktatások	68
5.4.	Fejlődési lehetőségek.....	68
5.4.1.	Érintésmentes beléptetés.....	68
5.4.2.	Egységes rendszerek	68
5.4.3.	Mesterséges intelligencia a beléptetőrendszerek területén	69
5.4.4.	Szabály- és attribútum alapú beléptetési rendszerek	69
5.4.5.	Intelligens analitika alkalmazása	69
5.4.6.	Smart (okos) kártyák alkalmazása	69
5.4.7.	Mobilos azonosítók elterjedése.....	70
5.4.8.	Drónok megjelenése	70
ÖSSZEGZÉS		71
SUMMARY		73
HIVATKOZÁSOK.....		75
ÁBRAJEGYZÉK.....		80

BEVEZETÉS

Erre a témára azért esett a választásom, mert 2020. márciusa óta egy multinacionális vállalatnál dolgozok a vállalatbiztonság területén. Ekkor gyakornokként kezdtem a cégnél, ahol napról napra egyre több mindenbe láthattam bele, de éreztem, hogy ez még csak a jéghegy csúcsa. 2021. júliusában felvettek főállású munkatársnak és ekkor kaptam meg a teljes hozzáférést a rendszereinkhez. Innentől kezdve jogosult lettem például belépőkártyákat készíteni. Ez a teljes folyamatot takarja, a nyomtatástól egészen a kódolásig. Természetesen már a beléptetőrendszerhez is hozzáfértem, ahol jogosultságokat osztottam, jogcsoportokat hoztam létre, kollégák belépőkártyáit tiltottam le. A grafikus felületen megtanultam, hogy távolról, hogyan tudok kinyitni egy helyiséget, s a többi. A későbbiekben természetesen abba a részbe is beleláttam, hogy egyáltalán hogyan épül fel egy ilyen rendszer, mik a szükséges feltételek, eszközök. Céлом az volt ennek a dolgozatnak a megírásával, hogy mélyebben beleássam magamat ebbe a világba és megismerkedjek a legújabb technológiákkal is, ne csak azokat ismerjem, amiket napi szinten a munkám során használok.

Az emberiség a fennállása óta a biztonságra törekszik. Ez egy alapvető igény, ami a mai napig fennáll, és szinte biztos, hogy a jövőben is prioritást fog élvezni. Az első felében a dolgozatnak a beléptetőrendszerek, majd a második felében a zárrendszerek fejlődését, felépítését, működését és integrációját mutatom be biztonságtechnikai környezetben. A technológia fejlődésével az évek során eljutottunk az egyszerű záraktól egészen az intelligens, hálózatba kapcsolt, automatizált rendszerekig. Ezek mára informatikai és elektronikai megoldások összetett rendszerét alkalmazzák, például a jogosultságok szabályozására, így arról már nem beszélhetünk, hogy ezek csak fizikai akadályokat képeznek az illetéktelen behatolók számára, mivel sokkal komplexebb a működési elvük, mint például egy sima hengerzárbetété.

A dolgozatomban strukturáltan fogom felvezetni a témákat. Először a biztonságtechnika fejlődéstörténetét fogom bemutatni, amely véleményem szerint elengedhetetlen ahhoz, hogy teljes képet kapjunk a választott témáról. Ez többek között azért lesz érdekes, mert itt megláthatjuk, hogy az évszázadok során mekkora fejlődésen esett át ez a szektor.

A kezdeti történeti áttekintés után áttérek a korszerű beléptető rendszerekre. Ezek típusait, működési elvüket részleteiben írom le. Részletezve bemutatom a különböző azonosítási technológiákat, rendszerelemeket (központi egység, kártyaolvasó, vezérlő, s a többi).

A beléptetőrendszerek után a zárrendszereket definiálom. Ebben a fejezetben fogok kitérni például arra is, hogy mi a különbség az elektromos záron belül egy normál működésű zár, illetve egy fordított működésű zár között, de először itt is az alapok fognak előnyt élvezni. Milyen típusok léteznek, a mechanikus zártól az elektromos záron keresztül egészen az okoszárákig.

A 4. fejezetben különböző környezetekben fogom bemutatni a beléptető- és zárrendszerek alkalmazását. Itt leginkább irodai és vállalati környezetben vett alkalmazásokra fogok kitérni, azonban szót fogok ejteni a lakossági és okosotthon rendszerekről is, mint például, hogy mobil alkalmazás segítségével hogyan lehet akár egy egész házat irányítani, hogyan tudjuk távolról kinyitni az ingatlanunk bejárati ajtaját. Kis részben érintem az ipari, illetve kritikus infrastruktúrákat is. Például, hogy egy kórházban miért van óriási szükség magára a redundanciára, illetve, hogy mi is az a redundancia egyáltalán. Továbbá ismertetem, hogy különböző gyártók milyen megoldásokat találtak ki arra, hogy például egy irodaházban egységes rendszer tudjon működni, hogyan tudják minél több eszközzel kielégíteni az ügyfelek biztonsági elvárásait.

Az 5. egyben az utolsó fejezetben az irányzatok, kockázatok és jövőbeli fejlődési lehetőségekről fogok írni. Az ember manapság már csak a fejét kapkodja, mert szinte minden nap kijön valami technikai újdonság. A fejlődési trendeket érintve szót fogok ejteni a biometriáról, valamint az AI-ról (magyarul MI: Mesterséges Intelligencia) is. Azoknál a dolgoknál, amikről még nem tudunk sok mindent, nem találkoztunk vele, felmerülhet bennünk, hogy ez mennyire lehet biztonságos egyáltalán. A kockázatoknál érinteni fogom a kiberbiztonsági sebezhetőségeket is. Valószínűnek tartom, hogy a már előbb említett mesterséges intelligencia elég nagy szerepet fog kapni. A kérdés itt az lesz, hogy a jövőben el tudunk-e szakadni a már jól bevált eszközöktől, vagy sem, illetve az, hogy egyáltalán el akarunk-e szakadni tőlük.

A kutatást befejeztem 2025.11.27. napján.

1. A BIZTONSÁGTECHNIKA FEJLŐDÉSTÖRTÉNETE

Ebben a fejezetben bemutatom, hogy a biztonságtechnika hogyan fejlődött az évszázadok során. Először a fogalmakat kell tisztázni, azért, hogy még mélyebben betekinthessünk, és még jobban megérthessük, hogy valójában mi is az a biztonságtechnika. Nagyon fontosnak tartom, hogy megismerjük a biztonság, a technika, illetve magának a biztonságtechnikának a fogalmát, mert így tudunk egy teljes képet kapni a következő fejezetekben.

A biztonságot nagyon sok féle képpen lehet értelmezni, ennek köszönhetően megannyi meghatározás, fogalom került leírásra az évek során. A különböző megfogalmazásokban természetesen nagyon sok a hasonlóság, ugyanis többnyire mindegyik egy veszélyektől, fenyegetésektől mentes állapotot ír le. A biztonság szó hallatán egyénenként eltérhet az értelmezés, ugyanis nem mindenkinek ugyanaz jut eszébe ennek a szónak a hallatán. Saját szavakkal a következő képpen tudnám megfogalmazni a biztonságot: Olyan veszélytelen állapot, ahol teljesen hétköznapi helyzetben - például az utcán sétálva, bevásárlás közben, munkában - egészségünket, testi épségünket, anyagi jólétünket semmilyen külső behatástól nem kell féltetnünk. A szakdolgozatom leginkább a személy- és vagyonbiztonság, ezen belül is a vagyonbiztonság területére irányul. A biztonság egy komplexebb megfogalmazása már egy szervezet állapotát is taglalja a személyeken kívül is. Összefoglalva ez a meghatározás arra terjed ki, hogy az egyént vagy a szervezetet nem veszélyezteteti szándékos, jogellenes cselekedet. Ezt a veszélyeztetések nélküli állapotot a velük szembe alkalmazott védelmi intézkedések, valamint erőforrások együttes megléte határozza meg. [1] A biztonság olyannyira fontos az ember életében, hogy Abraham Maslow piramisának öt szintje közül a másodikat foglalja el. Az amerikai pszichológus létrehozott egy piramist, ami a szükségletelméletről szól és a mai napig egy meghatározó szerepet tölt be, amikor az emberi szükségleteket kell csoportosítani, rangsorolni. A biztonság szükségességét csak a fiziológiai szükségletek előzik meg, mivel ezek nélkül az emberiség nem is tudna létezni. Ilyen szükségletek például az evés, ivás, alvás, s a többi. Az 1. ábra magát a piramist mutatja be, amit Maslow 1943-ban alkotott meg. A piramisra egy hierarchiaként kell tekinteni. Amíg az embernek nincsenek meg a fiziológia

szükségei, addig nem foglalkozik a biztonsággal. Amíg nincsen meg a biztonság, addig nem foglalkozik a szociális szükségletekkel, és így tovább.



1. ábra: Maslow-piramis [2]

A biztonság fogalmának megismerése után fontosnak tartom, hogy a technika meghatározását is bemutassam. Ókori görög „techné” szóból származik, ami jelenthet ügyességet vagy művészetet, ami valamilyen tárgy, eszköz elkészítésére vonatkozik. A biztonsághoz hasonlóan ennek is több fajta értelmezése létezik. Legjobban példákon keresztül lehet bemutatni, hogy mit is jelent ez a szó. Az ősidőkben például a halászatot, vadászatot, lakóépületek létrehozását, és ezeken kívül még sok mást jelentett ez a mondatem. Ezek a tevékenységek egyszerű eszközhasználatból fejlődtek ki. Az évek során természetesen ezek az egyszerű eszközök nagyon sokat fejlődtek, vadászathoz például már nem lándzsákat használunk, hanem lőfegyvereket a legtöbb esetben. [3]

A két szót összetéve megkapjuk a biztonságtechnikát, aminek az előző két fogalomhoz hasonlóan rengeteg definíciója ismert. Elgondolkozva az előbbi meghatározásokon sejteni lehet, hogy valami olyan eszközöket foglal magába a biztonságtechnika, amik a biztonságot teremtik meg, vagy tartják fent. Ezek lehetnek mechanikai, elektronikai, elektro-mechanikai, gépészeti eszközök, illetve olyan műszaki-technikai megoldások, melyek elősegítik az eredményes személy- és vagyonbiztonságot. Egy szélesebb körű értelmezésben a biztonságtechnikának a munkavédelemhez, a tűzvédelemhez, de még a katasztrófabiztonsághoz is köthető. Ezeken kívül számos olyan terület létezik még,

amihez szorosan kötődik. Az előbb felsoroltak alapján már tudjuk, hogy számottevő ponton kapcsolódik más műszaki tudományhoz, mint például a gépészmérnöki vagy a villamosmérnöki. Összefoglalva a biztonságtechnika azon technikai eszközöket, rendszereket jelenti, amik elősegítik a biztonság fenntartását, illetve csökkentik a kockázatát a vagyoni, illetve embert érő károknak. [4] [5]

Az alapfogalmak tisztázása után a következő bekezdésekben áttekintjük a történeti áttekintésre egészen az őskortól napjainkig.

1.1. Őskor

Az őskorban a beszéd kialakulása nagyon nagy hatással volt magára a biztonságra is. Eleinte csak hangokkal hívták fel a veszélyre a figyelmet, majd az idő előrehaladtával ezen hangok változtatásával folytonos kommunikációt értek el. Már a kezdetleges hangok is rendkívül fontosak voltak, mert ezekkel elkerülhették a sérüléseket, esetenként az egész törzs kihalását, mivel egy fontos tag elvesztése is végzetes lehetett az egész csoportra. A következő fontos és nagyon kérdéses pont a megfelelő lakóhely és környezet kiválasztása volt az ősember életében. [6] A 2. ábrán látható a hazai Kis-kevélyi-barlang bejárata. A képen jól megfigyelhető, hogy milyen széles és magas a bejárata. A barlang a Pilis hegységben található.



2. ábra: Kis-kevélyi-barlang bejárata [7]

Az idő előrehaladtával az ősember elhagyta a barlangokat és más élőhely felé tekintett, mivel ezek nem mindenhol voltak elérhetőek. A fejlődés következő pontjánál már

rájöttek, hogy stabilabb lesz a menedék, ha a fa rudakat leássák a földbe és ezeket ágakkal veszik körbe. Ezzel a módszerrel egy ellenállóbb szerkezetet kaptak, amire növényi szöveteket, illetve állati bőroket helyeztek, így már mondhatjuk azt is, hogy kezdetleges tetőszerkezetet hoztak létre maguknak. [8] A 3. ábra ezt az építkezési módszert mutatja be.



3. ábra: Nyeregsátor [8]

Ezt követően az építkezés már eljutott a legfelső fokra az akkori fejlettséget tekintve. Ekkor már ténylegesen házakat építettek maguknak letelepedési célból. Ezt a módot nagyon jól bemutatja Çatalhöyük az első falunak tekinthető település, amely Törökország területén található. Az itt élő emberek már földműveléssel és állattartással is foglalkoztak, ezért volt szükséges a letelepedés, illetve az időtálló épület. Érdekesség, hogy egymás mellé építették házaikat, olyannyira, hogy falaik közösek voltak. A bejárat a ház tetején volt található és létra segítségével tudtak bemenni, illetve kijönni a házból. A falu csúcsidőszakában nyolcezer ember is élhetett itt. [9] Az 4. ábra szemlélteti, hogy hogyan nézhetek ki a lakóépületek, valamint a település a maga korában.



4. ábra: Çatalhöyük [10]

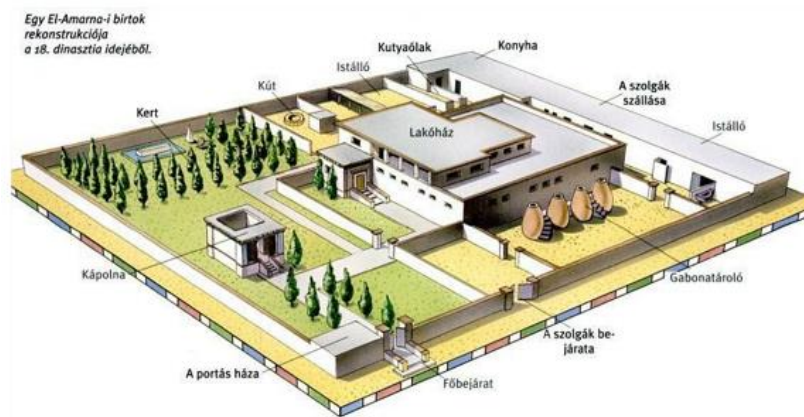
Az első tényleges biztonságtechnikai eszköz a házikutya volt. A házikutya a farkas domesztikációjából jött létre és először vadászatra majd később a ház őrzésére használták. Az első erre utaló lelet Kr. e. 12 000 körüli időből származik. [11] Nem meglepő módon a kutya a kitűnő érzékszervei miatt lett házasítva, továbbá a rendkívül jó alkalmazkodó képessége, illetve tanulékonyága miatt.

Az őskor kezdetleges biztonságtechnikai megoldásai után érdemes az ókort is szemügyre venni. Az ókort meghatározta már a szervezett életforma, illetve ekkor már társadalmak alakultak ki. Ennél a pontnál már nem csak az egyének, biztonsága volt fontos, hanem területeké, országoké is. A legtöbb biztonságtechnika releváns információt nyújtó országokat mutatom be a következő bekezdésekben.

1.2. Ókor

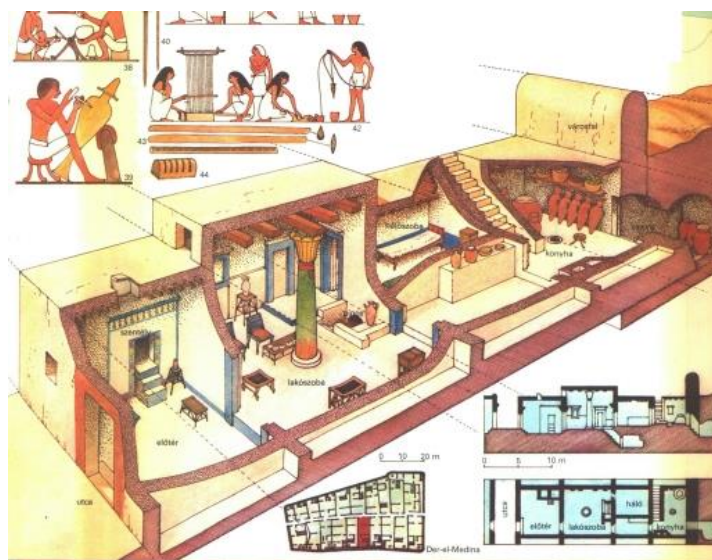
Az első ilyen ország Egyiptom. Az egyiptomiak is a biztonságra törekedtek a házaik megépítésénél. Az épületeik kellő védelmet tudtak nyújtani a külső behatásokkal szemben, mivel ezeket már vályogtéglából, égetett iszaptéglából, valamint fából készítették. Figyeltek már arra is, hogy a házakon minél kevesebb nyílás legyen, amiken keresztül a bejutás egyszerű és gyors módon történhetne. A gazdagabb családok, már olyan épületekben laktak, amiket kerítés vett körül. A következő 5. ábrán jól

megfigyelhető a kerítés is, valamint, hogy a házhoz külön bejáraton egy portán keresztül lehetett bejutni, míg a szolgáknak szintén volt egy másik bejárata porta nélkül. A ház mögött megfigyelhető, hogy a kutyáknak is volt egy elkülönített hely, így ez arra enged következtetni, hogy az objektumot kutyákkal is védték. Érdekesség még, hogy az épület ablakai, illetve ajtaja nem nyílt közvetlenül az utcára, továbbá az ablakok magasan pozícionáltak, kicsik voltak. A gabona tároló és a kút hosszabb idejű tartózkodás esetén is elláthatták az ott élőket étellemmel, valamint vízzel. [8]



5. ábra: Gazdag egyiptomi család birtoka [8]

A településeken belül természetesen teljesen máshogy néztek ki a lakóépületek. A hosszúkás elrendezést részesítették előnyben, mivel kicsi volt a hely, amit használatba vehettek. Ezeknél a házaknál is nagy hangsúlyt fektettek a biztonságra, ugyanis a legtöbb háznak egy bejárata és egy ablaka volt az utca felől. A 6. ábrán figyelhető meg egy átlagos elrendezésű ház. [8]



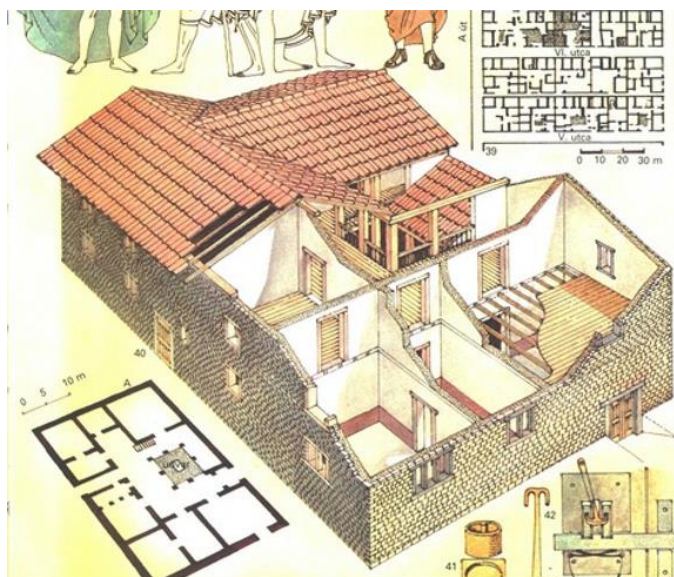
6. ábra: Egyiptomi kézművesek háza [12]

Ebből az elrendezési módból az is kiderül, hogy ekkor a legfontosabb érték az ember életében az élelem volt. Nem hiába a pince helyezkedett el a legtávolabb a bejáratától és volt az utolsó helyiség az épületben. A tolvajok helyzetét nehezítették ezzel. A bejáratú ajtók fából készültek, amiket éjszakára bezártak oly módon, hogy belülről keresztbe helyeztek egy fadarabot. A biztonságot nappal is fenntartották, ugyanis ekkor is maradt mindig valaki a házban, általában az idősek. Azonban természetesen akadtak olyan helyzetek, amikor a ház üresen maradt. Az egyiptomiak ilyenkor bezárták a házaikat. Így jutunk el a záruk feltalálásáig, ugyanis a mai záruk őseit az egyiptomiak találták fel. [8] Az egyiptomiak által kitalált zárat a 3. fejezetben mutatom be.

Kijelenthetjük, hogy ebben az időben az egyiptomiak is már foglalkoztak vele, hogy minél biztonságosabb körülmények között éljenek. Elsősorban mechanikai védelmet alkalmaztak. Ilyen védelem volt a gazdagabb családoknál például, hogy házaikat kerítéssel vették körbe, de a mechanikai védelmen kívül már portást, illetve kutyát is használtak már. Biztonságtechnika szempontjából egy nagyon nagy lépést tettek a fejlődés útján azzal, hogy feltalálták a zárat.

Az ókori Görögországban is nagyon nagy hangsúlyt fektettek a biztonságra. Sok ötletet vettek át az egyiptomiaktól, vannak, amiket tovább is fejlesztettek például a zárat. Hasonló módon a házaikat úgy építették, hogy a bejutás ne legyen egyszerű. Itt is jól

megfigyelhető, hogy az ablakokat magasan helyezték el a házakon. A 7. ábrán egy ókori görög ház látható. A kép jobb alsó sarkában pedig megfigyelhetjük, hogy ők milyen zárat használtak ajtajaikon. A 42-es számmal megjelölt eszköz pedig a kulcs volt. [8] Ennek a zárnak a működését is a 3. fejezetben mutatom be.



7. ábra: Ókori görög lakóépület [8]

Elmondható, hogy az ókori Görögországban is tudatosak voltak a biztonsággal kapcsolatban. Az egyiptomiaktól átvett módszereket alkalmazták, illetve újítottak is ezeken, ezzel még biztonságosabbá téve életterületüket. [8]

Ebben a bekezdésben a Római Birodalom kerül bemutatásra biztonsági szempontból. Az ókorban jól megfigyelhető, hogy a különböző országok, birodalmak sok technikai újítás, építési technikát vettek át egymástól. A technikai fejlettségük már egy magasabb szinten volt, ennek köszönhetően nem ugyanazokat a módszereket alkalmazták, hanem még tovább fejlesztették azokat. A házaikat igyekeztek úgy megépíteni, hogy az utcára ne is, vagy csak kevés ablak nézzen. [8] Az építkezési módot a 8. ábra mutatja be.



8. ábra: Ókori római lakóépület [8]

Az ajtóikat, illetve ládáikat zárral látták el. Ezekben a ládában tartották az értékeiket, amik vaspántokkal voltak rögzítve az aljathoz, így biztosítva azt, hogy ne lehessen egyszerűen felemelni és elvinni. Ezek a zárok már annyira fejlettek voltak, hogy elmondható, hogy valódi védelmet jelentettek az értékekre nézve. [8]

1.3. Középkor

A középkor kezdetén technikai szempontból visszaesést lehetett megfigyelni, a fejlődés csak nagyon lassan kezdődött meg. Fejlődésnek azt tekinthetjük, hogy az eszközök már vasból készültek, illetve, hogy emberi, állati erő helyett már kihasználták a környezet adta lehetőségeket víz, szélmalom segítségével. Épületek szempontjából a legfontosabbak a nemesek lakótornyai voltak, melyek kőből és fából készültek. Ezeket biztonsági szempontokat figyelembe véve alakították ki, ugyanis általában 3-4 emeletesek voltak. A földszinten nem alakítottak ki se ablakot, se bejáratot. A bejárat is az első emeleten helyezkedett el, illetve az ablakok is csak az emeleteken voltak megtalálhatóak. Az elhelyezkedése is fontos volt, ugyanis megpróbálták forrás vagy kút fölé építeni, hogy víz mindenképpen legyen a közelben. [8] A 9. ábrán a nagyvázsonyi Kinizsi vár látható. Itt jól megfigyelhető a lakótorony kialakítása.



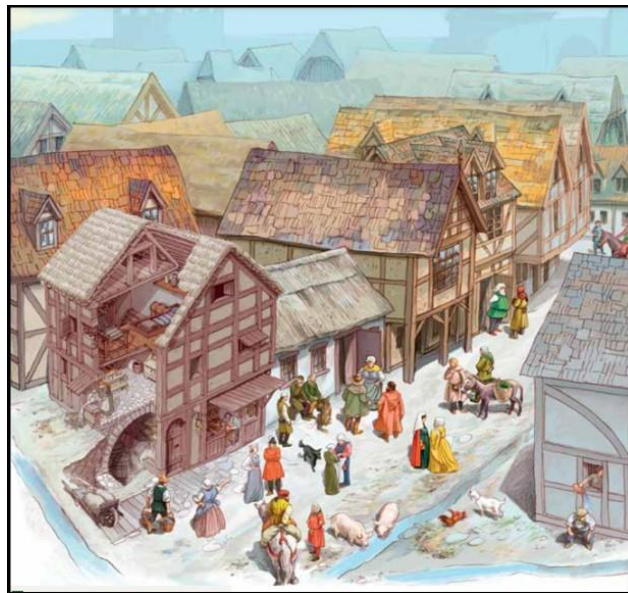
9. ábra: Nagyvázsonyi Kinizsi vár [13]

Ebben az időben a ház körüli kis területet kerítéssel zárták le, így kialakultak a telkek. Az egymás mellett elhelyezkedő telkek körül kialakultak az utcák. A települések növekedésének köszönhetően először kialakultak a falvak majd a falvakból a városok. A városokat a biztonság érdekében először árokkal vették körbe, majd később az árok és a város köré fából épült kerítést emeltek. Ezeken kapukat hoztak létre a be- és kijutást elősegítve. A fából készített kerítéseket idővel fejlesztették és kőre cserélték azokat. Ezek már nem kerítések voltak, hanem sokkal inkább falak. Ezek a falak látták el a terület mechanikai védelmét. A kapuk közelében a fal egy-egy helyein tornyokat alakítottak ki, amik az őrködésre szolgáltak. [8] A 10. ábrán jól megfigyelhető a település biztonságát elősegítő árok, illetve a fából készült kerítés is.



10. ábra: Középkori település részlet [14]

A városokon belül a helyhiány miatt elkezdtek felfelé építkezni. A polgárok a házaikat úgy alakították ki, hogy azok egyben a munkahelyüket is jelentették. A földszinten hozták létre például a műhelyt, kocsmát, boltot, s a többi. Az emeleti részek szolgáltak a lakhatásra. A földszinti bejáratokat ajtózárrakkal látták már el, melyek eleinte hasonlóak voltak a római zárahhoz. A kor végéhez közeledve már fejlesztettek ezeken, így egy magasabb biztonsági szintet elérve. Eleinte az ablakok még nem voltak üvegezettek, ezek csak a kor végére terjedtek el. Házaik alatt pincét hoztak létre, amit tárolásra használtak. Építőanyagként a fát és a követ használták. A városokban, falvakban is megtalálható volt a templom, ami biztonsági szempontból is egy nagyon fontos helyé nőtte ki magát. Abban az esetben, ha a város falain sikeresen áthatolt az ellenség, akkor az asszonyok a gyerekeikkel, illetve az idősek ide menekültek. Sokszor ez volt az egyetlen kőből épült épület, ami nagyobb biztonságot nyújtott. [8] A 11. ábrán egy középkori városrészlet látható, valamint a házaik belső kialakítása, elrendezése.

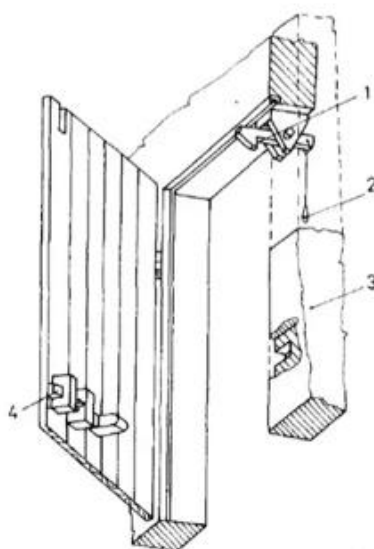


11. ábra: Középkori városrészlet [15]

A polgárok kötelesek voltak részt venni a város védelmében. A kor végére megjelentek a vasból készített zárah is, amit a rómaiak már régen használtak. Mesterség is kifejlődött, ami a zárkovács volt. Ők nem csak zárahkat készítettek, hanem az ajtóvasalatokat is, amelyek stílusban megegyeztek a zárahkal. Ezek csak a városokban terjedtek el, a falvakban élők maguk kellett, hogy megoldják az otthonaik zárását. Ki is találtak erre módszereket. Ezeket általában fából készítették el és az egyik ilyen a facsapda elnevezésű

zár volt. Az ajtótokra kampós csapdát szereltek, amelynek a feje a saját súlyánál fogva zárt állapotba esik. A kampónak ferde oldallapot alakítottak ki, ami miatt be tudott magától záródni az ajtó. Nyitáshoz ezt a csapdát fel kellett emelni, ami a csapda másik végén található zsinór segítségével történt. Az ajtó belső felére reteszt is raktak. [16] A házban lévő értékeket is elkezdtek védeni. Erre a célra ládákat használtak, melyeket zárral, illetve rejtett rekeszekkel láttak el. A 12. ábrán a facsapda és a tolóretesz látható.

A középkor fejlődési szempontból elég lassan indult, de a végére fellendült. Elmondható, hogy ebben a korban is figyeltek a biztonságra, amit árkokkal, kerítésekkel majd falakkal, zárral igyekeztek a kor engedte legmagasabb szintre emelni. A zárok újra feltalálásával sokkal biztonságosabb életet tudtak maguk számára biztosítani.



Facsapda és tolóretesz a középkorból
1 csapda; 2 zsinór; 3 ajtótok; 4 retesz

12. ábra: Facsapda a középkorból [16]

1.4. Újkor

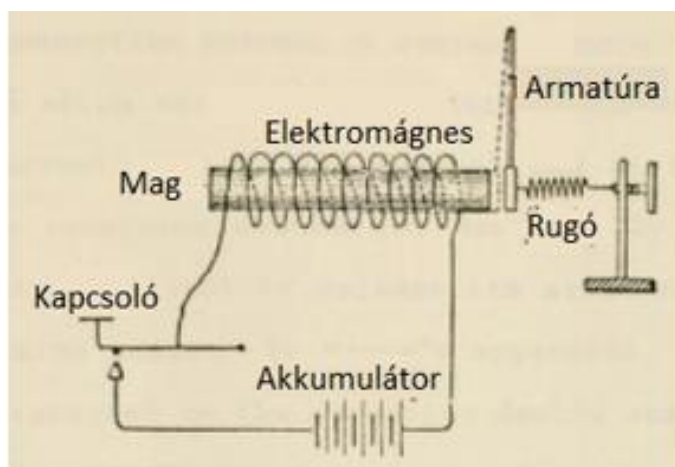
Az újkorban az ipar színvonala rohamosan nőni kezdett a gazdaságfejlődésnek köszönhetően. Ekkor a jobb anyagi helyzet lehetővé tette, hogy a papokon kívül már a polgárok is foglalkozzanak a technika fejlesztésével. A céhek ebben a fejlődésben nagyon nagy szerepet játszottak. Ezeken a helyeken tudtak már bonyolult szerkezeteket is

létrehozni. Az egyik ilyen szerkezet például az óra volt. Elkezdtek a gyerekeket iskolákban tanítani, így egyre több ember tudott a technika fejlesztésével foglalkozni.

A tudományos-technikai forradalmat a reneszánsz kor alapozta meg. Ekkor indultak el az emberek a tudomány és a technika fejlődésének útján. A céhekben dolgozók elismertsége rohamosan nőtt, illetve a tudósok számításai lehetővé tették, hogy a fejlődés fellendüljön. A városok biztonsága szempontjából változtatni kellett a védelmen, ugyanis a lőpor elterjedésével a henger alakú tornyok már nem tudtak ellenállni a lövéseknek, mivel a többszöri lövedék becsapódások után azok leomlottak. A tornyok után alacsonyabb, szélesebb védműveket építettek. Ezeket már bástyáknak hívták, és már nem henger formájúak voltak, hanem szögletesek. Ezzel a módszerrel ráláttak az ágyúkkal a szomszédos bástya előtti területre is. Ebben a korban is a céhek voltak a felelősek a védelemért, továbbá ők is tartották karban. Évente ellenőrizték a bástyák állapotát, illetve leltározták az eszközöket.

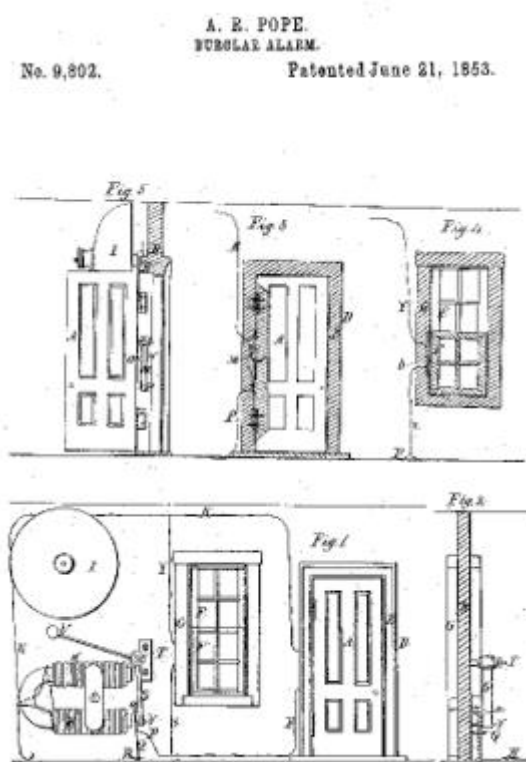
1.5. Az első riasztó

Az időben ugorva eljutunk az első elektromos árammal működő biztonságtechnikai eszközhöz, ami egy riasztórendszer volt. A riasztót Augustus Russel Pope (1819-1858) szabadalmaztatta az Egyesült Államokban 1853-ban. A rendszer elektromágnesességgel működő csengőből, vezetékekből és egy akkumulátorból áll. [8] A 13. ábrán látható maga a szerkezet, ami létrehozza a mechanikai mozgást.



13. ábra: Elektromágnessel működő mechanikai mozgást létrehozó szerkezet [8]

Ehhez hasonló csengőket használunk manapság is. Ahhoz, hogy működőképes legyen a szerkezet kellett csengő, elektromágnes, akkumulátor, megszakító- érintkező kapcsoló, fémlemez, amin volt egy kis kalapács, amivel megszólaltatták a csengőt, illetve lágyvas és fémhuzalok. A csengőn kívül ezek egy áramkörbe vannak csatlakoztatva. A csengő működéshez arra volt szükség, hogy az áramkör záródjon, ekkor az elektromágnes mágneses teret gerjeszt, ezzel maga felé húzva a fémlemezt, amely ráüt a csengőre. Ezután a fémlemez elemelkedik ezzel megszakad az áramkör és megszűnik a mágnesesség. A fémlemez visszatér a kiindulási helyére, így újra zárja az áramkört és kezdődik előlről a folyamat. Addig folytatódik ez a kör, amíg a kapcsoló zárt. Pope nyitott áramkört használt. Az előnye az volt, hogy az áramkör akkor zárt, amikor valaki kinyitotta az ajtót vagy ablakot, továbbá az akkumulátor nem merült, csak akkor, amikor riasztás volt. A rendszer eleme volt egy ki- és bekapcsoló megszakító is, amivel lehetett a rendszert aktiválni, illetve deaktiválni. 1858-ban eladta szabadalmát Edwin Holmes-nak. [8] A 14. ábrán látható az eredeti szabadalmi rajz.



14. ábra: Az eredeti szabadalom [8]

Edwin Holmes (1820-1901), mint később kiderült nagyon jó üzletet csinált azzal, hogy megvette Pope találmányát. Bostonból való elköltözése után New Yorkban megalapította a Holmes Burglar Alarm Telegraph nevű cégét, amely majdnem ötven éven keresztül virágzott. A kezdetekkor még nem volt sok megrendelése, mert az emberek nem szánták rá a pénzüket, nem ismerték annyira az elektromos áramot, illetve nem hittek a rendszer működésében. Tovább fejlesztett Pope rendszerét és már párhuzamos kapcsolásokat alkalmazott. Ezzel elérte azt, hogyha például a házban csak egy szoba áramköre záródik, akkor is szóljon a csengő. A következő nagy fejlesztése az volt, hogy a rendszerbe beszerelt egy úgynevezett annunciátort, ami azt tette lehetővé, hogy a segítségével meg lehetett mondani, hogy melyik helyiségből érkezett a riasztás. Ezen a szerkezeten annyi kar volt ahány szobában volt beszerelve riasztó. A karokon a szobák elnevezései szerepeltek. A nehézség az volt a működésében, hogy nem volt teljesen automatikus, így kellett hozzá valaki, aki tudta működtetni, például egy házmester. A riasztás lokalizálásához a karokat kellett forgatni. Amelyiknél megállt a csengő -zárult az áramkör-, abból a szobából érkezett a riasztás. Volt negatívuma is azonban a rendszernek, mégpedig az, ha a betörő tudta, hogy a házban van riasztó. A megállapításaik alapján az esetek többségében a betörők a pincén, az első vagy második emeleten törtek be a házakba. [8] A 15. ábra bemutatja, hogy hogyan nézett ki ez az új fejlesztés.



15. ábra: Annunciátor [8]

Az érzékelők fejlesztésével is foglalkozott. A működési alapelvet igazából Pope szabadalmaztatta, de Holmes ezt is tovább gondolta. A saját fejlesztését pontosított

kapcsolónak nevezte el. Az ajtókerethez erősített egy fémlemezt, ami egy szintben helyezkedett el az ajtóval. Amennyiben zárva volt az ajtó a fémlemez nyomást fejtett ki egy rúd segítségével egy rugóra, ami arra volt jó, hogy így a kapcsolókar megszakította a rugó kapcsolatát a lemezzel. Abban az esetben, ha az ajtó, ablak nyitva volt a rúd nem fejtett ki nyomást a rugóra, így az áramkör zárult és a csengő megszólalt. A felmerülő problémákon is gondolkozott, ezért később plusz kapcsolókat szerelt a rendszerbe, így az egyes házrészekben ki lehetett már kapcsolni a riasztót. A szabotázs védelmet is sikerült megerősítenie azzal, hogy külön áramkört adott a csengőnek, így az akkor is csengett, ha már a rendszer akkumulátora lemerült. Ezeket a rendszereket nem csak házakba szerelte be, hanem irodákba és bankokba is. A szabotázs védelmet a későbbiekben még tovább fejlesztette egy társával Henry C. Room-mal, A központosított rendszer is az ő nevéhez fűződik. Ötlete az volt, hogy a szekrény érzékelőit nem egy külső csengővel, hanem egy központi irodával köti össze, ahol az őrség a nap 24 órájában várta az esetleges jelzéseket. 1882-ben egy komplex rendszert alkotott, mivel létrehozott ugyanis egy vonulós élőerős szolgálatot. Ezzel kimondható, hogy ő alakította ki az első komplex vagyonvédelmi rendszert és működtette is. [8]

1.6. További fontos mérföldkövek

Bő 100 évet ugorva ismét az időben az 1970-es évektől elég gyorsan fejlődtek a biztonságtechnikai eszközök. 1973-ban a londoni metróban kiépítették az első kamerarendszert. Ezek a kamerák még fekete-fehér képet rögzítettek videokazettákra. Eleinte csak a megfigyelés volt a cél. Ekkor még nem lehetett beszélni automatizációkról, illetve távoli hozzáférésről sem. [17]

1984-ben a HID Corporation nevezetű cég bevezette az első mágneskártyás beléptető rendszerét. Nagy technológiai fejlődésnek számított, mivel így már nem kulcsokat kellett használni, illetve megalapozta az azonosítástechnikát. [17]

Axis NetEye 200 volt a neve az első IP-kamerának. Ez a kamera 1996-ban került bemutatásra az Axis Communications cég által. Ez a kamera tette lehetővé, hogy ma is tudunk ilyen kamerákat alkalmazni. Mivel IP alapú kamera, így nem volt már szükség a közvetlen kábeles összeköttetésre a rögzítővel. [17]

2008-ban került a piacra a Milestone XProtect nevezetű NVR rendszer. Ez a skálázható hálózati videómenedzsment szoftver tette lehetővé, hogy akár több száz, ezer IP-kamerát központosítottan, szoftver segítségével lehessen kezelni egyszerre. [17]

A mesterséges intelligencia felbukkanása hatással volt a biztonságtechnikai eszközökre is. A Hikvision 2016-ban előállt a DeepinView kameracsaláddal, amely mesterséges intelligencia segítségével képes volt az arcfelismeréstől kezdve a tömegszámlálásig. [17]

2023-ban a biztonságtechnikával foglalkozó cégek elkezdtek felhőalapú megfigyelőrendszereket kínálni, amelyek egyetlen platformon kezelnek különböző eszközöket úgy, hogy képesek előre riasztást generálni, ha a normális állapottól valamilyen eltérő dolgot tapasztalnak. Ezeket már távolról is lehet kezelni, így csökkenthetik egy telephely informatikai eszköz igényeit. [17]

2. KORSZERŰ BELÉPTETŐRENDSZEREK TÍPUSAI, MŰKÖDÉSI ELVEI

Ebben a fejezetben bemutatom, hogy a beléptetőrendszerek hogyan működnek, milyen azonosítási eljárások léteznek, valamint, hogy egy ilyen rendszer hogyan épül fel, milyen eszközök kellenek hozzá, például belépőkártya.

2.1. A beléptetőrendszerek alapjai és azonosítási módok

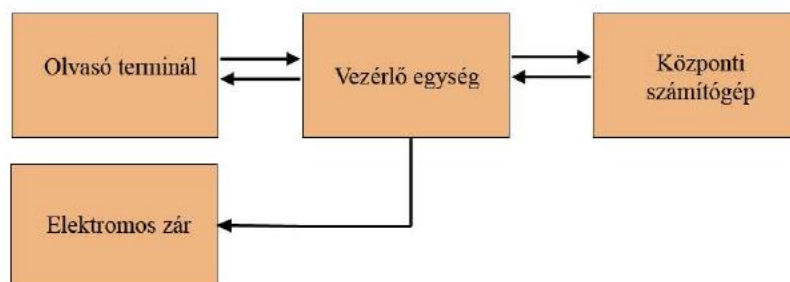
A fizikai biztonság egyik legfontosabb alappillérét a beléptetőrendszerek teszik ki. Ezekkel a rendszerekkel hatékonyan lehet szabályozni a hozzáférést például védett területekhez. A technológiai fejlődésnek köszönhetően mára eljutottunk a hálózatba kötött, intelligens és biometrikus rendszerekig. Kulcsfontosságú szempont lett az integrálhatóság, a megbízhatóság, illetve az azonosítás gyorsasága is. Napjainkban az eszközök lehetővé teszik a pontos, részletes naplózást, az egyszerű jogosultságkezelést, valamint, hogy ezeket távolról is el tudjuk érni. Ebben a fejezetben bemutatom a legelterjedtebb típusokat, ismertetem a működési elveiket, valamint rámutatok előnyeikre.

Elmondható, hogy ezeket a rendszereket alapvetően szabályzásra használjuk, viszont több más funkciót is képesek ellátni, mint például a munkaidő nyilvántartást, de adott esetben a gépjárművek beléptetését is tudják segíteni. Az utóbbi funkció a rendszámfelismeréssel lehetséges. Ahhoz, hogy teljes képet kapjunk fontos, hogy az elektronikus beléptetőrendszer fogalmát megismerjük. Egy olyan összetett elektromechanikai és informatikai rendszer, amely telepített beléptetőpontokkal szabályozza, hogy személyek, járművek mikor, honnan és merre mozoghatnak. A rendszer képes engedélyezni vagy adott esetben megtiltani a belépést a területre. Az eseményeket a rendszer rögzíti, illetve naplózni is tudja. [18]

A beléptetés során első körben azonosítjuk a személyt vagy járművet, amely be szeretne jutni a területre. Ezután a rendszer ellenőrzi, hogy van-e érvényes jogosultsága. Abban az esetben, ha igen, akkor a biztonságtechnikai eszköz áthaladást biztosít. A belépés után ez

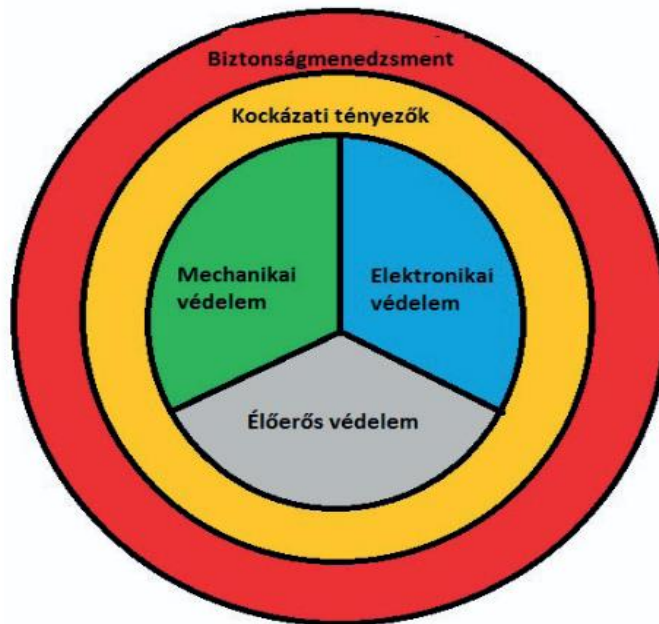
az eszköz egyből automatikusan visszazár. A rendszer folyamatosan naplózza az eseményeket. [18]

Ezen rendszerek négy fő részből állnak. Az első rész az olvasó, aminek a feladata az adatok eljuttatása a rendszer felé. A következő a vezérlő, ami arra szolgál, hogy az olvasótól érkező adatokat elemezze és eldöntse, hogy a személy jogosult-e a belépésre. A harmadik rész a felügyeleti rendszer (számítógép), ami ellenőrzi magát az egész egységet. Ennek segítségével lehet felprogramozni a vezérlőket, jogosultságokat kezelni, valamint az események rögzítéséért, visszakereséséért, listázásáért is ez felel. A negyedik rész pedig az áthaladást szabályozó eszközök, ami leegyszerűsítve megakadályozza az egyszerű be- és kilépést az adott objektumból. Ilyen eszközök például a forgóvillák, forgókapuk, gyorskapuk, elektromos zárok, s a többi. [18] A 16. ábra egy leegyszerűsített rajzon bemutatja, hogy hogyan épül fel egy ilyen rendszer.



16. ábra: Beléptetőrendszer felépítése [19]

Ahhoz, hogy ezek a rendszerek hol foglalnak helyet a vagyonvédelemben először a komplex vagyonvédelem elméleti modelljét kell megismernünk. [18] Ehhez a 17. ábra nyújt segítséget. Az ábrán jól látható, hogy három fő részre oszlik. Ez a három fő rész a mechanikai, elektronikai és élőerős védelem áll a középpontban. Az ábrán azonos arányban foglalnak helyet, mivel ezeket a meglévő környezet, sajátosság, szükséglet alakítja. A centrumon kívül található kör a kockázati tényezők, amik hatással vannak a fő elemekre. A három fő elem kialakítása, eloszlása attól függ, hogy a kockázati elemzéskor milyen eredmény keletkezett. Végül a biztonságmenedzsment veszi körbe az egész rendszert. Ez az egész rendszer vezető része, eleme. A biztonságmenedzsment felel a tervezésért, létrehozásért, működtetésért, valamint azért, hogy folyamatosan fejlessze az egész rendszert, hogy az megfelelően, hatékonyan tudjon működni. [20]



17. ábra: A biztonsági rendszer [20]

2.2. Beléptetőrendszerek csoportosítása

A beléptetőrendszereket két nagy csoportba tudjuk sorolni. Az első csoport az on-line működésű rendszerek, míg a második csoport az off-line működésű rendszerek.

On-line rendszerről akkor beszélünk, ha a rendszer folyamatos kapcsolatban áll a számítógéppel, így monitorozni tudjuk a különböző mozgási adatokat a beléptetőrendszer szoftverén keresztül. Ezek az adatok tartalmazzák például, hogy egy személy mikor, hol, milyen irányba közlekedett. Ehhez egy folyamatosan üzemben lévő számítógépre is szükség van, ami állandó kommunikációban van magával a beléptetőrendszerrel. A beléptetőrendszerek nagy része rendelkezik memóriával, így kapcsolat megszűnés esetén sem vesznek el az adatok, hanem eltárolódnak. [21]

Off-line rendszer esetén a folyamatos kapcsolat nem áll fenn, így az adatok nem is kerülnek rögzítésre a számítógépen. Belső memóriával ezek a beléptető is rendelkeznek. Az, hogy mennyi adat fér el rajtuk a memória nagyságától függ. A rendszer úgy működik, hogy amint eléri a maximális kapacitást a legrégebbi adatok felülíródnak. Ezek a típusú rendszerek egy-két belépési pontot tudnak csak kezelni. [21]

2.3. Azonosítási módok

Személyazonosítást aktív és passzív módszerekre szeparálhatjuk, továbbá a szükséges információk alapján három alapvető elvet különíthetünk el egymástól. Az első a tudás alapú azonosítás, ami azt jelenti, hogy a személy valami olyan dolgot tud, ami alapján ellenőrizni és azonosítani lehet. Ez lehet például egy PIN (Personal Identity Number-magyarul: Személyi Azonosító Szám) kód. A birtok alapú azonosításnál már egy eszköz is szükséges az azonosításhoz. Ezzel az eszközzel a személy rendelkezik, mint például egy belépőkártya. Az utolsó pedig a biometria alkalmazása. Ekkor a rendszer a személy valamelyik fizikai vagy biológiai sajátosságát ellenőrzi, mint például az ujjlenyomat, retina, s a többi. A szakirodalmi ajánlás, hogy ezek közül a módszerek közül legalább kettőt alkalmazni kell ahhoz, hogy a kellő védelem kialakuljon. Ezeket együttesen, de egymástól függetlenül kell alkalmazni. Ez a módszer könnyen negatív fordulatot vehet abban az esetben, ha például belépőkártyát, valamint PIN kódot kell használni egy helyiségbe való bejutáshoz, de a PIN kód rá van írva a kártyára. Ebben az esetben, ha a kártya egy illetéktelen személy kezébe kerül, akkor a beléptetőrendszer nem tudja ellátni megfelelően a funkcióját, ugyanis a személy könnyedén bejuthat a helyiségbe. [4]

Tudásalapú azonosítás előnye, hogy megbízhatónak mondható, a személynek nem kell semmilyen tárgyat magánál tartania, így az nem is veszhet el. A másik oldalon azonban a felhasználók többsége olyan jelszót, kódot ad meg, ami köthető valamilyen módon hozzá. Például születési év, édesanya neve. Mivel ezeket adott esetben sokszor meg kell adni, így nő az esélye annak is, hogy illetéktelenek tudomást vesznek róla. Használatuk során a biztonság szintje mindig csökken. Általában a jelszó kiválasztásához segítséget nyújt a felület, mivel támpontokat ad. Ezek lehetnek kikötések például az, hogy hány karakternek kell benne szerepelni, tartalmazzon kis- és nagybetűket, számot, s a többi. [1]

Birtok alapú azonosítás előnye, hogyha esetleg elveszik a belépőkártya, akkor a felhasználó erről tudja értesíteni a felelős személyeket a tényről, így ők azt a kártyát le tudják tiltani. Ezzel a módszerrel egy plusz biztonsági faktor lép életbe. Ami egyben az előnye az a hátránya is lehet, mivel egy jelszót nem tudunk elveszteni, de egy belépőkártyát igen. A belépőkártyáknak egyszerű és gyors a használata. A legfontosabb pont, hogy a belépőkártyákat ne lehessen másolni. Olyan kódolással kell ezeket ellátni, amiket nem lehet feltörni. Másolás szempontjából további három csoportra lehet osztani

ezeket. Az első csoportot a passzív eszközök teszik, mint például a vonalkód, vagy az olyan kártyák, amikről csak olvasni lehet az azonosításkor. Ezek elterjedésének oka, hogy olcsók és egyszerűen használhatók. A következő csoport az írható-olvasható aktív eszközök. Ezek már nehezebben klónozhatók, mivel komplex műveleteket is végre tudnak hajtani. Ilyen például a chip kártya. A harmadik csoportot az intelligens eszközök teszik ki, amik már többfaktoros kriptográfiai műveletekre képesek. Példaként a smartcard-ok említhetők, de ezeknek is csak a bizonyos típusai. Titkos kulcsot tartalmaznak, amit soha nem adnak ki magukból csak rejtjelzéshez. Természetesen ez a legbiztonságosabb a három csoport közül, mivel duplikálásuk kifejezetten nehéz. [1]

A személy azonosítás legmegbízhatóbb módszere a biometrikus azonosítás. Ehhez a módszerhez egy a gépek által is könnyen kezelhető fizikai vagy biológiai jellemző szükséges. Ez lehet ujjlenyomat, kézlenyomat, arc, s a többi. Itt már ténylegesen a személy azonosítása történik meg, és nem egy nála lévő eszközt, vagy az ő fejében élő jelszót azonosítunk. Ez a tulajdonság nem ellopható, nem másolható. Arra is van lehetőség, hogy a rendszer csendes riasztást generáljon, abban az esetben, ha a személy kényszerítve van az azonosításra. Ez úgy történhet meg, hogy például a mutató ujj helyett a gyűrűs ujját rakja rá az ujjlenyomat olvasóra. A hátrányok közé az sorolható, hogy az olcsóbb technikák megtéveszthetőek, viszont a minőségi termékek pedig nagyon drágák. Továbbá a fizikai érintkezés során a higiénia megkérdőjelezhető, valamint vannak módszerek, amik fogyatékkal rendelkező személyek esetében nem is használhatóak. A biometrikus jellemzőink az idő előrehaladtával változhatnak, valamint a sérülések is nehezítő körülménynek számítanak. A hibatűrés mértéke is egy sarkalatos pont. A negatívumok ellenére kijelenthető, hogy ez a legbiztonságosabb módszer egy személy azonosítására. [1]

A beléptetőrendszerek az azonosításon kívül a munkaidő adatok rögzítésére is alkalmasak. Ezt a módszert a leggyakrabban nagy vállalatoknál, gyáraknál, és egyéb nagy foglalkoztatási létszámú munkahelyeknél alkalmazzák. A rögzítés a munkaidő nyilvántartó terminálokön keresztül történik. Ezekhez kártyaolvasókat alkalmazunk általában, illetve a belépőkártyák szükségesek hozzá. A kártyát az olvasóhoz érintve rögzülnek a munkavállalók mozgási adatait, így egy nyilvántartás keletkezik arról, hogy mikor értek be, illetve mikor távoztak a munkából. Ezekből az adatokból riportok

készíthetők, amik a munkaügynek szükségesek lehetnek elszámolásokkor, túlórák kifizetésekor, s a többi. Automatizáció is beiktatható a rendszerbe, így a bérszámfejtést már nem manuálisan kell végrehajtani, hanem a bérszámfejtő szoftver kapcsolatban van a munkaidő nyilvántartóval. [19]

2.4. Belépőkártyák típusai

Vonalkódos kártyák esetén a vonalkód egy műanyag vagy papír felületen helyezkedik el. Az olvasó fénysugarakat bocsát ki, ezzel olvasva le a vonalkódot. Így jön létre az azonosítás. Előállítási költségük alacsony, de egyszerűen másolhatók, valamint a vonalkód könnyen lekophat. Általában belépőjegyeken használják ezeket, mivel itt nem fontos annyira a másolhatóság. Rendszerint egyszeri belépésre használják ezeket. [19]

A mágnesescíkos kártyákat úgy kell elképzelni, mint egy bankkártyát. A kártyák hátoldalán található a mágnesescík, ami az azonosítást teszi lehetővé. Nagyon elterjedt típus volt, de biztonság szempontjából már elavultnak számít, mert könnyen másolhatók. Előállításuk a vonalkódos kártyákhoz hasonlóan alacsony költségekkel jár. Használat során a kártya kopik, ezért viszonylag sűrűn cserélni kell ezeket. A mágnesesség és a koszolódás tönkre tudja tenni ezeket. [19]

Az infrakártyák érdekes módon működnek, ugyanis a kártya belsejében egy lyukkártyaszerű lapot speciális réteggel vonnak be. Ez a réteg csak az infravörös fényt engedi át. Olcsó, de manapság már nem használják. [19]

A passzív proximity (közelítő) kártyák a világon az egyik legelterjedtebb és legnépszerűbb típus. El lehetnek látva fix kódolással, de lehetnek egyszer vagy többször programozhatók is. A kártyák belsejében egy antenna és egy integrált áramkör található. Az antenna az egész kártyán körbe fut. A rendszer működtetéséhez elég a kártyát az olvasóhoz közelíteni, nem is kell hozzáérinteni. Ekkor az olvasó rádiófrekvenciás jelek segítségével energiát továbbít a kártyának. Ezt az energiát felhasználva az áramkör aktiválódik, majd ugyanúgy rádiójelek segítségével visszaküldi az olvasónak a benne található azonosításhoz szükséges információkat. A kártya használata nagyon egyszerű, nem kopik, nem érzékeny a mágnesességre. Olvasási távolság 10-80 centiméter is lehet. Általában sok munkavállalóval rendelkező helyeken használják ezt a típust. [19]

Aktív proximity (közelítő) kártyák nagyon hasonlóan működnek a passzív társaikhoz hasonlóan, de saját beépített energiaforrást tartalmaznak. Ennél az olvasó is kódolt rádiójelet ad ki magából, illetve a kártya is ilyen módon válaszol vissza. Ezt általában olyan helyeken használják, ahol az olvasási távolságnak nagyobbnak kell lenni, akár több méternek is. Gépjármű beléptetésnél nagyon hasznos. [19]

Chipkártyák esetén a kártya egy chipet tartalmaz. Smart változataik esetén már egy mikropocesszor is van bennük. Ezek több információ tárolására képesek, valamint az rajtuk lévő adatok bővíthetők, törölhetők. Létezik érintéses és érintésnélküli típusa is. Az érintésnélküli verzió a chipen kívül egy antennát is tartalmaz, így ez is a proximity kártyához hasonlóan rádiófrekvenciát kibocsátva tud működni. Chipkártyákat a legtöbb esetben a bankok, vállalatok használják. [19] A 18. ábrán egy Legic prime kártya látható, illetve, hogy hogyan fut benne az antenna, hogyan helyezkedik el benne a chip. Ennek a kártyának is két változata van. Az egyik, aminek a pontos neve Legic prime MIM256, a másik pedig a Legic prime MIM1024. A számok azt jelölik, hogy hány bites a memóriájuk. Természetesen ez a kártya már érintésnélküli típus, ami 13,56 MHz-en kommunikál. [22]



18. ábra: Legic prime kártya [23]

A kártyákat biztonsági szintjük szerint négy csoportba lehet sorolni. Az első csoport a nyílt biztonságú. Ezek egyszerű fix kóddal vannak ellátva, adattartalmuk pedig olvasható és értelmezhető. Másolásuk a mai fejlettséget figyelembe véve egyszerű. A második

csoport a kódolt. Fejlettebb technika, mint az előbbi annyi eltéréssel, hogy ez már nem értelmezhető. A következő az adathozzáférés védett. Ezek már jelszóval elérhetők, önmagukban másolhatatlanok, viszont visszafejthetők. Az utolsó a titkosított, ami a legbiztonságosabbnak minősül manapság. [24]

2.5. Példák beléptetőrendszer eszközökre

Rendszerstruktúra alapján megkülönböztetünk online és offline rendszereket. Online rendszerről akkor beszélünk, ha a kapcsolat folyamatos a felügyeleti rendszerrel. Offline pedig, amikor nincsen folyamatos kapcsolat. Ebben az esetben például a belépőkártyát az olvasóhoz tartva egy kódoló segítségével tudjuk felprogramozni. [24]

Kártyaolvasóként egy Lectus Select nevű olvasót választottam. Ez az olvasó képes Legic prime, Legic advant, Mifare Classic és Mifare Desfire EV1 és EV3 kártyák olvasására. A Legic prime kártyát ez az olvasó például körülbelül 6,5 centiméterről képes olvasni. Ezzel az előbb felsorolt kártyák közül ezt tudja a legtávolabbról érzékelni. Ennek az eszköznek van egy olyan variációja is, aminek az előlapján PIN kód beírására van lehetőség. A 19. ábrán egy ilyen olvasó látható. Az eszköz ára a roteiv-shop.de oldalon 2025.11.20-án 389 €, ami 148 622 Ft-nak felel meg a napi árfolyam alapján.



19. ábra: Lectus select olvasó [saját kép]

Vezérlők közül a Bosch AMC2 elnevezésű eszközt prezentálom. Ez a controller egyszerre maximum 4 darab olvasót tud kezelni. A Power Biztonságtechnika oldalán jelenleg

elérhető listaár 2025.11.20-án az bruttó 602 425 Ft. A tápellátáshoz 10-30 V szükséges. A 20. ábrán egy ilyen vezérlő látható.



20. ábra: Bosch AMC2 vezérlő [saját kép]

Áthaladást szabályozó eszköz lehet például forgóvilla, gyorskapu, és még sok egyéb eszköz. Működésük szempontjából ezek az áthaladást szabályozó eszközök lehetnek vagyonvédelmi típusúak, amit NC-nek hívnak. Az NC kiírva Normally Closed, ami magyarul alaphelyzetben zártat jelent, de szokták fail-secure-nak is, ami szintén ezt jelenti. A másik típus az életvédelmi típusúak, amit a szaknyelvben NO-nak hívnak. Az NO kiírva Normally Open, ami magyarul alaphelyzetben nyitottat jelent, ezt pedig fail-safe-nek is hívni. Életvédelmi típusról akkor beszélhetünk, ha tápkimaradás esetén az eszköz kinyit, így biztosítva a szabad menekülési utat. Vagyonvédelmi típus jellemzője pedig, hogy tápkimaradás esetén az eszköz bezár. [24] Példaként én a Dormakaba által gyártott Argus V60 elnevezésű gyorskaput választottam, ami a 2. ábrán látható. Ebben az az érdekesség, hogy a legkisebb gyorskapu a piacon a maga 240x180 mm-es ház méretével. [25] A gyártó oldalán, illetve az interneten nem található ár az eszközhöz.



21. ábra: Dormakaba Argus V60 gyorskapu [26]

2.6. A holnap belépőkártyája

Manapság az ember a telefonja nélkül az utcára sem lép ki. Így gondolkoznak azok a fejlesztők is, akik azon dolgoznak, hogy hogyan lehet azt megvalósítani, hogy a telefonunk egyben a belépőkártyánk is legyen. Személyes véleményem szerint a belépőkártyák használata lassan a múlté lesz.

Részt vettem a 2025-ös SecuriForum rendezvényen, ahol Papp Márton az az Assa Abloy színeiben tartott Mobil, mint belépőkártya című előadásában bemutatta, hogy hogyan lehet a telefonunk a belépőkártyánk az Inceso Pro Mobile Access rendszer használatával. Az egyik dián volt egy diagram, ami az azonosítók növekedési ütemét mutatta be a következő 5 évben. A fizikai kártyák mindössze 1,8%-ot értek el, míg a mobil azonosítók 32,5%-ot. Megjegyzésben le volt írva, hogy egyetlen más eszköz sem fog ilyen növekedési ütemet reprezentálni a beléptetőrendszerek területén. Az új generációk új igényeket teremtenek, így a belépőkártyák piaca nagyon le fog csökkenni. Nem csak egyedül ez lesz az oka, hanem a fenntarthatóság is. Az előadásban az egyik dia arról szólt, hogy a dolgozók 17%-a elhagyja a belépőkártyát, míg az irodaházakban az új kártyák cseréje 20%. A telefon elhagyások száma ennél valószínűleg egy kisebb szám. Számos kérdés felmerülhet a telefonon lévő kártyákkal kapcsolatban. Az előadás ezekre is választ adott. A mobil biztonságosabb, mint a fizikai kártya, a telefonos alkalmazásban is megjeleníthető, az RFID (Radio Frequency Identification, magyarul rádiófrekvenciás azonosítás) nélküli fizikai azonosító olcsóbb. Továbbá arra is választ adott, hogy mi

történik akkor, ha elveszik a telefon. A különböző lokátor alkalmazások lehetővé teszik a telefon megtalálását, illetve ezeket is, mint a kártyát távolról le lehet tiltani. A legfontosabb mozgató erők a kártyáról való áttérésre az az, hogy a telefon mindig a felhasználónál van, elvileg a legbiztonságosabb azonosító. Ebben a pontban személy szerint nem vagyok annyira biztos. A következő mozgatóerők a digitális átalakulás, a funkciókkal kapcsolatos növekvő elvárás és természetesen a fenntarthatósági szempont. Összevetette a Bluetooth-t és az NFC (Near Field Communication, magyarul közeli rádiófrekvenciás kommunikáció) működését is, hogy melyiket éri meg használni ilyen rendszernél. Az NFC annyival tud többet, hogy gyorsabb a küldési sebesség, viszont a Bluetooth pedig távolabbról képes működni. A virtuális kártyát többféle applikáció segítségével tudjuk használni, de véleményem szerint az Apple, valamint a Google saját tárcájához való rendelés a legjobb módszer. Az Apple például lehetővé teszi azt is, hogy alacsony töltöttség esetén is 5 órán keresztül használható a belépőkártya az új modellek esetén. A rendszer úgy épül fel, hogy kell egy HID Origo hozzáférés, egy mobil azonosító, egy HID Signo olvasó, valamint Aperio zárok. [27]

Számos kérdés felmerült bennem az előadás alatt. Az egyik ilyen például az volt, hogy egy nagyvállalat esetében a munkavállalókat hogyan lehet megkülönböztetni a vendégektől, ha olyan fejlettségre jut ez a rendszer, hogy a kártyákra már nem lesz szükség. A munkahelyemen még ez úgy történik meg, hogy többféle színű nyakpánt van a kártyákhoz és mást kap a munkavállaló és mást a vendég. A következő az volt, hogy a vendégek telefonjára, hogy fog felkerülni a szoftver. További érdekes kérdéseket vet fel ez az újdonság, amikre valószínűleg a gyakorlatban fogjuk megkapni a választ.

2.7. Tervezés és kivitelezés

A tervezés, illetve a kivitelezés során számos pont van, amiket figyelembe kell venni. Az első lépés mindig a kockázatelemzés, valamint az igények felmérése. Ennél a pontnál tisztázni kell, hogy pontosan mit kell védeni, milyen fenyegetésektől kell védeni, mekkora költségkeret áll rendelkezésre a projektre, valamint, hogy milyen specifikus igények merülnek fel. Ezek alapján lehet csak meghatározni, hogy milyen védelmi szintű rendszerre van szükség, valamint, hogy milyen eszközökkel. [18]

Fontos szempont, hogy a rendszer megkerülhetetlen legyen, valamint ne lehessen kijátszani. A megkerülhetetlenségkor úgy jöhet létre, ha minden belépési pontot védünk. A kijátszhatatlanságnál pedig figyelni kell a személyek egyedi azonosítására. [18]

Az életvédelmi előírások betartása mindig kötelező. A menekülési útvonalakat szabadon kell tartani. Az áthaladást szabályozó eszközöknek megfelelő átbocsátóképességének kell lennie, valamint, hogy senki ne rekedhessen benn egy zsiliprendszerben. [18]

A következő pont az empátia. A mindennapi közlekedést ne akadályozza a rendszer indokolatlanul. Nem a cégnél dolgozó alvállalkozókra, vendégekre, sőt még például a futárookra is gondolni kell. Nekik is biztonságos és kontrollált belépést kell biztosítani. A kivitelezéshez nagyon fontos a részletes dokumentáció. [18]

A telepítés során figyelni kell arra, hogy a vezérlő csak védett téren belül helyezkedhet el. A kábelezéskor is figyelni kell erre a pontra, vagy megfelelő fizikai védelemmel legyen ellátva. Az olvasókat megfelelő magasságba kell felszerelni, ügyelve az esetleges átolvasásra is. [18]

Végül megvalósulási dokumentációt kell biztosítani az átadáshoz, illetve a későbbi karbantartáshoz. [18]

3. ZÁRRENDSZEREK TÍPUSAI ÉS TECHNOLÓGIAI FEJLŐDÉSE

Ebben a fejezetben bemutatom a különböző zárat, zárszerkezetek. Az első fejezetben bemutattam, hogy a régmúltban mekkora fejlődésen estek át a zárok. A következő fejlődési szakasz a 19. században következett be, amikor megjelentek a cylinderzárak. Ezek használata már sokkal biztonságosabb és könnyebb volt. A 20. században megjelentek a különböző elektromos és biometrikus zárok. Utóbbiak működtetéséhez ujjlenyomat szükséges vagy egyéb biometrikus adat. Jelenleg a digitális zárok korszakát éljük, melyeket telefonos applikáció segítségével tudunk működtetni. [28]

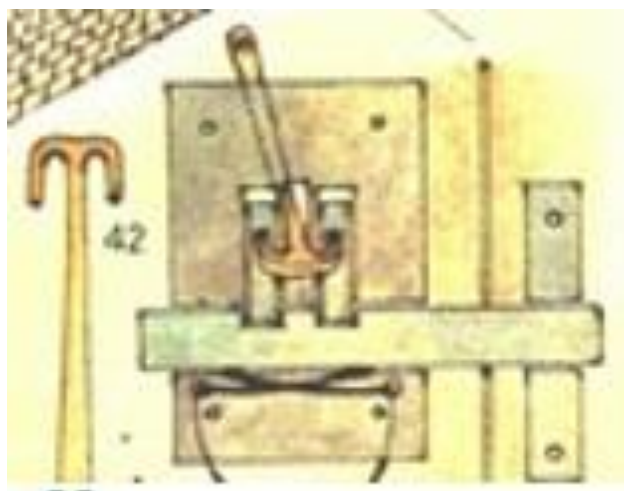
3.1. Zárok technológiai fejlődése

Az ókorban az egyiptomiak magas fejlettségi szintje lehetővé tette, hogy olyan zárat hozzanak létre, amik működési elve nagyban megegyezett a ma is használt zárákéval. Az akkori zárat is kulcsokkal nyitották már. Ezeket nem úgy kell elképzelni, mint a mai kulcsokat. Fából készültek és akár hatvan centiméteresek is lehettek. A kulcs szerepe a csapok mozgatása volt. A csapok a gravitációnak köszönhetően becsúsztak a retesznyelven kialakított lyukakba, így biztosították a zárast. Abban az esetben, ha a kulcs megfelelő volt a zárba, akkor pontosan a csapokat emelte meg, így a retesznyelv kihúzhatóvá vált. [29] A zárok feltalálása új mesterséget hozott létre, ugyanis ekkor jelentek meg a zárkovácsok. A 22. ábra bemutatja, hogy hogyan is nézhettek ki az egyiptomiak által használt zárok.



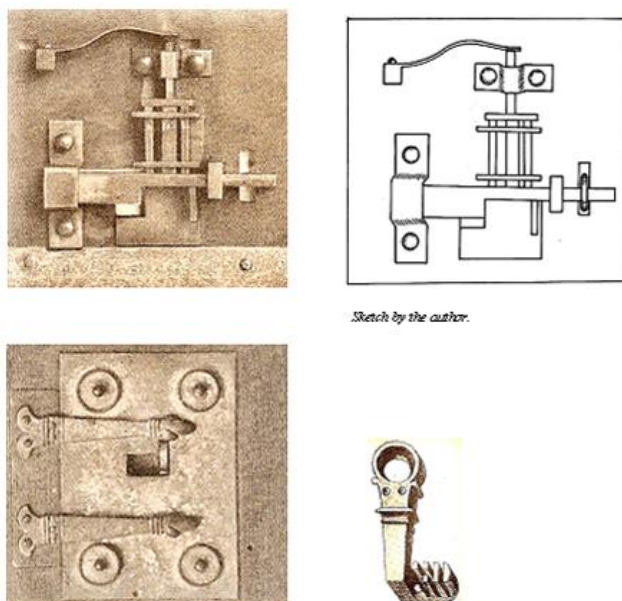
22. ábra: Egyiptomi zár [30]

Az ókori görögök az ajtó belső felén kereszttrudat alkalmaztak, amire egy emelhető elemet helyeztek. Ez az elem a kereszttrúdba kialakított mélyedésbe süllyedt bele, így megakadályozva a rúd elmozdíthatóságát. A biztosító elemben kettő darab lyuk volt található. A kulcsot az ajtón lévő résbe függőleges helyzetbe kellett behelyezni majd 90 fokkal elfordítva az előbb említett biztosító elembe fűrt két lyukba kellett betálcálni. Amint ez megtörtént a kulccsal ki kellett emelni a biztosító elemet a kereszttrúdból. Ezután a művelet után a kereszttrúd kihúzható volt, így az ajtót ki lehetett nyitni. [8] A 23. ábrán látható az általuk használt zár.



23. ábra: Ókori görög záruk [8]

Az ókori Rómában nagyon elterjedtek voltak a különböző záruk. Ezeket általában több fogú tollas kulcsok nyitották már, amiket státusz szimbólumként a ruházatukon kívül hordtak. Annyira gyorsan terjedt az alkalmazásuk, hogy rövid időn belül az összes házon megtalálhatóak voltak, így külön iparágga nőtte ki magát a zárszerelés. Annyira fejlett lett a technológia, hogy egy egész évezreden keresztül nem kellett további fejlesztéseket eszközölni. A kutatások szerint tipikus római zár a fém tolókulcsos zár. Az ilyen záruk kulcsainak már ténylegesen kulcs formájuk volt. A Római Birodalomban többféle kulcsmechanizmusok léteztek már, ezért ezeket a kutatók különböző rendszerek szerint csoportosították. Három típust különböztettek meg egymástól, amik a tolókulcsos záruk, rugós záruk, illetve a forduló kulcsos záruk. [31] [32] A 24. ábrán látható két római zár, illetve egy kulcs, ami gyűrű formájú. Ez nem véletlen, ugyanis akkoriban a nők a kulcsot az ujjukra húzták vagy a hajcsatjukhoz rögzítették. [33]



24. ábra: Ókori római záruk és egy gyűrűs kulcs [34]

A középkor nagyon nehezen indult a technológiai fejlődést figyelembe véve, viszont a záruk ebben a korban is tovább tudtak fejlődni. A zárkovácsok elkezdtek egyre bonyolultabb mechanizmusokat készíteni, így a biztonsági szint is elkezdett növekedni. A díszes záruk elterjedtek, így a gazdagabbak ezzel is ki tudták mutatni anyagi jólétüket. Ezek a záruk általában robosztus fém darabok voltak, amik magasabb védelmet biztosítottak. Azt, hogy a kulcsok már nem csak a feladatukat kellett ellátniuk, hanem szépen is kellett kinézniük, a reneszánsz hozta el. Használatuk annyira elterjedt, hogy külön ipar jött létre a záruk készítésére. [28]

A 1700-as évek végén Robert Barron által a technika elért egy újabb fordulóponthoz, ugyanis szabadalmaztatta a reteszzárat. Ezt követően nem sokkal 1784-ben Joseph Bramah pedig megalkotta az első biztonsági zárat, ami már a mostani kor zárjainak is megfelelt volna. A cserélhető kulcsos kombinációs záruk James Sargent nevéhez köthetőek, aki 1873-ban megalkotta az időretesz zárat is. [35]

Fontos megemlíteni ennél a fejezetnél Leonard Denner nevét, aki 1550-ben nem egy új zárat talált fel, hanem azt, hogy egy zárat hogyan lehet feltörni. A zártörője lehetővé tette a zajmentes ajtónyitást. A történelemben ez volt az a pont, amikor a zárszereléssel foglalkozók elkezdtek versengeni a zártörésekkel foglalkozókkal.

A 20. században jelentek meg az első elektromos és biometrikus záruk, amik feladták a leckét az ajtótoróknak, ugyanis ezeket feltörni már nehéz volt. Ez azt jelentette, hogy az emberek jóval nagyobb biztonságot élvezhettek. [35]

Manapság a trendek azt mutatják, hogy a digitalizáció a jövő, ugyanis elterjedtek a digitális záruk, amiket távolról akár telefon segítségével is lehet működtetni fizikai kulcs nélkül. A fenntarthatóság egy meghatározó pont a mai világban, így új anyagok is megjelentek a záruk világában. Az innovációkra az emberek figyelme kiéleződött. Véleményem szerint az elkövetkező években rohamosan fejlődni fog a technika ebben a szektorban is. Elképzelhetőnek tartom, hogy a mesterséges intelligencia még nagyobb szerephez jut. [28]

3.2. Zárak fogalma, típusai

A záruk olyan szerkezetek, amelyeket ajtókra, ablakokra, szekrényekre, vagy akár táskákra helyeznek el, ezzel megakadályozva az illetéktelen hozzáférést az objektumhoz, illetve tárgyakhoz. [36]

Az első típus a kulcsos zár. Ezek nyitása, illetve zárás úgy történik, hogy a kulcsot közvetlenül a zárba helyezzük. Két féle típus létezik belőlük. Az egynyelvű és a kéttollú. Biztonsági szintjük alacsonynak mondható még akkor is, ha a kéttollú típust nehezebb feltörni. [28]

Cilinderes zárról, vagy másnéven hengerzárakról akkor beszélünk, ha a zárnyelvet egy cylinderbetét működteti. Ezek már jóval biztonságosabbak, mint a kulcsos záruk. Maga a cylinderbetét cserélhető, így bármikor ki tudjuk azt cserélni, ha esetleg elhagytuk a kulcsot. Sok típusa létezik, ugyanis a különböző védelmi szempontok alapján több csoportba lehet őket sorolni. A fúrás védett hengerzárbetétek tulajdonsága, hogy a belső alkatrészek nagyon kemény anyagból készülnek, így ezek felfúrása szinte lehetetlen, de abban az esetben, ha sikerülne is nagyon sok idő kell hozzá. A sima záraknál a fúrás hatására a belső alkatrészek ronccsolódnak, így kinyithatóvá válik az ajtó. Finom nyitás ellen védett hengerzárbetét is létezik. Ezek különleges csapokkal vannak ellátva, amik különböző irányokban helyezkednek el, valamint teleszkopikusan reteszelve. Így akadályozzák meg a filmekből már jól ismert betörési stílust, amit más néven

zárférsülésnek is hívják. Ehhez a betörő nem kulcsot használ, nem is töri el a zárat, hanem egy speciális szerszámmal nyitják azt ki. Magkihúzás ellen védett betétről akkor beszélünk, ha a zárbetét kemény acélsapokkal és erősített zégergyűrűkkel van szerelve. Így hiába akasztanak erős csavart a kulcsnyílásba a betétet nem lehet kiszakítani. Savazás ellen védett betét is létezik, mivel létezhet olyan módszer, amikor a zárbetétbe savat öntenek, így a maró anyag tönkreteszi a belsejét. Nagyon kérdéses ez a módszer, de a csapokat feszítő rugók olyan anyagból készülnek, amik ellenállnak az ilyen anyagoknak, valamint a belső szerkezetük is úgy van kifejlesztve, hogy a sav ne juthasson el addig. Közkedvelt módszer, talán a legelterjedtebb betörési technika a hengerzártörés. A záruk két félből tevődnek össze, így biztosítva, hogy az ajtó mindkét irányból nyitható legyen, így a leggyengébb pontja a zárnak a közepe, mivel itt helyezkedik el a rotor, reteszvivő. Ezen a részen ezért a gyártók acélhíddal erősítik meg a szerkezetet, így az nem tud eltörni ezen a ponton. [28] [37] A 25. ábrán a Dormakaba által gyártott E-SP standrad betét látható.



25. ábra: Dormakaba standard hengerzárbetét [38]

A legközkedveltebb zártípus, amit az ajtó élébe kell beszerezni az a bevéső zár. Egy pontú záródása miatt nem számít biztonságosnak, ezért leginkább belső ajtónál, illetve régebbi típusú ajtónál találkozhatunk vele. [28]

Bejárati ajtók esetében nagyon gyakran használják a több pontos zárat. Ezek az ajtó teljes hosszán záródnak, így magas biztonsági szintet nyújtanak. A működtetésük többnyire a kilincs felhúzásával zajlik. [28]

Új lakások ajtajainál gyakran találkozhatunk biztonsági záakkal. Annyiból különböznek, hogy ezek már le, illetve fel irányba is záródnak. A záródáskor az ajtó tetején, illetve alján acéltüske emelkedik ki, süllyed le. [28]

Elektromos záraknak nevezzük azokat a zárat, amelyek elektronikus vezérléssel működnek. Szerelése az ajtó tokba süllyesztve történik az ajtózárral szembe. Ezeket már távolról is lehet vezérleni. Az elektromos záraknak számos típusa ismert. Vannak a normál, illetve fordított működésű zárok. Normál működésűről akkor beszélünk, ha feszültség hatására nyit. Abban az esetben, ha nincs feszültség, akkor zárt állapotban marad. Fordított működésű zár esetén feszültségmentes állapotban nyitható az ajtó. Impulzus üzemű zárnál a zár nyit egy pillanatnyi feszültségre, majd vissza is zár egyből, amennyiben nem kap további áramot. A zárnyelv érzékelő mágneszár érdekessége, hogy a beépített érzékelő visszajelzést ad a beléptetőrendszernek az állapotáról. Ezt úgy kell elképzelni, hogy a beléptetőrendszeren keresztül láthatjuk, hogy az az ajtó nyitott, vagy zárt állapotban van. A retesszel kiakasztható zár is egy elektromos zár típus, de egy retesz segítségével manuálisan tudjuk állítani a zár állapotát. Zárt állapotban a zárat a belépőrendszer segítségével tudjuk működtetni, viszont, ha a reteszt átállítjuk nyitott állapotba, akkor az ajtó mindaddig nyitva marad míg azt vissza nem állítjuk manuálisan. Szakítószilárdságot tekintve régen nem voltak annyira erősek, ugyanis körülbelül csak 50 kilogrammú erőnek tudtak ellenállni. A ma használatban lévők akár az 1 tonnányi erőnek is ellen tudnak állni. Feszültségparamétereket tekintve lehetnek 6 V-tól egészen 24 V-tal működő típusok is. Van olyan, ami AC-val (váltóáram), DC-vel (egyenáram) működik, de létezik olyan is, ami mindkettővel tud. [39] [40] A 26. ábrán egy normál működésű Dorcas által gyártott elektromos zár látható.



26. ábra: Dorcas-41-2-NF elektromos zár [41]

Mágneses zárat leggyakrabban biztonsági rendszerek kiegészítéseként használják. Működésük egy erős mágnes segítségével történik. [28]

A következő típus a kártyás zár. Ezekkel a leggyakrabban szállodákban, irodaházakban találkozhatunk. Belépőkártya használatával működnek. Biztonság szempontjából fontos tulajdonságokkal rendelkeznek, ugyanis ezeknél a zárnál nyomon lehet követni a ki- és belépéseket, illetve a hozzáféréseket is lehet szabályozni. [28]

Az ujjlenyomat-olvasós zárok a legbiztonságosabb zárok közé tartoznak. Működésükhöz biometrikus adatra van szükség. Magasabb biztonsági szintet nyújtanak, ugyanis csak az ujjlenyomat felismerése után nyithatók. Emiatt a funkció miatt használják ezeket olyan objektumoknál, amelyek ezt a magas fokú biztonságot igénylik. [28]

Kombinációs zárok esetén fontos, a zár típusa, a biztonsági igény, a kényelmi szempont, valamint az ajtó típusa a megfelelő zár kiválasztásához. Ezek működtetéséhez a megfelelő számkombinációra van szükség. Leggyakrabban széfekben fordulnak elő. [28]

Léteznek hevederzárak is. Ezeket már az ajtóra kell felszerelni utólag. Kétoldali zárast biztosítanak, azzal, hogy a reteszek a falba zárnak. Biztonságosabb megoldást nyújtanak ezzel egy sima zárnál, ugyanis a zárnyelvek sokkal mélyebben és nagyobb

keresztmetszetben zárnak. Ez egy olcsóbb megoldás, mintha biztonsági ajtót szereltetnénk be. Két fajtája van az egyik a függőleges a másik pedig a vízszintes hevederzár. Ez attól függ, hogy a zár milyen pozícióban helyezkedik el az ajtón. [40]

A végére a mai kor technikájának megfelelő okos zárat hagytam. Ezek a zárok nagyon elterjedtek az utóbbi időben. Azért ez lett a nevük, mert szenzorok, valamint különböző elektronikák folyamatosan figyelik a zár állapotát, így folyamatos kapcsolatot teremtenek egy vezérlő egységgel vagy mobilos applikációval. Ezáltal az ingatlan tulajdonosa akárhonnán meg tudja nézni, hogy a zár milyen állapotban van. Technológiai szempontból többfélék lehetnek, de a legelterjedtebbek a Bluetooth, Wi-Fi kapcsolatot használók. A Bluetooth-t használók érzékelik, ha a telefonunk a közelben van, majd leellenőrzik a jogosultságot. A Wi-Fi-s verzióknál a zár az otthoni hálózatra van felcsatlakoztatva, így ezek távolról is irányíthatók, megfigyelhetők. Vannak fejlesztők, akik olyan megoldásokat találtak ki, amik összefogják az okosotthon elemeit, így a zárat is. Mint mindennek ezeknek az eszközöknek is megvannak az előnyeik és a hátrányaik is. Az előnyökhöz lehet sorolni a kényelmi szempontot, ami lehet az, hogy távolról vezérelhetjük, vagy nem kell a különböző kulcsokra figyelnünk. Továbbá naplózzák az eseményeket, beépített risztóval rendelkeznek egyes fajták és azonnal értesítést küldenek a tulajdonosnak, ha valami történt. Okosotthon rendszerekbe könnyen beilleszthetők. A hátrányoknál felmerülnek a kiberbiztonsági kockázatok, mivel hálózatra csatlakoznak. Mint tudjuk tökéletes védelem nincs, de a fejlesztők folyamatosan frissítik őket, hogy a kockázat minél alacsonyabb legyen. A második hátrány pedig az ár. Alapból egy ilyen zár sokkal drágább, mint a sima változatok, illetve azzal is számolni kell, hogy esetlegesen a szoftver frissítésekért, karbantartásért plusz pénzt kell kifizetni. A digitálistekológiától való függés pszichés terhet jelenthetnek az ember számára. [42] A 27. ábrán egy okos zár látható.

Számos kutatás mutatott rá arra, hogy ez egy egyre növekvő piac és 10 éven belül hatalmas ugrás következhet be az eladások számában. Véleményem szerint is ez a jövő, ugyanis így már nem kell attól tartanunk, hogy elhagyjuk a kulcsunkat és nem tudunk bejutni a saját otthonunkba. Ezek a zárok több lehetőséget is biztosítanak arra, hogy mindenképpen ki tudjuk nyitni az ajtót. Telefonnal, PIN kóddal, vagy valamilyen biometrikus adatunk segítségével, akár távolról is.



27. ábra: HiSec okos zár [43]

Manapság az emberek életében egyre inkább fontos a kényelem, valamint, hogy minél biztonságosabb eszközök vegyék őket körül. Biztonság és kényelem szempontjából a legmegfelelőbb zárok az elektromos, illetve biometrikus típusok, de az egyszerűbb zárok alkalmazásával is magas szintet lehet elérni a biztonság terén, ehhez viszont az kell, hogy körültekintően kell kiválasztani a számunkra legalkalmasabb zárat, illetve így kell eljárni a telepítés során is. [28]

3.3. Zárbetétek biztonsági szintjei

Mint már tudjuk nem minden zár biztosítja ugyanazt a biztonsági szintet. Vannak egyszerűbb zárok és vannak olyanok, amiket tegyük fel bankok biztonságához használnak. Azt, hogy mennyire biztonságos egy zár az dönti el, hogy milyen anyagból készült, milyen a belső szerkezete, és a többi. Egy 2022-es kutatás szerint, amit a Lock Security Journal készített, a betörők 70%-ban a gyengébb zárbetéttel rendelkező ajtókat választják. [44]

Három biztonsági szint létezik. Az első az alap, a második a középszintű, a harmadik pedig a magas. Az alap biztonsági szintnél nem jellemző a fűrés, vagy törés elleni védelem. Az ebbe a kategóriába tartozó betéteket inkább belső tereknél használják, vagy ott, ahol nem annyira fontos a magas biztonsági szint. Előnyük, hogy olcsók. A középszintű biztonsági szintnél megjelennek a plusz védelmek. Ez lehet akár fűrés vagy másolás elleni védelem is. Abban az esetben, ha az árát, illetve a minőségét tekintjük, akkor elmondható, hogy az ebbe a szintbe eső zárok a legelterjedtebbek. A betörőknek ezekkel már nehezebb dolguk van. A magas biztonsági szintű zárok már több fajta védelemmel vannak ellátva. Ezeket már általában olyan kulcsok nyitják, amik különleges profillal készülnek, így feltörésük majdhogynem lehetetlen. Az áraikat tekintve már jóval drágábbak az előző szintekbe eső zárokhoz képest, de jóval nagyobb biztonságot is nyújtanak. [44]

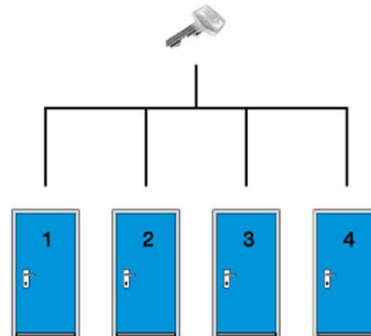
3.4. Zárrendszerek

A zárrendszereknek 4 fajtáját ismerjük. Az első az azonos zárlati rendszer, a második a portál rendszer vagy más néven főkulcsosrendszer, a harmadik csoport a vezérkulcsos rendszer, a negyedik pedig a központi zárrendszer.

Az azonos zárlati rendszerről akkor beszélünk, ha van egy kulcs, ami tegyük fel, hogy az összes zárbetétet, adott esetben az összes lakatot is nyitja a háznál. Például nyitja a kulcs a bejárati ajtót, a garázst, de még a postaládát is. Ez egy elég egyszerű rendszernek mondható, de annál hasznosabb mondjuk egy családház esetén, amikor nem kell keresgelnünk a kulcscsomón az éppen megfelelő kulcsot, így ez egy kényelmes megoldás lehet. [45] A 28. ábrán vizuálisan lehet látni ennek a rendszernek a működését.

MAUER
ASSA ABLOY

Azonos zárlatú rendszer

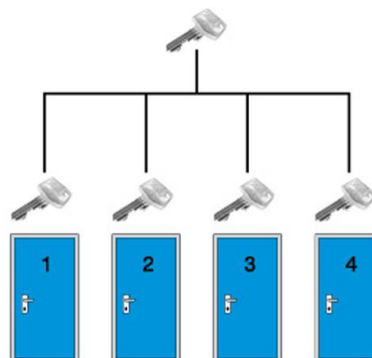


28. ábra: Azonos zárlatú rendszer [46]

A főkulcsosrendszert úgy kell elképzelni, hogy minden ajtóhoz van egy egyedi kulcs, ami csak egy bizonyos ajtót nyit, viszont van egy olyan kulcs is, ami pedig az összes zárbetétet nyitja. Leggyakrabban ez a rendszer szállodákban, fordul elő, amikor a vendégnek van egy kulcsa, ami csak a szobája ajtaját nyitja, viszont a takarítók már olyan kulccsal rendelkeznek, ami az összes szoba ajtaját nyitja. [45] A 29. ábrán a főkulcsos rendszer látható.

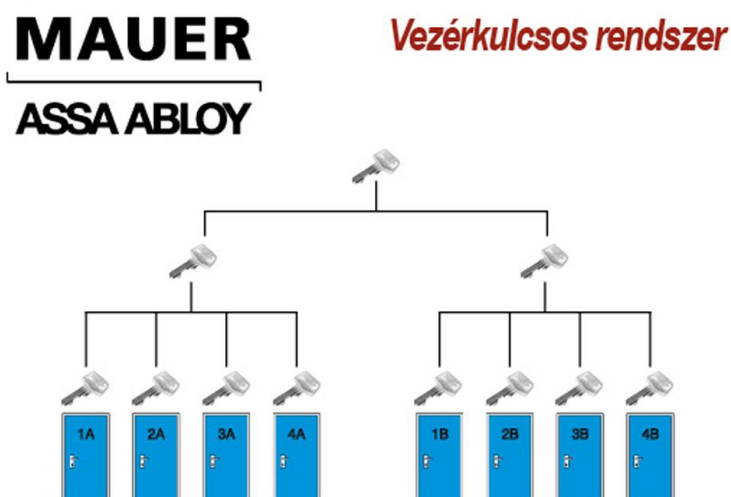
MAUER
ASSA ABLOY

Főkulcsos rendszer



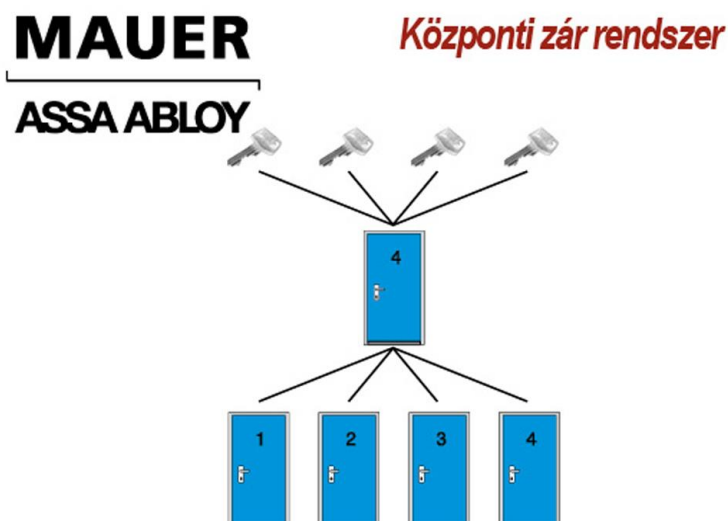
29. ábra: Főkulcsos rendszer [47]

A vezérkulcsos rendszer már egy jóval összetettebb struktúra szerint működik. Az ilyen rendszerek elkészítéséhez már komolyabb szaktudás szükséges. A rendszert úgy kell elképzelni, hogy van egy főkulcs, ami az összes zárat nyitja az épületben. Ez alatt a hierarchiában van egy alkulcs vagy csoport kulcs, ami tegyük fel, hogy nyitja az összes gépészeti helyiség és ez alatt helyezkedik el az egyedi kulcs, ami mondjuk csak az egyik gépészeti helyiséghez jó. A jó számolás és tervezés fontos alappillére ezen rendszereknek. Az ilyen zárrendszerekben lévő zárbetétekben a normál csapokon kívül találhatók úgynevezett kódcsapok is. Ezek a csapok nagyon vékonyak. Az elkészítéskor meg kell határozni a kulcs vágási adatait, illetve, hogy mennyi csap, kódcsap lesz a zárbetétben, valamint ezek pozícióját és méretét. Természetesen minél több a jogosultság annál nehezebb a rendszer kialakítása. [45] Elsőre bonyolultnak tűnhet elképzelni, de a 30. ábra segít ennek a rendszernek a megértésében.



30. ábra: Vezérkulcsos rendszer [48]

A központi zárrendszerek úgy épülnek fel, hogy van például egy központi ajtó, amin minden dolgozónak át kell jutnia, viszont a saját irodájuk ajtaját már csak az a kulcs nyitja, ami náluk van, viszont ezzel a kulccsal másik dolgozó irodájának az ajtaját már nem lehet kinyitni. A rendszer felépítését a 31. ábra szemlélteti.



31. ábra: Központi zárrendszer [49]

3.5. Kulcsok működése és típusai

A kulcsok a mindennapok részét képezik, de nem is biztos, hogy gondolnánk, hogy mennyi típusa létezik. Az ember általában, amikor elhagyja a házát vagy hazaérkezik, akkor az az első mozdulat, hogy bezárja vagy kinyitja a bejárati ajtót. Viszont a működésükről legtöbbször csak annyit tudunk, hogy balra nyit és jobbra zár. Ebben az alfejezetben bemutatom a pontos működésüket és a leggyakoribb típusokat.

3.5.1. Működés

Az első pont a beillesztés. Ekkor a kulcslyukon át a kulcsot behelyezzük a zárba. A második pont az illeszkedés. Ez azt jelenti, hogy a kulcs profilja beilleszkedik a zár belső mechanizmusába. Ekkor, ha a zárba megfelelően illeszkedik a kulcs, akkor a megfelelő módon pozicionálja a csapokat. A harmadik a mozgatás. A kulcs elfordításával a belső alkatrészek elmozdulnak. Abban az esetben, ha a kulcs megfelelő a zárba, akkor a csapok olyan pozícióba kerülnek, hogy nyithatóvá válik. A negyedik lépés a kioldás. Ilyenkor minden csap a megfelelő helyre kerül, így a zárnyelv elforgathatóvá válik. Az ötödik egyben utolsó lépés pedig a retesz működtetése. Ekkor a zárnyelv elmozdul, így nyitva vagy zárva az ajtót. [50]

Ezek tudatában felértékelődhet bennünk egy egyszerű kulcsnak a használata.

3.5.2. Legismertebb kulcstípusok

Az itt bemutatott kulcsok közül biztosan találkozott már mindenki a bemutatott fajtákkal. Az első típus a hagyományos fogazott kulcs. Ezekről a kulcsokról azt kell tudni, hogy síklemezek, melyek eltérő mélységű, egyenes vagy ferde bevágásokkal rendelkeznek. Ezek a bevágások teszik lehetővé, hogy csapok a megfelelő pozícióba kerüljenek. Előnyük, hogy olcsók, nagyon elterjedtek. Hátrányuk, hogy másolhatók, biztonsági szintjük elég alacsony. [50]

A második típus a hengerzár kulcs. Ezek hengeresebb formájúak. Ezeken már nem bevágások vannak, hanem hornyok, amik különböző mélységűek és szélességűek. A hornyok is azért felelnek, hogy emeljék vagy süllyesszék a csapokat, lamellákat. Előnyük, hogy nehezebb őket másolni, ezáltal magasabb biztonsági szintet biztosítanak. Hátrányuk, hogy drágábbak. [50]

A harmadik a tollas kulcs. Ezeket a típusokat régebben használták leginkább. Lapított formájúak a végen bevágásokkal. Ezeket a bevágásokat nevezzük tollaknak, amik illeszkednek a zárban lévő csapokba, lemezekbe. Előnyük, hogy egyszerűek. Hátrányuk, hogy nem túl biztonságosak, illetve a mai típusokhoz képest nagyobbak. [50]

Ebben a fejezetben bemutattam, hogy a zárok hogyan fejlődtek az évszázadok során. Az egyszerű egyiptomi zártól egészen a biometrikus zárukig. A különböző zárrendszerek, hogyan segíthetik egy vállalat működését, hogyan tehetik könnyebbé a kulcskezelést. Abban az esetben, ha zárokról beszélünk, akkor kulcsokról is kell, hogy szó essen, így az utolsó alfejezetben bemutattam a kulcsok működését, illetve pár ismert típust. Véleményem szerint a mechanikus zárok korszaka előbb-utóbb elmúlik, mert az ember folyamatosan vágyik az új technológiák kipróbálására, de ezek megbízható működését évszázadok bizonyítják, így szerintem teljesen kiváltani őket még egy darabig nem fogjuk tudni.

4. INTEGRÁLT BELÉPTETŐ- ÉS ZÁRRENDSZEREK ALKALMAZÁSA KÜLÖNBÖZŐ KÖRNYEZETEK BEN

Ebben a fejezetben bemutatom, hogy az integrált beléptető- és zárrendszerek hogyan jelennek meg más-más környezetekben. Elsőként, hogy teljes képet kapjunk és megértsük, hogy mit is jelent az integrált biztonságtechnikai rendszer, ezért fogalom meghatározásokkal kezdem ezt a fejezetet.

4.1. Integrált vagyonvédelem

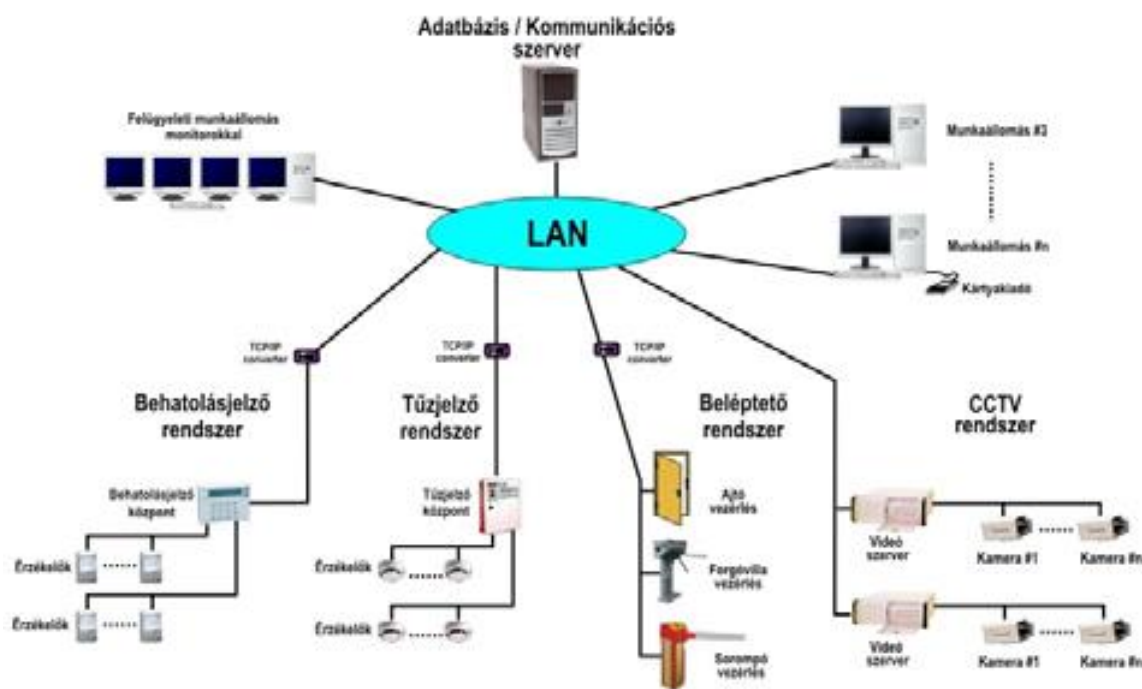
Az integrált rendszerek használata nagyon fontossá vált az idők során. Annyi új rendszer jött létre, hogy ezek egyesével történő kezelése már szinte lehetetlen feladatnak minősül. A biztonságtechnikai eszközöket gyártók, ezért elkezdtek azon dolgozni, hogy ezeket a különböző eszközöket hogyan tudnák egy felületen megjelentetni. Ezért mondhatjuk, hogy az integrált biztonságtechnikai rendszer célja, hogy a különálló alrendszerekből érkező információkat egyesítse és egy közös felületen jelenítse meg. További feladata, hogy a különböző rendszerek között biztosítsa az adatcserét, együttműködést, valamint támogassa a gyors és hatékony beavatkozást. Az események egységes naplózását is fontos feladat akár alrendszerenkénti bontásban is. [51]

A nemzetközi szakirodalom is felhívja a figyelmet az integráció fontosságára. Közvetlen hatással van az integráltsági fok és a technológia színvonala egymásra és ez befolyásolja az infrastruktúra kitettségét. [17]

Az integrált biztonságtechnikai rendszer központi eleme a központi számítógép, amelyen a vezérlés egységes, grafikus felületen jelenik meg. Ezen a felületen az eszközök különböző ikonokkal jelennek meg, valamint automatikusan megjeleníti az ezekhez tartozó eseményeket. A számítógép nem helyettesíti az alrendszerek saját központjait, ehelyett összegyűjti, feldolgozza és áttekinthető formában jeleníti meg, ezzel elősegítve a kezelők gyors és pontos reagálását egy adott eseményre. [51]

Ezek az események eseménynaplóba rögzülnek, amely részletes adatokat tartalmaz magáról az eseményről és annak kezelésének folyamatáról. A biztonsági személyzet előre meghatározott utasításokat kaphat a megfelelő kezelés érdekében. Ezek végrehajtása

szintén naplózásra kerül. A kezelőknek lehetséges van megjegyzéseket, kiegészítő információkat rögzíteni a naplóba. [51] A 32. ábra szemlélteti, hogy hogyan épül fel egy ilyen rendszer. Láthatjuk, hogy egységesen kezeli a különböző vagyonvédelmi rendszereket.



32. ábra: Integrált vagyonvédelmi rendszer [51]

4.2. Integrált beléptetőrendszerek különböző környezetekben

Ahhoz, hogy a környezetnek legmegfelelőbb rendszer tudjuk kiépíteni először tisztában kell lenni a védendő objektum sajátosságaival. Ehhez tudnunk kell azt, hogy mi minősül egyáltalán objektumnak.

Az objektumok olyan épületek, létesítmények, nyitott vagy zárt területek, melyek valami vagy valaki által veszélyeztetettek, így biztosításuk szükséges. Az objektumokat rengetegféle módon lehet csoportosítani. Funkciók, elhelyezkedés, építészeti körülmény, beléptetés, működés, valamint a biztosítást végzők szerint. [1]

4.2.1. Vállalati környezet

Vállalati rendszerek esetén fontos a hatékonyság, a kényelem, valamint, hogy az eszközök ne hátráltassák a munkavállalókat.

A munkahelyemen is jogosultság szerint tudunk beállítani belépési profilokat, időkorlátokat. Nagyon fontos egy vállalatnál, hogy a jogosultságkezelés rugalmasan és pontosan történjen. Például az egyik jogosultság úgy van létrehozva, hogy a raktárba a munkavállalók csak reggel kilenc óra és délután négy óra között tudnak belépni. A perimeter területek is időkorláttal lettek létrehozva, úgy, hogy hétvégén csak a főbejáraton keresztül tudnak belépni, mivel az őrszolgálatnak ellenőriznie kell, hogy jogosultak-e a hétvégi munkavégzésre. A munkaidőnyilvántartó szintén integrálva lett, így az időadatok már automatikusan elkerülnek a megfelelő helyre. A különböző helyiségek, területek zónákra lettek bontva. Ezek a biztonsági szinteket jelzik. Azok a területek, amik mindenki számára elérhetőek az első számú zónába tartoznak. A második zónába azok a területek foglalnak helyet, ahová már külön jogosultság szükséges a belépéshez. Ilyen terület például egy labor helyiség. A harmadik zónák kiemelt biztonságúak. Itt már több faktoros azonosítás szükséges, ami azt jelenti, hogy már nem elegendő egy sima belépési jogosultság a kártyán, hanem saját PIN kóddal is kell rendelkezni. A jogosulatlan belépési kísérlet a beléptetőrendszer grafikus felületén megjelenik, amire a vagyonőröknek azonnal reagálniuk kell. A hármas zónába tartozó helyiség lehet például szerverszoba vagy irattár.

Irodai környezetben gyakran fordul elő, hogy a munkavállalókhöz vendégek érkeznek mondjuk tárgyalás miatt. A gyorsabb beléptetés céljából kialakításra került egy úgynevezett Visitor Management System magyarul: látogatói menedzsment rendszer, ami azt teszi lehetővé, hogy a vendég regisztrációja után a vendégfogadó értesítést kap arról, hogy a vendége megérkezett.

A munkavállalók a belépőkártyáikat számos más célra tudják használni, mivel ezek a rendszerek is integrálva lettek. A kázinban az étel kifizetése előtt a munkavállalóknak azonosítaniuk kell magukat, ezután tudnak csak fizetni. A csomagautomaták is kártyaolvasókkal vannak ellátva, így a kártyahasználat és a vonalkód leolvastatása után a csomagautomata megfelelő rekesze kinyílik. A nyomtató használata is belépőkártyához kötött.

A rendszám felismerés is egy lehetséges integráció a beléptetőrendszerbe. Ez a rendszer úgy működik, hogy egy kamera figyeli a sorompóhoz érkező autók rendszámát. Abban

az esetben, ha a rendszám rögzítve van a beléptetőrendszerben, a sorompó kinyílik, így a munkavállaló be tud hajtani a parkolóházba, anélkül, hogy a belépőkártyáját használta volna a sorompó nyitásához.

4.2.2. Kórházi környezet

Kiemelten fontos környezet, ugyanis ez egy nagyon komplex terület. Azért, hogy a veszélymentes állapotot fenn lehessen tartani a különböző biztonságtechnikai eszközöket összehangoltan kell kezelni. A jól kiépített rendszereknek köszönhetően a betegáztatás biztonsága folyamatos lehet. [1]

A rendszerek kiépítésénél nagy figyelmet kell fordítani arra, hogy a kórházakba belépő személyek csoportja heterogén, a látogatottság nagy, illetve, hogy ezekben az objektumokban a tevékenységi körök szerteágazók. Figyelembe kell itt is venni, hogy a biztonsági rendszerek ne tartsák fel a különböző tevékenységeket, hanem védelmezzék azokat. Természetesen a kórházakban vannak olyan helyek, melyek védelme kiemelten fontos feladat. Az ilyen helyiségeknél a belépők, illetve az eszköz, anyag mozgások monitorozása elengedhetetlen. Azonosítás szempontjából ebben a környezetben dolgozó személyzetnek a legmegfelelőbb a belépőkártya. Az ilyen nagy objektumoknál nem mindig áll rendelkezésre elegendő számú biztonsági személyzet, ezért kell úgy felépíteni a rendszert, hogy minél több eszköz integrálható legyen. [1]

A kórházakban gyakran alkalmazzák a betegek körében a karkötőkbe integrált transzponderes módszert. Ezzel a módszerrel monitorozni lehet, hogy a beteg az osztályon tartózkodik-e vagy esetleg valamilyen vizsgálaton vesz részt. A kórházakban a látogatói létszámot is keretek közé kell szorítani, így az előbb említett módon a látogatót lehet arról tájékoztatni, hogy a látogatás lehetséges-e. A beléptetőrendszerek képesek jelezni, ha a látogatók létszáma elérte a maximumot, így az őrszolgálat tagjai időben korlátozni tudják a belépéseket. [1] A 33. ábrán látható a transzponderes karkötő, amit gyakran használnak a kórházakban.

A be- és kilépések monitorozhatósága az integrált rendszerben hatékony védelmet tud nyújtani az illetéktelen behatolásokkal szemben, így biztosítva a betegek, illetve dolgozók értékeinek megóvását. [1]



33. ábra: Transzponderes karkötő [1]

A betegazonosítás is egy rendkívül fontos dolog a kórházi ellátás során. Sajnos fordultak elő esetek, amikor a nem megfelelő beteg esett át nem megfelelő műtéten. Ez hatalmas kockázatot jelent ebben a környezetben. A beléptetőrendszerbe integrált RFID technológia használata megkönnyíti az azonosítást. [1]

A gyógyszerrel való visszaélés is előfordulhat. A gyógyszerekhez való illetéktelen hozzáférést a megfelelő jogosultságkezeléssel és belépési adatok nyomon követésével ki lehet küszöbölni. Sok helyen tapasztaltam, hogy a gyógyszeres szekrényekben bent hagyják vagy bent felejtik a kulcsot. Ezzel a módszerrel ez a kockázat megszüntethető, ugyanis a szekrényeket is el lehet látni kártyaolvasóval, valamint nyitásérzékelővel is, így a beléptetőrendszer értesítést tud küldeni az őrszolgálatnak, ha egy ajtó túl hosszán nyitva van. [1]

A műtőkben csak megfelelő öltözetben lehet tartózkodni, viszont távozáskor ezeket kivinni nem lehet. Erre egy olyan módszer lett kitalálva, hogy a műtős ruhákba kicsi RFID transzponder van elhelyezve, így a belépőkapun áthaladva a rendszer egyből jelzést ad, ha egy ilyen ruha kikerül a műtős környezetből. [1]

4.2.3. Könyvtári környezet

A könyvtárak esetében is a különböző biztonságtechnikai eszközök egymásra épülő megbízható működése elengedhetetlen fontosságú. Könyvtári objektumvédelemnél is használják a legfontosabb technikákat a könyvtári igényekhez alkalmazkodva. Lehet szó

behatolás védelemről, riasztástechnikáról, videós megfigyelésről, beléptetőrendszerekről és az állományvédelemről. Ezek az intézmények a kezdetektől fogva rendelkeztek valamilyen személyazonosító rendszerrel. Itt is megtalálhatóak a tudás alapú, birtoklás alapú, biometrikus alapú azonosítási formák. A birtoklás alapú az egyik legelterjedtebb, ilyenkor RFID-val ellátott olvasó kártyával azonosítja magát. A szoftverben ezáltal minden szükséges adat megtalálható és monitorozható. Általában a könyveket is ellátják már RFID címkével, így, ha valaki jogosulatlanul akar kivinni egy könyvet, a rendszerben egyből riasztás generálódik. Ahogy a vállalati környezetben és a kórházi környezetben úgy a könyvtáraknál is figyelembe kell venni, hogy a biztonsági rendszerek ne zavarják az embereket. [1]

4.2.4. Szoftverek

Ahhoz, hogy valahol lássuk a különböző eseményeket, riasztásokat, egy olyan szoftverre van szükségünk, ami kezelni tudja a különböző eszközeinket.

Az egyik ilyen szoftver a Bosch által fejlesztett BIS (Building Integration System magyarul épületintegrációs rendszer). Napi szinten használom ezt a rendszert a munkám során. Használata elég gyorsan elsajátítható, de idő kell a teljeskörű megismeréséhez. A szoftverbe a beléptetőrendszeren kívül integrálva van a tűzjelző, a rendszámfelismerő, behatolásjelző, a riasztó, valamint a munkaidőnyilvántartó is. A rendszer képes arra is, hogy a munkavállalók arcképét névvel ellátva a forgóvilán való áthaladáskor megjeleníti. Ez egy fontos funkció, mivel a vagyonőrök tudják ellenőrizni, hogy a kártyahasználó tényleg az a személy, aki jogosult a belépésre.

A Bosch rendszerén kívül számos egyéb más gyártó szoftvere is megtalálható. Az egyik ilyen például a Predor, ami egy magyar fejlesztésű szoftver. A fejlesztő oldalát átnézve egy nagyon felhasználóbarát sok funkciót kezelni bíró rendszerről beszélhetünk. Ami nekem személyesen nagyon megtetszett, hogy egy tűzeset során egy evakuálási listát generál a mobiltelefonra, így a gyülekezési ponton gyorsan kideríthető, hogy esetleg ki maradt még az épületben. A leírás alapján bármilyen mechanikus eszközt tudnak kezelni, így a megrendelőnek nem kell azon gondolkoznia, hogy milyen eszközhöz, milyen szoftver illik. A BIS-hez hasonlóan ez is képes a rendszámfelismerésre. [52]

4.3. Integrált zárrendszerek

Integrált zárrendszerekről ugyanúgy akkor beszélünk, ha a zárrendszer valamilyen szoftverbe integrálva van például más rendszerekkel együtt. Ebben a fejezetben bemutatom, hogy a zárrendszerek integrációja egy egységes rendszerbe mennyi plusz funkciót hozhat létre.

Ezeket a rendszereket számos környezetben lehet alkalmazni, mint például irodaházak, kórházak, szállodák, gyártó üzemek.

Az integrál zárrendszerek mögötti gondolat az, hogy a hozzáférési pontok ne önálló kulccsal rendelkezzenek, hanem egy szoftver segítségével ezek is egy egységet képezzenek.

A központi szoftver segítségével az ajtók vezérelhetők. Ez azt jelenti, hogy távolról a rendszeren keresztül egy ajtót ki lehet nyitni, valamint be is lehet zárni, ha arra van szükség. A BIS-ben például ez úgy néz ki, hogyha egy ajtó tartós nyitásra állítunk, akkor a zár folyamatosan nyitott állapotban van, így a helyiségbe akárki be tud menni anélkül, hogy használta volna a kártyáját. A másik a normál mód, amikor a zár csak kártyahúzásra nyit, amikor az illető rendelkezik a megfelelő jogosultsággal.

A rendszer akkor tud a legjobban működni, ha a különböző alrendszerek megfelelően kommunikálnak egymással. Felépítéséhez szükség van elektromos zárra, valamilyen azonosítási technológiára, egy közös hálózatra, valamint egy szoftverre, ami képes ezeket együtt kezelni.

A zárrendszereket össze lehet kötni a videómegfigyelő rendszerrel, riasztórendszerrel, tűzjelző rendszerrel, beléptetőrendszerrel, valamint épületautomatizálási rendszerrel is.

Videómegfigyelő rendszer esetén, ha egy jogosulatlan belépési kísérletet hajt végre valaki, akkor az egységes szoftverben megjelenhet a kamerakép, ami az adott helyiség ajtaját figyeli. Ez előnyös lehet szerverszobáknál, irattáraknál, főbejáratoknál. Riasztórendszereknél például a zár automatikusan bezárt állapotba kerülhet. Ez a funkció bankoknál lehet hasznos, hogy a betörő ne tudjon kimenekülni az épületből, amikor megszólal a riasztó.

Tűzjelző rendszereknél pedig előírás van róla, hogy tűzjelzés esetén a menekülés útvonalon található ajtóknak automatikusan nyílniuk kell a könnyebb menekülés érdekében.

Beléptetőrendszerek esetében azért hasznos, mert nem kell a különböző kulcsokat keresgetni, hogy egy helyiséget ki tudjunk nyitni, hanem elég hozzá egy belépőkártya, ami el van látva a megfelelő jogosultsággal.

Épületautomatizálási rendszereknél azért hasznos, mert ha egy zártól az az információ jön vissza, hogy zárt állapotba került, akkor a rendszer például automatikusan lekapcsolja a villanyt.

5. IRÁNYZATOK, KOCKÁZATOK ÉS JÖVŐBELI FEJLŐDÉSI LEHETŐSÉGEK

Ebben a fejezetben rávilágítok azokra az irányzatokra, amerre a biztonságtechnikai szektor tart. A mai kor jellemző felgyorsult világban szinte naponta jönnek ki új technológiák, amik trendeket alakítanak ki. A kérdés az, hogy ezek az új rendszerek mekkora kockázatokat hordoznak, mivel ezen technológiák egyik napról jelennek meg a másikkra, így véleményem szerint elég nagy kockázatokkal járnak. Szót ejtek a jövőbeli fejlődési lehetőségekről is, valamint arról, hogy én hogyan látom a jövőt ezzel a témával kapcsolatban.

5.1. Irányzatok a biztonságtechnikában

Ebben az alfejezetben bemutatom, hogy jelenleg hol tart a technológiai fejlődés, valamint, hogy a jövőben milyen eszközöket, újdonságokat fogunk alkalmazni a biztonságtechnikai szektorban.

5.1.1. Digitalizáció

Az irányzatot most a digitalizáció határozza meg. Egyre inkább azon dolgozunk, hogy a rendszereket alrendszereket hogyan tudjuk a legkönnyebben és a legjobban együtt kezelni. Ehhez digitalizációra van szükség. A digitalizációnak köszönhetően jutottunk el mára arra a szintre, hogy eszközeinket akár távolról is tudjuk vezérleni. A munkát nagyban megkönnyíti, hogy például egy jogosultság kiosztásnál nem kell személyesen megjelennünk az adott olvasónál, hogy felkódoljuk a kártyára a jogosultságot. Ez egy erre a célra kialakított számítógép segítségével nagyjából két kattintás alatt elvégezhető ez a művelet. A digitalizáció tette azt is lehetővé számunkra többek között, hogy a belépőkártya használatokat valós időben tudjuk monitorozni, illetve egy behatolási kísérlet esetén egyből tudunk reagálni, mert a rendszer értesítést küld. Azok a vállalatok, amelyek nem akarnak saját szervereket üzemeltetni lehetőségük van felhő alapú szolgáltatások igénybevételére. Az alrendszereket a hálózatok segítségével tudjuk integrálni. Ennek köszönhetően láthatjuk egy felületen a tűzjelzőt, a beléptetőrendszert, kamerarendszert, de kibővíthetjük akár épületautomatizálási rendszerekkel is. Így kapunk

egy komplex egy helyről vezérelhető infrastruktúrát. A digitális fejlődés érintette a záruk piacát is, ugyanis megjelentek az okoszárok ennek köszönhetően. Ezek előnye, hogy nem kell már a fizikális kulcsokat magunkkal hordani, elég hozzá a telefonunk is, hogy a lakásunk ajtaját ki tudjuk nyitni.

A digitalizációnak számos előnye ismert ezen a téren is. Az egyik, hogy rugalmasan és gyorsan tudjuk a jogosultságokat kezelni. A másik pont a költséghatékony üzemeltetés. A harmadik pont pedig, hogy azonnal látjuk, ha valami történik és vissza is tudjuk ellenőrizni.

5.1.2. IoT – Internet of Things (Dolgok Internete)

Sokan úgy vélik, hogy a digitalizáció volt a legutóbbi paradigma váltás a biztonsági rendszerek terén. Nagy a valószínűség arra, hogy a következő az IoT (Internet of Things magyarul dolgok internete) lesz. Ez a folyamat igazából már el is kezdődött akkor, amikor a különböző okoseszközök megjelentek az otthonokban. Ezt a piaci szegmenst az emberi kényelem hozta létre, ugyanis, ha nem muszáj, akkor nem hordunk magunknál lakáskulcsot, vagy mire hazaérünk a munkából lehűtjük vagy felfűtjük a lakást, mindezt úgy, hogy a telefonunkról elindítjuk a klímát vagy a gázkazánt. [53]

Számos előnye lehet az ezen technológián alapuló beléptetésnek vezérlésnek is. Az elsődleges pont a kényelem fokozása. Ezek a rendszerek már több, illetve részletesebb információt tudnak biztosítani. A következő a költséghatékonyság. A vállalatok rengeteg pénzt tudnak megspórolni a segítségével. Nagyobb rugalmasságot biztosítanak a felhasználó számára. Az azonosítási adatok elemzésével megállapítható, hogy a munkavállalók mely helyiségekben tartózkodnak a legtöbbet, illetve hol a legkevesebbet, így elősegíthető a munkaterület jobb kihasználása. [53]

Hátrányokkal is rendelkezik, ugyanis ezek használatával nő a kiberbiztonsági kockázat is. A másik nagy hátrány az pedig az internettől való függés.

5.1.3. Biometrikus azonosítás elterjedése

A fejlődési irányt nagyban befolyásolták a biometrikus azonosító eszközök megjelenése. Ezen eszközök megjelenésével fokozni lehetett a biztonsági szintet, mivel ezek általában az ember valamely egyedi tulajdonságát használják fel az azonosításhoz. A biztonsági

szintet azért növelték, mivel ezek a tulajdonságok sokkal nehezebben másolhatók, mint például egy kulcs.

Míg az ujjlenyomat alapú azonosítás a legrégebbi és legelterjedtebb módszer, addig az érhálózat alapú azonosítás a legújabb módszerek közé tartozik. Ez az eljárás úgy működik, hogy infravörös fény segítségével egy szenzor a vér áramlását érzékeli. Ez nagy pontosságot és gyorsaságot eredményez. Az azonosítás során nem szükséges fizikai kontaktus, mivel a kezünket elég, ha elhúzzuk az eszköz felett. Nincsen olyan kitettség, mit az ujjlenyomat alapú azonosításnál, hogy az ember ujjja sérült, vagy nagyon ritka esetben, de nincsen ujjlenyomata. Elmondható, hogy a világon majdnem az összes embernél alkalmazható. [54] Ezt a módszert a 34. ábra mutatja be.



34. ábra: Érhálózat alapú azonosítás [55]

A hangalapú azonosítás is az új technológiák közé sorolható. Ennél a módszernél a hang frekvenciáját, hangszínt, hanglejtést, ritmust azonosítja a rendszer. Két fajtása létezik. Az első, amikor magát a beszédet ismeri fel a rendszer, a második pedig, amikor a hangot, illetve az ember jellemzőit. Nagyon sok mindentől függ a mért hang, például távolságtól, személyiségtől, és még sorolhatnánk. Hátrányok közé tartozik, hogy nagyon érzékeny a rendszer így, ha az ember lebetegszik már nem biztos, hogy az azonosítás sikeres lesz. Összetettsége miatt inkább másodlagos alkalmazásra jelenthet megoldást. [54]

A biometrikus azonosításhoz használt adatok rendkívül szenzitívek, így azok kezelésére és tárolására nagy hangsúlyt kell fektetni.

5.1.4. A mesterséges intelligencia megjelenése a biztonságtechnikában

Egy pár éve a mesterséges intelligenciáé (továbbiakban MI) a főszerep. Minden gyártó olyan eszközöket, olyan szoftvereket kezdett el gyártani, fejleszteni, amiben az MI már egy meghatározó szerephez jutott. A videómegfigyelés terén nagyon nagy az előrelépés az MI segítségével. Vannak olyan szoftverek, amik már képesek az ember mozgásából megítélni és előre jelezni, hogy milyen szándék vezérli, ezzel tulajdonképpen elemelve az emberi viselkedést. Ennek a módszernek anomália-elemzés a megnevezése. A videó elemzéseknél már az is lehetséges, hogy leírások alapján az MI megkeresi az adott embert például fekete pulcsiban, majd a kameraképeket összerakva végig kíséri, hogy hogyan jutott el a kiindulási ponttól a szerverszobáig. Ez túlmutat a már jól ismert analitikán. [56] Előbb utóbb a beléptetőrendszerekhez is eljut az MI. El tudok képzelni egy helyzetet, amikor az integrációnak köszönhetően a videómegfigyelő rendszer elemzi egy ember viselkedését, mozgását, és ha úgy ítéli meg, akkor a szoftver a vezérlőn keresztül letiltja a kártyaolvasót, vagy már magát a kártyát, így nem engedi belépni a telephelyre, az esetlegesen ittás munkavállalót.

5.2. Kockázatok

Az új kor új kockázatokat hozott magával. Régen még fizikai módszerek okozták a legnagyobb problémákat, azonban manapság már attól kell félnünk, hogy az adataink ne kerüljenek ki az internetre. Minél több eszközünk van fent a hálózaton, annál nagyobb a kockázat is. A biztonsági szint a számítógépek esetén már magasnak mondható, de ha egy okoszárról van szó, akkor ez már teljes nyugalommal nem kijelenthető. A beléptetőrendszerek területén is nagy a hátrány, ugyanis valamennyi belépőkártya már fel lett törve, de még mindig használatban vannak. Ennek az is oka lehet, hogy nem lehet mindig lecserélni mondjuk egy vállalatnál az összes kártyát, mivel a procedura végére érve valószínűleg a kiosztásra került új kártyát is feltörték már. [53]

5.2.1. Kiberbiztonsági kockázatok

Informatikai rendszerek - hálózatok, szerverek, számítógépek - védelmére irányuló intézkedések összessége, melynek célja a támadások, jogosulatlan hozzáférések és az ezek által okozott károk megelőzése. [57]

Az uniós kiberbiztonsági szabályozás egy olyan keretrendszert biztosít, ami biztosítja a tanúsítását a digitális termékeknek, szolgáltatásoknak, folyamatoknak. [57]

Az Európai Unióban három leggyakrabban előforduló fenyegetés a rendelkezésre állást fenyegető veszélyek, a zsarolóvírusok, illetve azok a veszélyek, amik az adatainkat érintik. A rendelkezésre állást fenyegető veszélyek, azok, melyeknek célja a rendszerek megbénítása, ezáltal ellehetetlenítve a szolgáltatások, rendszerek igénybevételét. A zsarolóvírusok által a támadók át tudják venni az irányítást a rendszerek felett. Adatokat fenyegető veszélyekről pedig akkor beszélünk, amikor az adatainkhoz jogosulatlanok férnek hozzá, megmásítják ezeket, vagy kikerülnek a világhálóra. [57]

A kiberbiztonsági kitettség egyre nő a világon. Számos támadási formát ismerünk, amik ellen a fejlesztők folyamatosan harcolnak. A gyártókkal szemben az igény is nő, hogy az eszközök saját azonosítóval rendelkezzenek a gyártás első mozzanatától kezdve. Mára világossá vált, hogy a megszokott módszerek már nem nyújtanak megfelelő védelmet. Ilyen megszokott módszer egy szoftverbe történő belépés során a név vagy felhasználónév és egy jelszó használata. Az MFA (Multi-Factor Authentication magyarul többtényezős vagy többlépcsős hitelesítés) egy hatásos megoldás lehet erre. Ez azt jelenti, hogy több azonosítási tényezőt kell megadni. Például nem elég csak a PIN kódot megadni, hanem az arcunk is kell az azonosításhoz. Ilyen hitelesítésekkel leggyakrabban a bank szektorban találkozhatunk. Ennek a hitelesítésnek az a célja, hogy minimalizálja a kockázatot. Az egyik adatunk kiszivároghat, de még akkor is van egy, amire már kisebb az esély. [53]

Ezek a támadások könnyebben kivédhetők, ha pár pont teljesül gyártói, viszonteladói, rendszer integrátori, valamint végfelhasználói oldalról. Gyártói oldalról fontos, hogy a biztonság mindig prioritást élvezzen a tervezés első pillanatától kezdve. Ne alkalmazzon olyan technológiákat, amik már fel lettek törve. Viszonteladói oldalról fontos, hogy az igényeket a gyártó felé közölje, valamint ne forgalmazzon olyan eszközöket, melyek már nem felelnek meg a biztonsági követelményeknek. Rendszer integrátorként tisztában kell lenni az igényekkel. Olyan rendszereket ne telepítsen, amelyek nem tudják biztosítani a biztonságos hozzáférést az adatokhoz. A két lépcsős azonosítást részesítse előnyben, valamint csak olyan eszközöket alkalmazzon, melyek megfelelnek az előbb említett

követelményeknek. Végfelhasználóként csak a megfelelő védelemmel bíró eszközöket vegye figyelembe. Digitális azonosítók használata a fizikaiakkal szemben. Részletes napló használata, melyből kinyerhetők a legfontosabb információk. Automatizált beléptetőrendszerek használata manuális verziók helyett. [53]

A kiberbiztonságban vannak olyan támadási formák, ami az utóbbi időben elterjedtek. Az első támadási forma az úgynevezett replay attack (magyarul visszajátszásos támadás), amelyek során a támadók elfognak és újra felhasználnak adatátvitteleket, így jogosulatlan hozzáférést szereznek a rendszerekhez. Ez azt jelenti, hogy a támadó például elfog egy tranzakciót, amit később változtatás nélkül újra küld a címzettnek, így a rendszer hitelesnek fogja fel a korábbi üzenetet és megismétli a folyamatot. [58]

A következő pont a lehallgatási forma, amikor a támadó egy gyenge titkosítást, úgymond lehallgat, de igazából lemásol. Ennek az a célja, hogy egy gyenge titkosítással rendelkező belépőkártyáról a kódolást lelopja, így az objektumba már be tud lépni.

A harmadik módszer az az, amikor a számítógépre egy olyan nem hitelesített firmware frissítést telepítenek, amik egyből zsarolóvírussal támadják meg a számítógépet. Ezzel a módszerrel akár képesek az egész rendszert irányítani, megbénítani.

5.2.2. Biometrikus adatok kockázata

Biometrikus adatok kezelése nagyon kockázatos feladat. Sokan úgy gondolják, hogy ez az azonosítási mód a legbiztonságosabb ilyen téren is, de ez koránt sem így van. Az ilyen adatok kiszivárgása sokkal súlyosabb problémákat tud okozni, mint a hagyományos társaiknál. Ugyanis az ember, ha feltörik a PIN kódját tud készíteni úja, amennyit csak szeretne. A biometrikus adatok, ha kiszivárognak, azok megmásítása, újra cserélése már lehetetlen. Elviekben a kiszivárgott adatok nem visszafejthetők, de a valóságban sajnos ez nem igaz. A biometrikus rendszereket a támadók többféle képpen képesek átverni. Az első, amikor magas felbontású képek alapján lemásolják az ujjlenyomatot. Ehhez általában zselatint vagy latexet használnak. Elhunytak esetében is alkalmazható ez a módszer. Az arcfelismerés alapján működő rendszereket is képesek átverni. A módszer nagyjából ugyanaz, mint az ujjlenyomatoknál. Magas felbontású képek alapján készítenek 3D maszkokat, de elterjed már egy másik módszer is, amikor MI generált videókat alkalmaznak. Ezekkel a kevésbé megbízható rendszereket könnyedén át tudják

verni. Létezik ezeken kívül még az a módszer, amikor az írisz adatokat, valamint a hang adatokat lopják el. Az előbb említett módszerek bebizonyítják, hogy habár a biometrikus azonosítás azért jött létre, hogy fizikai jelenlét esetén működjenek csak, ezekkel a módszerekkel könnyen átverhetők. [59]

A liveness detection (magyarul élőségvizsgálat) pont ezért jött létre. Ezzel a megoldással a fejlesztők azt akarták kiküszöbölni, hogy hamisított adatokkal a támadók bejussanak a rendszerekbe. Az élőségvizsgálat valamilyen mozgást detektál, ami lehet pislogás, fejmozgás, s a többi. Ujjlenyomat olvasásánál hőmérsékletet figyelnek általában. [59]

Sok biometrikus rendszer központilag tárolja az adatokat. Abban az esetben, ha ezt az adatbázist sikeres támadás éri, akkor hatalmas mennyiségű adat kerülhet illetéktelen kezekbe. Ezért ezeket az adatbázisokat különböző titkosításokkal kell ellátni, valamint fokozott biztonsággal kell tárolni. [59]

A fejlesztők folyamatosan dolgoznak azon, hogy a biztonsági réseket eltüntessék. Számos módszer találtak ki a támadók ellen. Az első ilyen az MFA, amiről korábban már írtam. A második a sablonvédelem, amit az egyirányú kódolással próbálnak megoldani. Létezik olyan módszer is, amikor a sablonokat eltorzítják vagy módosítják tárolás előtt, így feltörés esetén a támadók nem a valódi adatokhoz jutnak hozzá. A következő módszer a viselkedés alapú biometria, ami azt takarja, hogy a rendszer figyeli például a járásmódot, így, ha azt feltételezi a belépés előtt, hogy nem a jogosult ember próbál meg belépni a helyiségbe, akkor kér még egy azonosítást. Decentralizált adattárolás is egy megoldás lehet, ami azt jelenti, hogy a felhasználók eszközein tárolják az adatokat és nem egy központi szerveren. Így, ha a szerveret támadás is éri, akkor az adatokhoz nem férnek hozzá. [59]

5.3. Emberi kockázat

Számos más kockázat típus ismert még, de ami akár nagyobb kockázatot is jelenthet egy rendszer támadásnál az az emberi tényező.

5.3.1. Felhasználói kockázatok

A munkahelyemen is gyakran előfordul, hogy a kollégák nyitva hagyják egy helyiség ajtaját, ami egyébként beléptetőrendszerrel van felszerelve, mivel kettes biztonsági zónába tartozik. Ebből is látszik, hogy a rendszer biztonsága az emberi tényezőkön is múlik. Előfordulnak olyan esetek is, amikor a kollégák átadják másnak a belépőkártyát, hogy azzal közlekedjen. Ez szabályzatban is le van írva, hogy illetéktelen kártya használat. Abban az esetben, ha az őrszolgálat ezt észleli, akkor az esetről jegyzőkönyv készül. Többszöri előfordulás esetén a kolléga vezetője tájékoztatva van az esetekről. Egy gyakran előforduló eset, hogy a különböző jelszavakat, PIN kódokat egy cetlire írva tartják. Kollégák rendszeresen beengedik egymást helyiségekbe, ahova amúgy nem lenne a másik félnek jogosultsága. Az ajtók kitámasztása is egy gyakran előforduló probléma, amivel napi szinten szembesülünk. A kiemelt helyekre alvállalkozók csak vagyonőr jelenlétében léphetnek be. Ilyen hely például a szerverszoba is.

A belépéseken túl az információvédelemi kockázatokban is nagy szerepük van a felhasználóknak. Sokszor sajnos figyelmen kívül hagyják, hogy egy e-mail kitől jött. Látnak egy linket és már nyitják is meg, mert azt írták az e-mail-ben, hogy nyertek valamit. Nagyon nagy veszélyeket hordoz ez magában, mivel a hivatkozásra kattintva mér lehet, hogy hozzá is férnek a munkavállalók adataihoz.

5.3.2. Operátori kockázatok

Természetesen azok a személyek is hibázhatnak, akik a rendszert kezelik. Az előforduló hibák, mulasztások a jogosultság kezelésnél történnek. Ilyen lehet például egy meghagyott kártyajog, vagy kilépő kollégák hozzáféréseinek késői törlése. A munkahelyen gyakorlatban ezt úgy tudjuk kiküszöbölni, hogy minden kilépőnek le kell adnia a kártyáját. A kártyaleadáskor a beléptetőrendszerben lévő profil törlésre kerül, majd a kártyát megsemmisítjük. Előfordulhat olyan eset is, amikor nem megfelelő munkavállalónak kerül a jog kiosztásra, ami csak egy kis idő múlva derül ki. Ezek a hibák jól felépített folyamatok alapján a minimális szintre csökkenthetők.

5.3.3. Oktatások

Azért, hogy a kockázatok a legalacsonyabb szintre legyenek csökkentve a munkavállalóknak kötelező oktatásokat kell abszolválniuk. Ezek olyan tréningek, amik mélyítik a biztonságtudatosságot példákon keresztül. Ezek általában egy teszt kitöltésével végződnek, hogy a munkáltató meg tudjon győződni arról, hogy a munkavállalók tisztában vannak a felmerülő veszélyekkel és adott esetben kezelni tudják őket. A munkahelyemen nem rég szerveztünk egy biztonsági napot, ahol azok a csoportok voltak jelen, mint kiállítók, akik a biztonság területén dolgoznak. A kollégák különböző játékokon vehettek részt, valamint különböző feladatokat kellett végrehajtaniuk. Úgy gondolom, hogy ez egy remek oktatási forma, ugyanis játékokon keresztül a munkavállalókban talán jobban elmélyülnek az ott látottak, hallottak.

5.4. Fejlődési lehetőségek

A fejlődési lehetőségek tárháza végtelen. Az MI megjelenésével nagyon sok kapu nyílt ki a biztonságtechnikai eszközök piacán is. A beléptetőrendszereket tekintve véleményem szerint egyre jobban el fognak terjedni a biometrikus azonosítással működő eszközök, valamint a belépőkártyák nagyvalószínűséggel eltűnnek a piacról. A mechanikus záruk helyét átveszik az okoszáruk és a digitális kitettség el fog hatalmasodni, ha nem szabjuk majd meg a határokat.

5.4.1. Érintésmentes beléptetés

A vállalatok egyre jobban figyelnek az egészségre, a biztonságra és a kényelemre. Az érintésmentes beléptetés megvalósításához mobilos azonosítókra van szükség, vagy biometrikus azonosításra, mint például az arcfelismerő rendszerek. Úgy gondolom, hogy ezek a rendszerek jelentik a jövőt. A mobilos beléptetés nagyobb rugalmasságot tesz lehetővé, valamint az elhagyott belépőkártya sem okoz már gondot. [60]

5.4.2. Egységes rendszerek

Manapság is gyakran vannak alkalmazva az integrált rendszerek, de a jövőben még több eszköz kerülhet be egy szoftver alá. Ezek a rendszerek még tovább fogják könnyíteni a biztonsági feladatokat és csökkenteni fogják az üzemeltetési költségeket. Az őrszolgálat tagjai a belépési adatok, illetve a videómegfigyelő rendszer összekapcsolásával

gyorsabban tudnak majd reagálni az eseményekre, illetve könnyebb lesz a kielemezésük. Minél több rendszer lesz összekapcsolva annál könnyebb lesz a fenyegetéseket felismerni. [60]

5.4.3. Mesterséges intelligencia a beléptetőrendszerek területén

Az MI és a gépi tanulás át fogják alakítani az eddig ismert rendszereket. A fejlett automatizáció és az intelligens funkciók rövid távon belül el fognak terjedni. Ezek már belépési mintákat, illetve anomáliákat fognak elemezni. A szokatlan belépési mintáról képesek lesznek azonnal riasztást adni. Szokatlan belépési minta lehet majd például egy nagyon késői belépési kísérlet. Képesek lesznek kizárni az esetleges emberi hibákat, ezzel növelve a biztonsági szintet. [60]

5.4.4. Szabály- és attribútum alapú beléptetési rendszerek

A jogosultságkezelés egyre inkább ebbe az irányba mozdul el. Szabályalapú beléptetésen azt értjük, hogy előre definiált szabályok alapján működik, például munkakörökhöz igazított belépési profilokat. Az attribútumalapú pedig azt, hogy bizonyos jellemzők alapján bírálja el a belépést, ami lehet, hely, idő, s a többi. Ezek a rendszerek sokkal magasabb szintű biztonsági mechanizmusokat hoznak létre. [60]

5.4.5. Intelligens analitika alkalmazása

A videómegfigyelő szegmensben feltehetően az MI, a gépi tanulás, illetve a mély tanulás integrálása megváltoztatja a különféle kockázatok felismerését. Ezek ugyanis való idejű adatok elemzésére képesek, valamint a kockázatokról előre jeleznek. Ezzel az őrszolgálat tagjai proaktívan be tudnak avatkozni egy esetleges behatolásra. Olyan helyzetekre fogják tudni felhívni a figyelmet, amit az ember lehet, hogy észre se venne. [60]

5.4.6. Smart (okos) kártyák alkalmazása

Ezek a kártyák már chip található, valamint fejlett titkosítással rendelkeznek, így nem lehet őket lemásolni vagy klónozni. Olyan területeken fontosak, amik rendkívül érzékenyek egy esetleges illetéktelen behatolásra. A jogosultságokkal való visszaélések számát nagyban lehet ezekkel csökkenteni. Habár fenntarthatóság szempontjából nem a legjobb választásnak számítanak, a biztonságot tekintve nagyon fejlettek. [60]

Véleményem szerint ebben az esetben a fenntarthatósági kérdés nem előzheti meg a biztonságit.

5.4.7. Mobilos azonosítók elterjedése

Ez a módszer szerintem rövid időn belül el fog terjedni, így a belépőkártyás beléptetést le fogja váltani. Biztonságos megoldást nyújtanak úgy, hogy közben a kényelmi igényeket is kielégítik. A fejlett technológia miatt számos támadásnak lehetnek a jövőben az ellenszerei. [60]

5.4.8. Drónok megjelenése

Mint tudjuk a legnagyobb kiadás a munkáltató számára a munkavállaló. A drónok megjelenésével számos biztonsági személyzet által ellátott feladatot ki lehet váltani. Ilyen feladat lehet például a járőrözés is. Igaz, hogy maga a drón, illetve az ehhez szükségszerűen kialakított infrastruktúra is nagyon drága még, de a megtérülése nagy valószínűséggel bír. Az drónrendszerek kialakítása rendkívül bonyolult feladat és nagyon sok szabálynak meg kell felelni az alkalmazásukkor.

Ebben a fejezetben bemutattam, hogy a biztonsági piacon milyen trendek uralkodnak jelenleg, ezek milyen biztonsági kockázatokkal járnak, valamint azt is, hogy a jövőben a fejlődés milyen rendszereket, eszközöket hozhat magával. Véleményem szerint a jövőben a biztonságtechnikai eszközök nagy része már hálózaton fog kommunikálni, így integrációjuk egyszerűbb lesz, mint jelenleg. A kérdés az, hogy a digitalizációtól való függés kifizetődő lesz-e.

ÖSSZEGZÉS

A szakdolgozatom célja az volt, hogy bemutassam a beléptető, illetve zárrendszerek fejlődését az idők során. Ezek a rendszerek szorosan összefonódnak a modern biztonságtechnika vívmányaival. A trendekről azt lehet elmondani, hogy a mai korra a fizikai védelem és az informatikai rendszerek összhangja, integrált módon biztosítják a szükséges biztonsági szintet. Ezek a technológiai trendek azt is jól tükrözték, hogy a biztonsági megoldások egyre komplexebbé válnak, valamint a felhasználói kényelem kiszolgálása egyre nőtt.

A korai beléptetőrendszerek még nem kommunikáltak egymással, nem lehetett valós időben monitorozni ezeket, de a feladatukat ellátták. A jelenkori változataik azonban már központosított rendszerek, amik több alrendszerrel képesek egy időben kommunikálni. Az integráció lehetővé tette, hogy a jogosultságkezelés gyors és pontos legyen. Emellett a biztonsági szint is sokat fejlődött, ugyanis az eseményeket már valós időben lehetett elemezni. Ezek működéséhez már hálózatra van szükség, valamint több azonosítási módszert is tudnak kezelni, ami lehet birtoklás alapú azonosítás, de akár biometrikus azonosítás is. A biometrikus azonosítás megjelenése nagy ugrást jelentett a technológiában, ugyanis ez lehetővé tette például a belépőkártyák alkalmazásának mellőzését. A biztonságot tekintve is nagy előrelépés volt a technológiában.

A klasszikus mechanikus zárat is érintette a dolgozatom. Ezek a zárok már több évtizedet látják el a feladatukat. Elsődleges előnyük, hogy rendkívül tartósak, használatuk egyszerű és nincsenek hálózatra kötve, így ilyen téren nem érheti támadás őket. A technológia fejlődésével ezek a háttérbe szorultak, ugyanis az elektromos zárok megjelenése megnövelte a biztonsági szintet, valamint használatuk már kényelmesebb volt, mivel nem kellett a fizikai kulcsra figyelni, hanem elég volt akár egy belépőkártya is a működtetésükhöz.

Összességében elmondható, hogy olyan irány alakult ki, ahol a fizikai védelem, illetve a digitális megoldások együtt járnak. A modern biztonságtechnika már nem arról szól, hogy megtudjuk, hogy egy esemény a múltban hogyan történt, hanem arról, hogy az esemény

be se következhesen, mivel a mesterséges intelligencia már képes előre jelezni, ha valami szokatlan helyzetet tapasztal.

Véleményem szerint a jövőt a mesterséges intelligencia különböző felhasználásai fogják meghatározni. Vannak kételyeim az ezen alapuló megoldásokkal kapcsolatban, de ha be tudjuk határolni a működésüket megfelelően, akkor nagyon gyors, kényelmes -ami manapság szinte a legfontosabb- és biztonságos rendszereket fogunk kapni.

SUMMARY

The aim of my thesis was to present the development of access control and locking systems over time. These systems are closely intertwined with the achievements of modern security technology. In terms of trends, it can be said that today, physical protection and IT systems work in harmony to provide the necessary level of security in an integrated manner. These technological trends also reflect the fact that security solutions are becoming increasingly complex and user convenience is becoming increasingly important.

Early access control systems did not communicate with each other and could not be monitored in real time, but they performed their tasks. However, their current versions are centralized systems capable of communicating with multiple subsystems simultaneously. Integration has enabled fast and accurate access control. In addition, security levels have also improved significantly, as events can now be analyzed in real time. These systems require a network to operate and can handle multiple identification methods, including possession-based identification and even biometric identification. The advent of biometric identification was a major leap forward in technology, as it made it possible, for example, to dispense with the use of access cards. It was also a major step forward in terms of security.

My thesis also touched on classic mechanical locks. These locks have been doing their job for decades. Their primary advantage is that they are extremely durable, easy to use, and not connected to a network, so they cannot be attacked in this area. With the advancement of technology, these have been pushed into the background, as the advent of electric locks has increased the level of security and made them more convenient to use, since there is no need to keep track of physical keys; an access card is sufficient to operate them.

Overall, it can be said that a trend has emerged where physical protection and digital solutions go hand in hand. Modern security technology is no longer about finding out how an event happened in the past, but about preventing the event from happening in the

first place, as artificial intelligence is now able to predict when something unusual is about to happen.

In my opinion, the future will be defined by various uses of artificial intelligence. I have my doubts about solutions based on this, but if we can limit their operation appropriately, we will end up with very fast, convenient—which is almost the most important thing these days—and secure systems.

HIVATKOZÁSOK

- [1] L. Dr. Berek, T. Dr. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016.
- [2] „Brandbook,” [Online]. Elérhető: <https://brandbook.hu/2020/06/maslow-piramis>. [Hozzáférés dátuma: 2025.11.10.].
- [3] L. Ropolyi, „Technika és etika,” in *Kortárs etika*, Budapest, Nemzeti Tankönyvkiadó, 2004, pp. 245-292.
- [4] L. Dr. Berek, Biztonságtechnika, Budapest: Nemzeti Közszerológati Egyetem, 2014.
- [5] S. Kiss, „A biztonságtechnika kialakulásának történetéről,” *Hadmérnök*, pp. 24-29, 2015. X. Évfolyam 4. szám.
- [6] H. N. Network, „History News Network,” [Online]. Elérhető: <https://www.hnn.us/article/cavemen-chose-caves-using-five-criteria>. [Hozzáférés dátuma: 2025.11.11.].
- [7] „Wikipedia,” [Online]. Elérhető: <https://hu.wikipedia.org/wiki/Kiskev%C3%A9lyi-barlang>. [Hozzáférés dátuma: 2025.11.11.].
- [8] I. Laky, Szerző, *Biztonságtechnika történet*. [Előadás]. 2023.
- [9] C. Belmonte, „National Geographic,” [Online]. Elérhető: <https://www.nationalgeographic.com/history/history-magazine/article/early-agricultural-settlement-catalhoyuk-turkey>. [Hozzáférés dátuma: 2025.11.11.].
- [10] „National Geographic,” [Online]. Elérhető: <https://www.nationalgeographic.com/history/history-magazine/article/early-agricultural-settlement-catalhoyuk-turkey>. [Hozzáférés dátuma: 2025.11.11.].
- [11] B. Andrásfalvy, I. Balassa, M. Égető, I. Gráfik, B. Gunda, J. Kotics, A. Paládi-Kovács, T. Petercsák, A. Selmeczi Kovács, E. Solymos, J. Szabadfalvi és M. Szilágyi, Magyar néprajz II. - Gazdálkodás, Budapest: Akadémia Kiadó, 2001.
- [12] „Sulinet Tudásbázis,” [Online]. Elérhető: <https://tudasbazis.sulinet.hu/hu/tarsadalomtudomanyok/tortenelem/életmodtorten-et-oskor-es-okor/az-elet-keretei-az-okorban/lakas-es-eletszinvonal-az-okorban>. [Hozzáférés dátuma: 2025.11.11.].

- [13] „Kulturális Örökség Napjai,” [Online]. Elérhető: <https://oroksegnapok.gov.hu/helyszin/1018>. [Hozzáférés dátuma: 2025.11.16.].
- [14] „Pixabay,” [Online]. Elérhető: <https://pixabay.com/hu/photos/bach-lovagok-kast%c3%a9lya-lovagv%c3%a1r-1588788/>. [Hozzáférés dátuma: 2025.11.16.].
- [15] „Blog.hu,” [Online]. Elérhető: https://toriora2.blog.hu/2024/01/18/a_kozepkori_varosok_es_a_reneszansz?utm_medium=doboz&utm_campaign=bloghu_cimlap&utm_source=kult. [Hozzáférés dátuma: 2025.11.16.].
- [16] G. Kákonyi, „Zárak, lakatok,” 1986. [Online]. Elérhető: <https://www.scribd.com/doc/106942406/Kakonyi-Gyula-Zarak-lakatok#page=20>. [Hozzáférés dátuma: 2025.11.16.].
- [17] G. Andriská, „A modern biztonságtechnika kihívásai: eszközüeltartam és technológiai fejlődés,” *Biztonságtudományi Szemle*, pp. 15-24, 2025.
- [18] Á. Bunyitai, „A beléptetőrendszerek helye és szerepe a vagyoncédelemben,” *Hadmérnök*, pp. 17-25, 2011. VI. Évfolyam 4. szám.
- [19] G. Dr. Lukács, A. Döring és P. Hell, *Vagyonvédelmi rendszerek I.*, Budapest: Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kár, 2015..
- [20] Z. Zólyomi, „A biztonság és a biztonságmenedzsment vizsgálata vállalati nézőpontból,” *Hadmérnök*, pp. 19-29, 2020. XV. Évfolyam 1. szám.
- [21] „Tétényi Security,” [Online]. Elérhető: <https://www.tetenyisec.hu/belepteto-rendszerek/>. [Hozzáférés dátuma: 2025.11.17.].
- [22] „Youcard.com,” [Online]. Elérhető: <https://www.youcard.com/products/chip-cards/legic-chip-cards/legic-prime/>. [Hozzáférés dátuma: 2025.11.19.].
- [23] „Youcard.de,” [Online]. Elérhető: <https://www.youcard24.de/de/RFID-Chipkarten-LEGIC-prime-MIM-1024.html?srsId=AfmBOoqRG6KXxwU2KuQa2JvvIhonX0HDkmab26q5nsyWlleLhy9SVRRx>. [Hozzáférés dátuma: 2025.11.19.].
- [24] Á. Bunyitai, „A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból,” *Hadmérnök*, 2011. VI. Évfolyam 1. szám.
- [25] „Dormakaba,” [Online]. Elérhető: https://www.dormakaba.com/hu-hu/ajanlat/termekeink/belepteto-es-bejarati-rendszerek/gyorskapuk/argus-v60-gyorskapu--dk_33100.

- [26] „Dormakaba.com,” [Online]. Elérhető: https://www.dormakaba.com/hu-hu/ajanlat/termekeink/belepteto-es-bejarati-rendszerek/gyorskapuk/argus-v60-gyorskapu--dk_33100. [Hozzáférés dátuma: 2025.11.20.].
- [27] M. Papp, Szerző, *Mobil, mint belépőkártya*. [Előadás]. 2025.10.01..
- [28] „Zartunder.hu,” [Online]. Elérhető: <https://zartunder.hu/zarak-fajtai-es-tortenelme/>. [Hozzáférés dátuma: 2025.11.21.].
- [29] K. Biro, „Promotions.hu,” [Online]. Elérhető: <https://promotions.hu/orszagos/tech-tudomany/2023/09/18/zar-kulcs-tortenelem-okori-egyiptom-piramis>. [Hozzáférés dátuma: 2025.11.13.].
- [30] „Kulturbakancslista,” [Online]. Elérhető: https://kulturbakancslista.blog.hu/2017/02/21/kr_e_2000_mechanikus_zar. [Hozzáférés dátuma: 2025.11.13.].
- [31] D. Gáspár, Zár- és kulcstörténet, Budapest: Múzsák Közművelődési Kiadó, 1986.
- [32] D. Gáspár, Régi kulcsok és záruk, Budapest: Múzsák Közművelődési Kiadó, 1985.
- [33] „Zárbarát.hu,” [Online]. Elérhető: <https://zarbarat.hu/tudta-okori-roma/>. [Hozzáférés dátuma: 2025.11.14.].
- [34] „Historical Locks,” [Online]. Elérhető: <https://www.historicallocks.com/en/site/h/other-locks/19-keys-and-locks-from-imperial-rome/roman-door-locks>. [Hozzáférés dátuma: 2025.11.14.].
- [35] Racsexpress, „Rácsexpressz,” [Online]. Elérhető: <https://ujoldal.racsexpressz.hu/2017/05/31/zar-es-kulcs-tortenete/>.
- [36] I. Elek, „Mechanikus zárszerkezetek a biztonságtechnikában traszológus szemmel,” *Hadmérnök*, pp. 24-32, 2010. V. Évfolyam 1. szám.
- [37] „Biztonságtechnika.hu,” [Online]. Elérhető: <https://web.archive.org/web/20161105033615/http://www.biztonsagtechnika.hu/zarbetet.html>. [Hozzáférés dátuma: 2025.11.22.].
- [38] „Dormakaba,” [Online]. Elérhető: https://www.dormakaba.com/hu-hu/ajanlat/termekeink/vezerkulcsos-zarrendszerek/fogazott-kulcsos-zarak/dormakaba-e-sp--ka_500042. [Hozzáférés dátuma: 2025.11.22.].
- [39] „Forschnit.com,” [Online]. Elérhető: <https://forschnit.com/product-category/magneszar/elektromos-zar/>. [Hozzáférés dátuma: 2025.11.22.].

- [40] „Biztonságtechnika.hu,” [Online]. Elérhető: https://web.archive.org/web/20161102233404/http://www.biztonsagtechnika.hu/elektromos_zar.html. [Hozzáférés dátuma: 2025.11.22.].
- [41] „Power Biztonságtechnika,” [Online]. Elérhető: <https://powerbizt.hu/termek/dorcas-41-2-nf>. [Hozzáférés dátuma: 2025.11.22.].
- [42] „Zartunder.hu,” [Online]. Elérhető: <https://zartunder.hu/okos-zarak-es-a-modern-biztonsagtechnikak/>. [Hozzáférés dátuma: 2025.11.22.].
- [43] „HiSec,” [Online]. Elérhető: <https://hiseczar.hu/blog/okos-zar-amely-ujjlenyomattal-es-egyeb-modon-is-nyithato>. [Hozzáférés dátuma: 2025.11.22.].
- [44] „Zartunder.hu,” [Online]. Elérhető: <https://zartunder.hu/a-zarbetetek-biztonsagisintjei/>. [Hozzáférés dátuma: 2025.11.22.].
- [45] „Kulcskirály,” [Online]. Elérhető: <https://www.fokulcsrendszer.hu>. [Hozzáférés dátuma: 2025.11.22.].
- [46] „Mauer,” [Online]. Elérhető: https://mauer.hu/Azonos_zarlatu_rendszer. [Hozzáférés dátuma: 2025.11.22.].
- [47] „Mauer,” [Online]. Elérhető: https://mauer.hu/Fokulesos_zarrendszer. [Hozzáférés dátuma: 2025.11.22.].
- [48] „Mauer,” [Online]. Elérhető: https://mauer.hu/Vezerkulcsos_zarrendszer. [Hozzáférés dátuma: 2025.11.22.].
- [49] „Mauer,” [Online]. Elérhető: https://mauer.hu/Kozpontizar_zarrendszer. [Hozzáférés dátuma: 2025.11.22.].
- [50] „Zartunder.hu,” [Online]. Elérhető: <https://zartunder.hu/kulcsok-mukodese-es-tipusai-reszletes-attekintes/>. [Hozzáférés dátuma: 2025.11.24.].
- [51] A. Tóth és L. Tóth, Biztonságtechnika, Budapest: Nemzeti Közsolgálati Egyetem Rendészettudományi Kar, 2014.
- [52] „Predor,” [Online]. Elérhető: <https://www.predor.hu/hu/megoldasaink/irodahazaknak>. [Hozzáférés dátuma: 2025.11.23.].
- [53] „LDSZ Biztonságtechnika,” [Online]. Elérhető: <https://www.lds.hu/az-iot-es-a-biztonsagi-rendszerek-azonositok-id-es-beleptetes-208>. [Hozzáférés dátuma: 2025.11.26.].
- [54] P. Ujhgyi, „A biometria elterjedésének elemzése,” *Belügyi Szemle*, pp. 1463-1491, 2023/8.

- [55] A. Sereg, „Index,” [Online]. Elérhető: <https://index.hu/belfold/2023/09/14/biometrikus-azonositas-venaszkenner-ujjlenyomat-arcaazonositas/>. [Hozzáférés dátuma: 2025.11.25.].
- [56] „Detektor Security,” [Online]. Elérhető: https://detektorsecurity.hu/wp-content/uploads/2025/03/DetektorSec_2025_01_egyben_red.pdf. [Hozzáférés dátuma: 2025.11.25.].
- [57] „Európai Tanács,” [Online]. Elérhető: <https://www.consilium.europa.eu/hu/topics/cybersecurity/>. [Hozzáférés dátuma: 2025.11.26.].
- [58] „TeamPassword,” [Online]. Elérhető: <https://teampassword.com/blog/replay-attack-prevention>. [Hozzáférés dátuma: 2025.11.26.].
- [59] „IrányOnline,” [Online]. Elérhető: <https://iranyonline.hu/a-biometrikus-adatok-sebezhetosege-valoban-biztonsagosabb-a-cyberbiztonsag-igy/>. [Hozzáférés dátuma: 2025.11.27.].
- [60] „Honeywell,” [Online]. Elérhető: <https://buildings.honeywell.com/us/en/brands/our-brands/lenels2/news/insights/access-control-trends>. [Hozzáférés dátuma: 2025.11.27.].

ÁBRAJEGYZÉK

1. ábra: Maslow-piramis [2].....	10
2. ábra: Kis-kevélyi-barlang bejárata [7]	11
3. ábra: Nyeregsátor [8]	12
4. ábra: Çatalhöyük [10]	13
5. ábra: Gazdag egyiptomi család birtoka [8]	14
6. ábra: Egyiptomi kézművesek háza [12].....	15
7. ábra: Ókori görög lakóépület [8]	16
8. ábra: Ókori római lakóépület [8]	17
9. ábra: Nagyvázsónyi Kinizsi vár [13]	18
10. ábra: Középkori település részlet [14]	18
11. ábra: Középkori városrészlet [15]	19
12. ábra: Facsapda a középkorból [16]	20
13. ábra: Elektromágnessel működő mechanikai mozgást létrehozó szerkezet [8].....	21
14. ábra: Az eredeti szabadalom [8].....	22
15. ábra: Annunciátor [8]	23
16. ábra: Beléptetőrendszer felépítése [19].....	27
17. ábra: A biztonsági rendszer [20]	28
18. ábra: Legic prime kártya [23]	32
19. ábra: Lectus select olvasó [saját kép]	33
20. ábra: Bosch AMC2 vezérlő [saját kép]	34
21. ábra: Dormakaba Argus V60 gyorskapu [26]	35
22. ábra: Egyiptomi zár [30]	38
23. ábra: Ókori görög záruk [8]	39
24. ábra: Ókori római záruk és egy gyűrűs kulcs [34]	40
25. ábra: Dormakaba standard hengerzárbetét [38]	42
26. ábra: Dorcas-41-2-NF elektromos zár [41].....	44
27. ábra: HiSec okos zár [43].....	46
28. ábra: Azonos zárlatú rendszer [46]	48
29. ábra: Főkulcsos rendszer [47]	48
30. ábra: Vezérkulcsos rendszer [48]	49
31. ábra: Központi zárrendszer [49]	50
32. ábra: Integrált vagyonvédelmi rendszer [51]	53
33. ábra: Transzponderes karkötő [1]	56
34. ábra: Érhálózat alapú azonosítás [55]	62