

XXXI. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2013. április 16-18.
Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

A BÁNKI DONÁT KAR SZEMÉLYI BELÉPTETŐ RENDSZERÉNEK BIZTONSÁGTECHNIKAI SZEMPONTÚ ELEMZÉSE

Szerző: Lindmayer Andrea
Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai
Mérnöki Kar

Konzulens: Dr. Szűcs Endre, adjunktus
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,
Biztonságtechnikai Intézet

Tartalomjegyzék

BEVEZETÉS	2
A TÉMA AKTUALITÁSA	2
A KUTATÁS- CÉLJA.....	3
1. A BELÉPTETŐ RENDSZEREK RÉSZEI.....	4
1.1. FOGALOM MEGHATÁROZÁSOK.....	4
1.2. A BELÉPTETŐ RENDSZER FŐ RÉSZEI	5
1.2.1. Kapuk, vagyis az áthaladást szabályzó eszközök	5
1.2.2. Olvasók és kapcsolódó eszközök	6
1.2.3. A felügyeleti rendszer	12
2. A KAR BELÉPTETŐ RENDSZERE.....	15
2.1. A RENDSZER SZÜKSÉGESSÉGE, FŐ FELADATA	15
2.2. A BIZTONSÁGTECHNIKAI RENDSZER ELEMEL	15
2.3. A BELÉPTETŐ RENDSZER RÉSZEINEK RÉSZLETES ISMERTETÉSE, MŰKÖDÉSE A GYAKORLATBAN.....	15
2.3.1. Az áteresztés eszközei	16
2.3.2. Az olvasók típusai, működésük	20
2.3.3 A rendszerfelügyeletet ellátó szoftver	26
2.4. AZ EGYES ESZKÖZÖK MŰKÖDÉSI SEBESSÉGE, FELLÉPŐ HIBÁK, ÁTERESZTÉSI SZÁMÍTÁSOK	28
3. A VIZSGÁLT RENDSZER ELŐNYEINEK ÉS HÁTRÁNYAINAK PÁRHUZAMBAN ÁLLÍTÁSA.....	31
3.1. A KARON ELHELYEZETT RENDSZER ELŐNYEIRE ÉS HÁTRÁNYAIRA VALÓ RÁVILÁGÍTÁS ..	31
3.1.1. Előnyök.....	31
3.1.2. Hátrányok	32
3.2. KÖVETKEZTETÉSEK, JAVASLATOK.....	33
BEFEJEZÉS	36
IRODALOMJEGYZÉK	37
TÁBLÁZATJEGYZÉK	38
KÉPJEGYZÉK.....	39

BEVEZETÉS

A téma aktualitása

A XXI. század információs társadalom működésének fontos eleme a vagyonvédelem, melynek többek között részét képezik a beléptető rendszerek. Ezen a rendszereknek kiemelt a szerepük a különböző rendeltetésű épületek – legyen szó akár irodaházakról, iskolákról vagy éppen nemzetbiztonsági és nemzetgazdasági szempontból fontos objektumokról – védelmében. Napjainkban a beléptető rendszerek elsődleges feladata az illetéktelen személyek belépésének megakadályozása a védett területre, a személyforgalom kontrollja, nyilvántartása, valamint a vendégforgalom zavartalan és zökkenőmentes lebonyolítása, ellenőrzése, nyomon követhetősége.

A beléptető rendszerek tervezése előtt figyelembe kell venni, hogy az adott rendszer milyen feladatok ellátásának feleljen meg. Különösen hasznos lehet, ha a beléptető rendszer rendelkezik egy központi egységgel vagy a beléptető egységek hálózatba vannak fűzve és egy – akár részben – arra kijelölt számítógéphez csatlakoznak, ahol az erre jogosult személy nyomon követheti az egységek személyenkénti használatát. Így lehetőség van a dolgozók mozgásirányának, hollétének meghatározása az objektumon belül, mivel a rendszerben látható, hogy az illető személy milyen belépési vagy kilépési pontokon haladt át. Ennek előnyét leginkább nagy alapterületű objektumoknál, irodaházaknál, gyártelepeknél lehet érezni.

Manapság minden jelentős objektumnál elvárás, hogy vagyonvédelmének részeként egy olyan rendszer kerüljön kiépítésre, amelynél az ellenőrzésnek megfelelően gyors és megbízható legyen, egyértelműen és minden kétséget kizáróan ki kell szűrnie a belépésre jogosultak körét, nem gátolhatja mozgásukat és a nap 24 órájában működőképes legyen.

Ahogy fejlődött és a mai napig fejlődik a technika, egyre jobban teret nyertek és terjednek azok az azonosítási lehetőségek, melyek teljesen egyediek, nem másolhatók, azaz a biometrikus azonosítás lehetőségei. Ugyan még nem jutott el ez a fajta technológia mindenhova, de a nagy biztonsági fokot megkövetelő objektumokban, mint például a Paksi Atomerőmű, már alkalmazásra kerültek. Ez a technológia egyre jobban teret fog nyerni és a végén talán már csak retinánk, ujjnyomatunk vagy tenyérerezetünk segítségével juthatunk be munkahelyünkre, iskolánkba vagy a bankba.

A kutatás célja

A témám kiválasztása során nagy szerepet játszott az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karon (a továbbiakban: Kar) levő beléptető rendszer napi használata és az ezzel járó kellemetlenségek. Felkeltette az érdeklődésemet, hogy mégis mi állhat ennek a háttérében, ennek következtében biztonságtechnikai mérnök szakos hallgatóként úgy éreztem, fontos lenne ennek a rendszernek a részletes bemutatása, rávilágítva a biztonsági résekre, amelyek az épületben tartózkodók biztonságát csökkentik.

A dolgozat során bemutatásra kerülnek a személybeléptető lehetőségek, illetve a valóságban is üzemben levő rendszer szakmai szempontú ismertetése.

Dolgozatom célja röviden ismertetni és összehasonlítani azokat a kiforrott, széles körben alkalmazott és elfogadott személyazonosítási eljárásokat, amelyeket a jelen kor rendszerei is alkalmaznak. A tanulmányban kitérek az információ-, a tárgy- és a biometria alapú módszerek főbb jellemzőinek bemutatására, azonban terjedelmi okok miatt lehetetlen a beléptető rendszerek átfogó ismeretinek vázolása.

Célom továbbá a beléptető rendszerek egy közérthető, rövid áttekintő összefoglalásának készítése biztonságtechnikai szempontból. Nem foglalkozom azonban az elavultabb, sérülékenyebb, illetve a személyazonosításra kevésbé használatos rendszerek bemutatásával. Dolgozatom során biztonsági szempontból vizsgáltam a Kar beléptető rendszerét, előnyeinek és hátrányainak kiemelésével, melyhez önállóan végzett mérések segítségét vettem igénybe. A vizsgálat eredményeinek segítségével a jövőre vonatkozó, hatékonyságot növelő javaslatokat fogalmazok meg, ezzel hozzásegítve a szakértőket a rendszer fejlesztéséhez és a biztonság maximalizálásához.

1. A BELÉPTETŐ RENDSZEREK RÉSZEI

Ebben a fejezetben a beléptető rendszerekhez kapcsolódó legfontosabb fogalmakkal, illetve a rendszer részeivel foglalkozom részletesen. Az eszközök, elemek bemutatása nem teljeskörű, mert a feldolgozandó témában nem jelent meg minden olyan elem, amely a biztonságtechnika szakterületén elérhető.

1.1. Fogalom meghatározások

A dolgozat témájának könnyebb megismerése érdekében az alábbi meghatározásokat használom fel.

Beléptető rendszer: „Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését.”¹

„A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!”²

Automatikus: amely emberi beavatkozást nem igényel, ide sorolható például az ujjnyomat azonosítás vagy más biometrikus eljárás is, mely során az összehasonlítást a számítógép végzi. Nem sorolható ide a fényképes igazolvány alapján való azonosítás, amelyet az arra kijelölt személy végez.

Azonosítás: személy vagy tárgy azonosságának vagy különbözőségének megállapítása.

Személyazonosítás: az az eljárás, mely során minden kétséget kizáróan, egyértelműen megállapítható az egyén kiléte, vagyis, hogy valóban az-e, akinek kiadja magát.

Biometrikus azonosítás: a személyazonosítás egyik fajtája, az ember egyéni biológiai jegyein, élettani vagy viselkedési jellemzőin alapuló azonosítási eljárás. [1]

¹ Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személy azonosítási eljárásai biztonságtechnikai szempontból, Hadmérnök , VI. évfolyam 1. szám, 2011 március, ISSN 1788-1919 , 2011. 09. 01.

² Ugyanott : 4. oldal

1.2. A beléptető rendszer fő részei

Az alábbiakban a rendszerben található eszközök – mind fizikai, mind szoftveres eszközök – kerülnek részletes ismertetésre, elsőként a felügyeleti rendszer, annak elemei és fő feladatai.

Az **olvasó(k)** feladata, hogy azonosításra alkalmas adatokat szolgáltatson a rendszer felé. A **vezérlő(k)** feladata, hogy az olvasóról beérkező adatok alapján eldöntse, hogy az adott személy az adott időpontban adott irányban jogosult-e az áthaladásra, valamint működtesse, felügyelje az áteresztés eszközeit (a továbbiakban :APAS³) és a naplózást.

A **felügyeleti rendszer** feladata a rendszer ellenőrzése, a vezérlő egységek működtetése és a jogosultságok eldöntése, továbbá az események rögzítése, listázása. A felügyeleti szoftver rendszerstruktúrája alapján lehet online vagy offline rendszer. *Online*-nak nevezünk egy beléptető rendszert, ha folyamatosan kapcsolatban van a felügyeleti rendszerrel. *Offline*-nak hívunk egy beléptető rendszert, ha nincs folyamatos kapcsolata a rendszerrel, vagyis nem online.

Az **APAS** feladata, hogy kizárólag az arra jogosultak belépését tegye lehetővé (jogosulatlan személy be/ki lépésének akadályozása mechanikus vagy elektromechanikus eszközökkel), szingularizáció azaz egy azonosítás, egy áthaladás ezeken túl a gátló-szerkezet állapotának (nyitott, zárt, stb.) megállapítása. [1]

1.2.1. Kapuk, vagyis az APAS eszközök

Az APAS feladata, hogy az olvasó által beolvasott, illetve a központi szoftver által visszaigazoltan elfogadott személy számára biztosítsa a fizikai áthaladást. Mindamellet gátolja a fizikai áthaladást abban az esetben, ha az illető nem jogosult rá. Tehát összefoglalva a kapuk az objektumban tartózkodók fizikai közlekedését befolyásolják. Az APAS eszközök működése szempontjából lehet életvédelmi (fail safe) vagy vagyonvédelmi (fail secure). Életvédelmiről akkor beszélhetünk, ha tápkimaradáskor az eszköz állapota nyitott, vagyis szabaddá válik a menekülési út. Tehát ebben az esetben az elsődleges szempont az emberélet védelme. Míg vagyonvédelmiről abban az esetben beszélhetünk, ha tápkimaradás esetén az állapota reteszelt, ekkor az elsődlegesen védendő dolog maga a vagyontárgy.[1]

Az áteresztés eszközei csoportosíthatók továbbá fizikai megjelenésük szerint is, ez az alábbiakban olvasható.

³ Access Point Actuators and Sensors angol kifejezés rövidítése, melynek magyar megfelelője az áteresztést szabályzó eszközök

Elektromos zárral ellátott ajtó: ide azok az ajtók tartoznak jellemzően melyek a központi tértől, folyosótól elválasztanak egy kisebb, szeparált helységet. A zárás történhet mágneszárral, elektromotorral vezérelt zárral, elektromágneses ajtórögzítővel, ajtóbehúzó hidraulikával illetve automatizált ajtómozgatóval – területi okok miatt – a dolgozat során nem tértek ki.

Forgóajtó: ez esetben az áteresztés egyenként történhet vagy több személy haladhat át egyszerre. Ezen eszközök vagy szabadon futóak, vagyis működtetésük kézzel történik, vagy motorral hajtottak – ebben az esetben a forgó mozgást egy motor végzi. Ha az ajtó motorral hajtott, szükséges felszerelni érintésérzékelővel, így az ajtólap érintésekor az automatikus mozgás megszűnik, és az ajtó megáll. Többféle kivitelben forgalmazták ezeket az eszközöket, fix ajtótáblával, mely nem hajtható össze és összehajtható ajtótáblával. Egy veszélyhelyzet esetén gyorsabban végezhetjük a kiürítést, ha az ajtószárnyak automatikusan összehajthatók.

Zsilip rendszer: ebben az esetben két darab ajtón kell áthaladni az adott személynek. Az első ajtón való áthaladás után csak akkor haladhat át a másodikon, ha az első zárt állapotban van és a második ajtó nyitásához is van jogosultsága. Ez a megoldás magasabb védelmet nyújt az előzőekben felsoroltakhoz képest. A zsilipbe (a két ajtó közötti térész) akár súly-, magasság- vagy fémdetektor beépítése is lehetséges ezzel tovább növelve a biztonságot és még inkább kiszűrve a nem kívánt behatolót.

Sorompóval megvalósított áteresztés: történhet lengőkaros, forgókeresztes, lebillenő ágú illetve szétnyíló karú sorompóval. Ezzel az eszközcsoporttal későbbiek során foglalkozom részletesen.

1.2.2. Olvasók és kapcsolódó eszközök

A beléptetés során fontos szerepet töltenek be az olvasók és az azonosító jelet hordozó eszközök. Ebben a fejezetben ezek részletes ismertetésére kerül sor.

A beléptetési folyamatban kiemelt szerepet játszik az antipassback. Az **antipassback** jelentése az azonosító áthaladása utáni visszaadásának megakadályozása. Segítségével nincs lehetőség ugyanazzal az azonosítóval újbóli belépésre, ez különösen ideiglenes jogosultság esetén fontos. Az antipassback **fajtai:**

- a logikai, amely nem engedélyez egymás után azonos irányú mozgásra,
- az időzített, mely adott időn belül nem ad lehetőséget az újbóli áthaladást,
- a területileg ellenőrzött, amely csak a rendszer által nyilvántartott helyről engedélyezi az áthaladást.

A beléptetés folyamata:

- azonosítás,
- a jogosultság eldöntése,
- APAS működtetése, naplózás,
- áthaladás,
- következő azonosító fogadása.

Kétféle azonosítási módot különböztethetünk meg algoritmus szerint: pozitív és negatív kiválasztáson alapulót. ***Pozitív kiválasztás***nak nevezzük, ha a rendszer a belépőtől kapott azonosító információkat csak az adatbázisban hozzá rendelt adatokkal veti össze („biztosan Ő az?”). ***Negatív kiválasztás***nak nevezzük, ha a felhasználótól a belépéskor kapott információkat a teljes adatbázisban keresi, vagyis visszalépéses keresési algoritmust használ („ki az?”).

Könnyen belátható, hogy a pozitív kiválasztás sokkal gyorsabb – mivel nem kell a teljes adatbázist vizsgálni – hátránya, hogy meg kell határozni, hogy milyen azonosítót rendeljünk az egyes személyekhez (például kártya száma, ujjnyomat stb.). Több mutató áll rendelkezésre az azonosítási módok minősítésére. Ezek a következők:

- Hamis Elfogadási Hányad – False Accepting Rate – (a továbbiakban FAR): megmutatja, hogy milyen arányú a hibásan elfogadott jogosulatlan általi hozzáférései kísérleteinek száma.
- Hamis Elutasítási Hányad – False Rejecting Rate – (a továbbiakban FRR): megmutatja, hogy mekkora arányú az elutasított jogosult felhasználók száma.[1]

A személy azonosítás módszerei

A személy kilétének megállapítására többféle eljárást dolgoztak ki, ezeket 3 fő csoportba sorolhatjuk:

- tudás (információ) alapú,
- birtokolt tárgy alapú,
- biometrikus tulajdonság alapú azonosítás.

„Egy beléptető rendszer biztonsága a felismerés osztályozásán és a jogosultság osztályozásán alapul.”⁴ Az azonosítás biztonságának fokozásának érdekében célszerű a fentiek kombinálása.

⁴ Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személy azonosítási eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. évfolyam 1. szám, 2011 március, ISSN 1788-1919, 2011. 09. 01.

Az MSZ-EN 50133:2006 Riasztórendszerek. Beléptető rendszerek biztonságtechnikai alkalmazásokhoz, 1. rész: Rendszerkövetelmények szabvány négy felismerési osztályt határoz meg:

- 0.: azonosítás nélküli,
- 1.: a felhasználó által ismert információ alapján,
- 2.: azonosító tárgyon vagy biometrián alapuló,
- 3.: azonosító tárgyon vagy biometrikus azonosítón túl információ is szükséges az azonosításhoz.

A biztonságos programozhatóság érdekében „a különböző lehetséges kódok száma és a jogosult személyek száma közötti arány legalább 1000:1 legyen illetve a különböző kód változatok száma legalább 10.000 legyen”.⁵ A 2. és a magasabb szintű felismerési osztály esetén legalább 106 db eltérő felismerési kód kezelhetőségére van szükség, FAR<0,01% és FRR<1%. A „jelkulccsal vagy biometriával kapcsolatban használt személyes kód esetén”⁶ minimum 10.000-ret kell tudnia kezelni a rendszernek.

Amennyiben a beléptető rendszer valamely része egy behatolás-jelző rendszer részét képezi, ennek a résznek a behatolás-jelzési szabványok vonatkozó követelményeit is ki kell elégítenie. Kockázatfokozatok alapján meghatározott eltérő számú minimális kódvariáció vagy fizikai kulcs javasolt. Megkülönböztethető: alacsony, alacsony és közepes közötti, közepes és magas közötti és magas kockázat. Alacsony kockázat esetén minimum 1.000 eltérő kódot vagy minimum 300 fizikai kulcsot; magas kockázat esetén minimum 1.000.000 kódot vagy 100.000 fizikai kulcsot kell tudni kezelnie a rendszernek. A pontos meghatározások és értékek megtalálhatók a vonatkozó szabványban. [1]

Azonosítás felhasználó által ismert információ alapján

Ez jellemzően a numerikus személyi azonosító szám, amely általában 4, 6, 8 jegyű decimális szám hosszúságú, illetve meghatározott hosszúságú alfanumerikus jelsorozat, mely minimum 5 karakter hosszú.

A 4 digit hosszúságú numerikus kód variációnak száma $V_{nk,i} = nk$ képlet alapján 104. Ebből következően a 6 digit hosszúságú kód variációinak száma 100-szorosa, a 8 digitésé 10.000-szerese a 4 digitésének. Az alfanumerikus karakterekből álló jelszavak esetén, ahol az angol ABC 26 betűjét és a tíz számot alapul véve, 5 karakter hosszúságú kódsorból $(26+10)^5 = 60.466.176$ féle verzió hozható létre.[1]

⁵ Ugyanott: 7. oldal

⁶ Ugyanott: 7. oldal

Azonosítás birtokolt tárgy alapján

Az azonosító eszközzel szemben támasztott követelmények a következők, személyhez köthető,

- másolás és hamisítás ellen védett,
- hordozza az adott beléptető rendszer és az eszköz tulajdonosára jellemző információkat,
- kis méretű,
- könnyen kezelhető,
- a sorozatban gyártható,
- a környezeti behatásokat adatvesztés nélkül elviselő,
- esztétikus és olcsó legyen.

A modern beléptető rendszerek között napjainkban a beléptető kártyás rendszerek a legelterjedtebbek. A beléptető kártya alapvető feladata, hogy hozzájáruljon az áthaladás elősegítéséhez azokon a beléptető kapukon, amelyeken a kártya tulajdonosa jogosult be, vagy kijutni. Használata egyszerű és kényelmes. Megjelenését tekintve lehet karóra formájú, kicsi kör alakú – ezt tarthatjuk nyakba akasztva, vagy akár a kulcstartónkon is –, és lehet egy bankkártya méretű téglalap alakú kártya, amit szintén nyakba akasztva, vagy a többi kártyánk között, például a pénztárcánkban tárolhatunk.

Itt fontos megemlíteni az eszközök biztonságát. Alapvetően négyféle típus különböztethető meg adat- és információvédelem szempontjából. Ezek lehetnek:

- Nyílt (open): egyszerű fix kód, olvasható és értelmezhető.
- Kódolt (encoded): a kód kiolvasható és másolható, de csak a kulcs segítségével értelmezhető.
- Adathozzáférés védett (password protected): jelszóval elérhető. A kód egy olvasó és hozzá tartozó kártya birtokában visszafejthető.
- Titkosított (encrypted): az adatokat csak a címzett tudja olvasni.

Alkalmazható szimmetrikus kulcsú algoritmus (a titkosításhoz és a visszafejtéshez ugyanazt a kulcsot használja). Az algoritmus paraméteréül 112 bites kulcs szolgálhat.

Használható továbbá nyílt kulcsú algoritmus is ez lehet a Data Encryption Standard (a továbbiakban DES⁷), Three- Data Encryption Standard (a továbbiakban 3-DES⁸) stb. adattitkosítási algoritmus, amelyek tárgyalása azonban ennek a tanulmánynak nem célja.

⁷ Helyettesítéses-permutációs blokkrejtjelező. 64 bites blokkos rejtjelezés, vagyis a nyílt szöveg egy 64 bit méretű blokkjához rendel egy ugyanakkora rejtjeles blokkot.

A beléptető kártyák fajtái esetén a működésüket tekintve beszélhetünk passzív, vagyis amelyek csak adatot hordoznak, de információt nem küldenek, illetve beszélhetünk aktív kártyákról, melyek nem csak adatot tárolnak, hanem kommunikálnak is az olvasóval a bennük található mikrokontroller segítségével.

Lyukkártya: manapság már nem használatos kártyafajta, mely esetén az információt a lyukak hordozták, amelyek jelentését egy mindenkori kódtáblázat tartalmazza.

Vonalkódos kártya: létezik belőle $1D^9$ (egy dimenziós), $2D^{10}$ (kétdimenziós), illetve a Quick Response (a továbbiakban QR¹¹) kód. Az $1D$ -s kártyák egy dimenzióban tárolnak csak adatokat, ahhoz, hogy az olvasó értelmezni tudja, az egész kódsort látnia kell. A $2D$ -s kártyák már két dimenzióban tárolnak adatokat, így több információ fér el rajtuk. A QR kód skálázható, bármely szögből azonosítható, azaz nagy adattároló képességű.

Induktív kártya: az információkat a kártyán található fém lapok hordozzák. Variációszáma korlátozott.

Mágneskártya: az információt a mágnescsík hordozza. Kapacitása az előzőekhez képest jóval nagyobb. Előnye, hogy programozható. Érzékenysége és gyors elhasználódása okán a mágneskártya rendszeres beléptetésre nem használatos.

Memóriakártya: programozható memória áramkört tartalmaz. Nagy memóriakapacitással rendelkezik, többszörösen átirható. A tárolt adatok kóddal védhetők.

Optikai kártya: nagy memóriakapacitású, a beírt adatok nem törölhetők róla. Az adatok kiolvasása kóddal védhető.

IButton: speciális elektronikus kódkulcs, ami egy garantáltan egyedi azonosítót tartalmaz. Nagyon rövid ideig kell az olvasóhoz érinteni, és ha érvényes az azonosító, a rendszer végrehajtja a hozzá rendelt műveletet. Egyre nagyobb számban terjed. Mivel jól ellenáll a mechanikai hatásoknak, és a folyamatos igénybevételt is kitűnően bírja, ezért élettartama szinte korlátlan.[7]

Proximity kártya (Radio Frequency IDentificant, a továbbiakban RFID): napjainkban a legszélesebb körben elterjedt eszköz, mely sokféle változatban létezik. Alapvetően két félé –

⁸ DES-nél használt kódoló és dekódoló eljárások háromszori megismétlése. Szintén 64 bites adatblokkon dolgozik, de a titkosításhoz a konkrét felépítéstől függően 64, 128 vagy 192 bites kulcsot használ.

⁹ A köznyelv vonalkódként ismeri, különböző vastagságú, függőleges vonalakból álló jelzés, amelyben legtöbbször csak számjegyeket kódolnak, melyeket gyakran a vonalkód alatt fel is tüntetnek. A vonalkódok készítését és visszaféjtését szabvány írja le.

¹⁰ Datamátrix néven is ismert vonalkód típus, Négyzetes elrendezésű nagy sűrűségű kódrendszer. Változó kapacitású kód, helyzetét a négyzetet alkotó keretvonalak határozzák meg. Többfokozatú hibavédelemmel rendelkezik.

¹¹ Hasonló a $2D$ -s kódokhoz, nagy kapacitású, mátrix struktúrájú. Helyzetét a négyzetes struktúra három sarkában található ábrák segítenek meghatározni.

aktív és passzív – proximiy technológiáról beszélhetünk. Ezzel a kártyatípussal a későbbiekben részletesen foglalkozom.

Azonosítás személyes tulajdonság alapján

Ezek jellemzően a biológiai tulajdonságokon alapuló személyazonosító eszközök. Lehet: ujjnyomat-, tenyérynymat-, kézgeometria-, tenyérerezet-, ujjerezet-, írisz-, retina-, testhőkép-, DNS-, hang-, írásazonosító, arcfelismerő.

A biometrikus azonosítás előnye, hogy az azonosító „eszköz” magának a személynek valamilyen biológiai tulajdonsága, ami állandó jelleggel rendelkezésre áll, ezért nem kell egy külön eszközt magunknál tartani. Igaz, hogy ezek az információk nehezen hamisíthatóak, viszont sérülésre érzékenyek, és az idő múlásával változhatnak. További hátránya a biometrikus azonosításnak, hogy a tárolt információ nagyon nagy mennyiségű, ezért nehezebben is kezelhető. Alkalmazása során az azonosítás lassabb, mert sok felhasználó esetén a leolvasott mintát nagyon sok tárolt mintával kell összevetni

Az alábbiakban az azonosítási módszerek rövid összefoglalása olvasható, melyek részletes kifejtésére a területi korlátok miatt nincs lehetőség.

Ujjnyomat: nem hamisítható, viszont sérülésre érzékeny, ezért célszerű több ujjról mintát venni. Hátránya, hogy drága a működtetéséhez szükséges olvasó berendezés. Kb. 95%-os felismerési arány jellemzi.

Tenyérlenyomat: nem hamisítható, de költséges, ezért kevésbé elterjedt. A tenyérynymat alapú azonosításnál a jellemzők például

- a fővonalak,
- a fodorszálak,
- a szövetmintázat.

Arc: hátránya, hogy hamisítható, ezért beléptetésre nem nagyon használják. Alkalmazása inkább repülőtereken jellemző, keresett személyek kiszűrésére.

Retina: Mivel a retina-azonosítás rendkívül nagy pontossággal működő biometrikus technológia, így elsősorban magas biztonsági fokot igénylő alkalmazásokban használják (katonai alkalmazások, pénzügyi intézetek stb.).

Tenyérerezet: speciális (infrához hasonló) fény segítségével a szkennertől 4-5 centiméterre helyezett tenyérrel felvételt készítenek. A bőrfelület alatti erek beolvasás után fekete mintázatot rajzolnak ki, amely az azonosítás alapjául szolgál.

Írisz: A vizsgálat a szívrághártya látható (pl. rajzolat), valamint láthatatlan (pl. infravörös) tulajdonságain alapul. A képet általában közeliről kell készíteni, hogy megfelelően részlet

gazdag legyen, majd meg kell keresni az írisz határait. Ez nem egyszerű, hiszen a kör alakot takarhatják a szemhéjak. Nagy megbízhatóságú módszer, de nagy hátránya, hogy a leolvasáshoz szükséges berendezés rendkívül drága, így kevéssé elterjedt a módszer „hétköznapi” használatban.

Hang: A hanghullámok elemzésén alapul és főleg technikai kérdés a hangmintázat matematikai felbontása. Hátránya, hogy a háttérzaj zavarja, rekedtség, pillanatnyi egészségi állapot befolyásolja, tehát nehéz az egyénre jellemző, de állandó komponensek azonosítása, valamint felvételtől könnyen utánozható.

Kézirás: Az aláírás formai és dinamikai elemzése (nem teljesen biometria, átmenet a tudásazonosítás felé). Megvalósítása még drága, de áttörés várható. Kísérletek kimutatták, hogy bár az aláírást látszólag lehet hamisítani az írási idő, a nyomásdinamika, az alak- és mozgáseltérések másolása lehetetlen. A hibaarány elismert határértéke a jó rendszerek esetében ma kisebb, mint 1 százalék.

Kézgeometria: Jellemzően a kéz geometriai sajátosságait használják az azonosításhoz, nevezetesen:

- az ujjak hosszúságát és szélességét,
- a kézfej szélességét és
- a tenyér / ujjak méretarányát.

Pozicionáló tűskék segítségével határozzák meg a legjellemzőbb geometriai paramétereket: az ujjakat négy tűskéhez illesztik és ezekhez képest 14 tengelyt vesznek fel.

Szag azonosítás: A test illatát adó anyagokat könnyű megszerezni az emberek testéről. Emellett a testszag az étrendtől, betegségektől, érzelmi állapottól erősen függ, percek alatt megváltozhat. Vannak ugyan egyedi szagmolekulák, de ezek variabilitása az emberek között alig ismert, pontos azonosításuk pedig nem megoldott.

DNS: rendkívül megbízható, az egyént pontosan azonosítja, évek múltán is változatlan marad, viszont nagyon könnyen lemásolható mintázat (pl.: hajszálból)[8][9][10]

1.2.3. A felügyeleti rendszer

Ebben az alfejezetben csak érintőlegesen kerül ismertetésre a felügyeletet ellátó szoftver annak sokfélesége, illetve a hely hiánya miatt csupán a fő paramétereket emelem ki, melyek minden rendszerben hasonlóak.

Alapvető elvárás a rendszerrel szemben az, hogy a rendszer kezelje és nyilvántartsa a belépésre jogosultakat, a különböző jogosultsági szinteket, a kezelői jogosultságokat, továbbá

az időkereteket személyekre és csoportokra bontva, a forgóvillák irányfigyelését, valamint szűrőfeltételek szerinti lekérdezéseket biztosítson.

A rendszerek fontos paramétere a rendszerkapacitás, vagyis a felhasználói kártyák száma, azon kívül az áteresztési pontok száma, azaz az olvasóterminálok száma. Ez minden egyes rendszernél változó az adott objektum szükségletei miatt. A felügyeleti rendszer természetesen rendelkezik egy **kezelői felülettel** melyen keresztül a jogosult és arra kiképzett személy vagy személyek kezelik azt.[1]

A kezelői szoftver fő jellemzői a következők:

A **belépési profil**: a belépők jogosultsági szintjei adott áteresztési pontokon. A belépési időtáblázatból olvasható ki az adott jogosult mikor lépett be egy adott helységbe, helyesebben mikor távozott onnan. Munkaidő nyilvántartási szempontból fontos adat illetőleg könnyen nyomon követhetők így a személyek.

Az **eseménykezelés**: az áteresztési pontok, a kívánt szolgáltatások, például kétkártyás üzemmód, ajtónyitás riasztások, tűzriasztás kezelése tartozik ide. Ez történhet automatikusan, vagyis kezelői beavatkozásra. Például a rendszer jelez a kezelőnek, hogy egy védett helyre illetéktelen akar belépni, a rendszer nem engedi be, de a tényleges beavatkozást a kezelő teszi meg, odaküldi például az őrszolgálatot. Míg egy zsilipes áteresztés esetén lehetőség van arra, hogy a jogosulatlant beeressze a szoftver majd „bezárja” a zsilipbe, amíg az őrszemélyzet megérkezik.

Hozzáférési szintek: beállítható, hogy az egyes kezelők milyen szintű hozzáféréssel rendelkezzenek. Például aktiválni tudjon egy új kártyát vagy csak nyomon tudja azt követni. Jellemzően 2-4 személy rendelkezik teljes hozzáférési szinttel egy rendszer esetén.

Kártya vagy egyéb azonosító eszköz érvényesítése, kivonása: mint azt az előzőekben említettem, ehhez nincs minden kezelőnek jogosultsága, így bármikor bárki nem tud azonosítót aktiválni vagy deaktiválni. Az azonosító eszköz felvitelekor (vagyis aktiváláskor) az eszközt személyhez kell kötni, ez történhet név, beosztás, cím vagy születési év alapján. Jellemzően több adat alapján teszik azonosíthatóvá a kártya tulajdonosát, hisz nemegyszer fordul az elő, hogy egy munkahelyen több azonos nevű dolgozó dolgozik, így őket meg kell különböztetni.

Naplózás: ehhez a szolgáltatáshoz csak a rendszert felügyelő, vagyis jogosult személy férhet hozzá. A szoftver naplózza a rendszer beállítási paramétereit, a kezelők tevékenységét, a rendszerben történt eseményeket és a riasztásokat.

További szolgáltatások, modulok, amellyel a rendszer szükség esetén bővíthető:

- dolgozók munkaidő nyilvántartása,

- gépjármű beléptetés,
- portai modul: a vendékkártya leadásra egy hangüzenet figyelmeztet, igény esetén vendékkártya elnyelő oszlop illeszthető a rendszerhez,
- véletlenkiválasztó modul (motozás),
- tűzjelző rendszerhez történő illesztés,
- fizetős és egyéb szolgáltatások igénybevételének kezelése, (pl. étterem, fénymásoló stb.),
- öltözőszekrények nyitása, zárása,
- helyszínrajz megjelenítés,
- személykeresés,
- arckép megjelenítés.

2. A KAR BELÉPTETŐ RENDSZERE

A következőkben a Kar épületében található beléptető rendszert ismertetem részletesen, feladatainak és eszközeinek kiemelésével.

2.1. A rendszer szükségessége, fő feladata

Az elmúlt időszakban sajnálatos módon megszorodtak az intézményben a vagyonellenes cselekmények, így az ezek elleni fellépés eszközeként a kar vezetése biztonságtechnikai fejlesztésre szánta el magát, amely képes ellátni a videó-megfigyelés és a beléptetés feladatait. Tehát ez a beléptető rendszer is elsősorban ellenőrzési feladatot lát el. Működése során ellenőrzi a karra belépő és az onnan kilépő személyeket, valamint gépjármű ellenőrzést végez. Összefoglalva a Kar épületében található beléptető rendszer fő feladata az illetéktelen személyek kiszűrése és ez által az esetleges bűncselekmények megakadályozása.

2.2. A biztonságtechnikai rendszer elemei

A személyi beléptetés (Népszínház utca) három, forgóvillás beléptető ponton keresztül valósul meg. A beléptetés mindhárom helyen biometrikusan (akik hozzájárulnak biometrikus adataik felvételéhez ujjnyomat, illetve az egyik villánál kézerezet), vagy különböző fizikai megjelenésű proximity kártyával (lap, kulcstartó, stb.) történik. A forgóvillákon kijáratirányban nincsen azonosítás (szabadon-futó üzemmód), azon felül kiegészítésképpen lengőkapuk is elhelyezésre kerülnek az esetleges gyors épületelhagyás érdekében.

Gépkocsik számára a beléptetés (Kisfaludy utca) rendszámfelismerés révén automatikusan, vagy egyszeri belépési engedély alapján kerül megvalósításra egy gyors működésű kapun (nyitás kevesebb, mint 3 másodperc) keresztül. A kiléptetés azonosítás nélkül, automatikusan történik. A gépjárművek beléptetése – hely hiányában – nem témája ennek a tanulmánynak.

2.3. A beléptető rendszer részeinek részletes ismertetése, működése a gyakorlatban

Ebben az alfejezetben a 2.2. alfejezetben már említett eszközök részletes bemutatására kerül sor, amely során típus szerint ismerhetők meg az egyes eszközök és műszaki paramétereik.

2.3.1. Az átérésztés eszközei

Forgóvillák

A kar épületében három darab forgóvilla van elhelyezve. Kettő a földszinti aula irányában, illetőleg egy villa a bejáráshoz képesti bal mellékfolyosón került elhelyezésre.

A beszerelt eszközök Gunnebo márkajelzésűek. Mindhárom forgóvilla háromágú, ejtőkar funkcióval ellátott szerkezet. Mindegyik képes kétirányú üzemmódra, belépés során szükséges az olvastatás, míg kilépés során szabadonfutó üzemmódba vannak állítva.

Az alábbiakban a Gunnebo SlimStile BA típusú forgóvilla kerül bemutatásra, melyből két darab lábon álló (1. kép) azon kívül egy darab falra szerelt (2. kép) készülék került beszerelésre a Karon.



**1. kép Gunn
forgókereszt,
Készítet**

**2. kép Gunnebo SlimStile BA
forgókereszt, falra szerelhető kivitel,
Készítette: A Szerző**

Ez egy kompakt és költséghatékony bejárási megoldás, működése sima és csendes. A használat során fellépő kopás minimálisnak tekinthető, és alacsony fogyasztása alkalmassá teszi a használatát olyan területeken, ahol nagy számú az áthaladó emberforgalom, így ideális nagy forgalmú területeken.

A készülék műszaki adata a következőkben olvashatóak. A berendezés rozsdamentes acél kivitelű, a ház és fedele 304-es szemcsés rozsdamentes acélból készül. Az állványzati agy öntött alumínium festett szürke felülettel, míg a karok 304 polírozott rozsdamentes acélból vannak. A készülék méreteit tekintve elmondható, hogy 950 mm magasságú, 520 mm szélességű valamint karjainak hossza 480 mm, átmérőjük 38 mm. Az kereszték kézi működtetésűek, vagyis a „zöld” jelzést követően a belépő személynek kell a kart 120°-al elfordítania az áthaladása érdekében. Ez mind a be mind a kiléptetés során manuálisan – áthaladó személy által – történik.

Az áthaladást a központi rendszer jelzésére továbbá nyomógomb hatására engedélyezi, egyszerre egy ember áthaladása lehetséges csak, így akadályozva meg az illetéktelen áthaladást. A kapu állapota a led kijelzőn jelenik meg (szabad, nem szabad) a bemeneti, valamint a kimeneti oldalon egyaránt. Vészhelyzet esetén a karok automatikusan függőleges helyzetbe kerülnek, így biztosítva a könnyebb, gyorsabb áthaladást. A kijelző mindkét irányban elektronikusan vezérelt. Lehetőség van alapértelmezetten nyitott állapotba (a kereszt szabadon forgó) állítani a keresztet, ebben az esetben, ha a belépés jogosulatlan a kereszt nem fordítható át. Ez a beállítás jóval energiatakarékosabb, és vész esetén akár ejtőkar funkció nélkül is gyorsan és hatékonyan ki lehet üríteni az adott helységet. Az alapértelmezetten zárt esetben, a kereszt nem szabadon futó állapotban van, jogosult áthaladás esetén nyit a zár és a kereszt 120°-os fordulatot tesz.

Az elektromechanikus fej mechanizmusa a következőképpen írható le: egy időpillanatban egy személy áthaladása lehetséges. Az áthaladás maximálisan megengedett ideje 5 másodperc, vagyis a szabad jelzést követően a belépő személynek 5 másodperc áll rendelkezésére, hogy a kart 120°-al elfordítva áthaladjon a kapun. Önbeállítóval rendelkezik, amely biztosítja az áthaladás (kar átfordítása) után alaphelyzetbe való visszaállást. Tehát a karok csak 0, 120, 240, illetve 360°-os szögben állhatnak. A készülék hidraulikus lengéscsillapítóval van felszerelve a zökkenőmentes működés érdekében. Fontos funkció a visszafordítás gátló, amely lehetővé teszi, hogy 60°-nál nagyobb elfordulás esetén már nem lehet a kart visszafelé mozgatni. Áramszünetes esetén a táplálás akkumulátorról vagy szünetmentes tápról történik. Vész esetén a táplálás hasonlóképpen történik, mint áramszünet esetén, de ebben az esetben az épület gyors kiürítése érdekében a karok függőleges helyzetbe kerülnek.

Az eszköz vezérlő logikája a következőképpen épül fel, egy bemenet, mely a bármely irányba való nyitást vagy zárást értelmezi, két védett kimenet szolgál, a nyitás vagy zárás vezérlésére. Négy védett kimenet a mozgás irányát értelmezi, két védett kimenet van kialakítva a számláló számára, két 0V kimeneti relé jelzi az elérhetőséget valamint a használatot, vagy egy számláló számlálja a bármely irányú áthaladások számát. Két nyitott kollektoros NPN kimenet van kialakítva, amely vagy számlálásra, vagy jelzi, a rendelkezésre állást és annak irányát. Mindezek mellett egy védett bemenet tartozik az ejtőkar funkcióhoz. A forgókereszt kommunikációs interfésze RS485.

Alapértelmezetten nyitott állapot esetén (NO) a berendezés tápfeszültsége 230VAC, ezen a feszültségen a rezgése 50Hz, teljesítménye pedig 50VA. A kapu környezeti működési hőmérséklete 0 és 45 ° C között van, ennél alacsonyabb vagy magasabb hőmérséklet esetén a

rendeltetésszerű üzemeltetés nem biztosított. Az áteresztési eszköz IP minősítése IP20, vagyis közepes méretű szilárd tárgyak ellen védett, de víz elleni védelemmel nem rendelkezik. Az MCBF¹² értéke 1,5 ciklus ez körülbelül 2.500.000 átfordulásnak felel meg. A készülék természetesen túlfeszültség és rövidzár ellen védve van. Áteresztési sebessége viszonylag nagy, 40 fű/perc. A fentebb ismertett eszköz műszaki adatait a 1. számú táblázat tartalmazza.

Mivel anyagukat, műszaki adataikat és áteresztési képességüket tekintve a két eszköz tökéletesen megegyezik, csupán beszerelhetőségükben térnek el, így az utóbbiról nem adok részletes ismertetőt.

Kivitel	Háromágú állványos	
Anyaga	Burkolat	304 szemcsés rozsdamentes acél
	középrész	Öntött, festett szürke alumínium
	forgórész	Polírozott acél
	forgókar	304 rozsdamentes acél, 38 mm átmérőjűek és 480 mm hosszúságúak.
Vezérlés (logikai egységgel)	alapfunkciók	Egy-egy bemenet nyitásra/zárásra mindkét irányban.
		Egy védett bemenet az ejtőkar funkcióhoz.
		Két védett kimenet a számlálónak
		Egy kimeneti jel a forgóvilla állapotának jelzésére (foglalt jel).
		Négy védett kimenet a mozgás érzékeléséhez
áramforrás	230VAC	
Környezeti működési hőmérséklet tartomány	0-45° C	
számláló	digitális	
Erőszabályzó	hidraulikus	
Vezérlés	elektromechanikus	
Eljtőkar funkció	van	
Kar működtetése	mechanikusan	
Állapot kijelző	led	
IP védelem	IP20	
Kommunikációs interfész	RS485	
Műveletek száma meghibásodás nélkül	1,5 ciklus (kb. 2.500.000 átfordulás)	

¹² A hibamentes ciklusok száma.

Tűz esetén	Függőleges helyzetbe kerülnek a karok
Túlfeszültség elleni védelem	igen
Rövidzár elleni védelem	igen
Áteresztő képessége	40 fő /perc
Áthaladási idő	5 sec
Olvasási idő	0,5 sec
Követési idő	1 sec
Áteresztési idő	3-5 sec

- 1. Számú táblázat: Gunnebo SlimStile BA forgókereszt műszaki adatai,
Készítette: A Szerző, a Gunnebo SlimStile BA gyártói katalógusa alapján**

Lengőkapu (kasszázár)

A Karon található beléptető rendszerben Wanzl márkajelzésű mechanikus lengőkapuk – más néven kasszázárak- is találhatóak áteresztési eszközként (3. és 4. kép). Ezen kapuk ismertetésére kerül sor a következőkben:



**3. kép Wanzl lengőkapu, Készítette:
A Szerző**



**4. kép Wanzl lengőkapu 2, Készítette:
A Szerző**

A személyi beléptető rendszerekben feladat lehet csomaggal érkező vagy akadályoztatott személyek átengedése egyaránt, melyre a forgóvilla és forgókereszt típusú átjárók nem, vagy csak korlátozottan alkalmasak. E feladat ellátására különösen alkalmas a lengőkapu. A karon található kapuknak az előzőeken túl vész esetén van jelentőségük, amikor is a kapuk automatikus kinyitásával szélesebb keresztmetszet jön létre a menekülők számára, így biztosítva a minél gyorsabb kiürítést.

A működést tekintve a kasszázár manuális működtetésű. Lehetőség van a kapuk lezárására a kapu állványzatán elhelyezett kulccsal zárható zár segítségével. Abban az esetben, ha a berendezés nem lett bezárva a zártok felfelé húzásával, kézzel kinyitható a kapu. Kireteszelés után a kar mindkét irányba elfordítható és mindig a 90° helyzetben reteszelődik.

be, tehát mint befelé mind kifelé nyithatóvá válik. A befelé haladási oldalon tilos jelzéssel van ellátva, míg a kifelé haladási oldalon a haladási irányt jelző jelölés található.

Az áteresztési eszköz műszaki adatai a következőkben olvashatók. A berendezés anyagát tekintve a keret rozsdamentes acél, míg a szárny fehér Dibond panel, komplett jelzésekkel ellátva: bemenni tilos és menekülési út ábra található rajta. Méretei az alábbiak, magasság 108 mm, az oszlop átmérője 60 mm, a kapuszárny hossza 1200 mm-ig állítható és magassága 31 mm. A lengőkapu fentebb ismertetett adatait táblázatos formában a 2. számú táblázat tartalmazza.

Kivitel	egyszárnyú	
Anyag	Keret	Rozsdamentes acél
	Szárny	Fehér Dibond panel, komplett jelzésekkel
Áthaladási szélesség	750-1200 mm	
Méretei	Magassága	108 mm
	Oszlop átmérője	60 mm

**2. Számú táblázat: Wanzl lengőkapu műszaki adatai,
Készítette: A Szerző, a Wanzl gyártó katalógusa alapján**

2.3.2. Az olvasók típusai, működésük

A Karon proximity kártyás és biometrikus azonosításon alapuló olvasók kerültek elhelyezésre. A biometrikus olvasók ujjnyomat (9. ábra), valamint tenyérerezet olvasó (10. ábra). A kar hallgatói és dolgozói vagy proximity azonosító eszközzel, vagy ujjnyomatukkal, illetőleg a kiszolgáló személyzet számára tenyérerezet lenyomattal lehet a létesítménybe belépni. Az ujjnyomat leadása nem kötelező csak kényelmi lehetőséget biztosít a belépők számára.

Ebben az alfejezetben a biometrikus azonosítás módszereit és az ezekhez kapcsolódó, a Karon használatban levő olvasók működését részletezem, továbbá a proximity kártyák működése is kifejtésre kerül.

Mivel a proximity kártya a rádiófrekvenciás azonosítási eszközök közé tartozik, melyek a korábbiakban csak röviden kerültek bemutatásra, így ezekről az alábbiakban részletes ismertetés található. A használatban levő proximity kártyák kódolási módjai nem része a fejezetnek és nem témája a dolgozatnak sem.

A legelterjedtebb eszköz a rádiófrekvenciás azonosító eszköz (RFID, Radio-Frequency IDentification) biztonságossága és érintésmentes használhatósága végett. Felépítése igen egyszerű, egy műanyag tokban antenna és egy mikrokontroller helyezkedik el.

Csoportosításuk:

Működési frekvencia szerint	125 kHz
	13,56 MHz
	430 MHz
	862-956 MHz (UHF)
	2,45 GHz
	Egyéb szabad felhasználású frekvenciák
Olvasási távolság szerint	Contactless <5cm
	Proximity 5-50cm
	Hands free 0,5-2m
	Long range >2m
Energiaellátás módja szerint	Passzív
	Aktív
	Szemi-passzív(BAP, Battery Assisted Passive)
Végezhető művelet szerint	Gyárilag programozott
	Egyszer írható
	Átírható
	Írható/olvasható

3. Számú táblázat, RFID kártyák csoportosítása, Készítette: A Szerző¹³,

Működésükben eltérnek a passzív, az aktív és a szemi-passzív típusok. A passzív kártyák olvasása úgy történik, hogy a kártyát az olvasóhoz közelítve, belépve annak elektromágneses erőterébe, a benne lévő antennában feszültség indukálódik, amely biztosítja a kommunikációhoz és a belső chip működéséhez szükséges energiát. Az aktív tag amint detektálja az olvasó erőterét, saját energiaforrásból sugároz, így nagyobb olvasási távolság érhető el. A szemi-passzív tag a saját működését belső energiaforrásból biztosítja, a kommunikációhoz viszont az olvasó által sugárzott jelet használja (csak reflektál). Zavarérzékenységet tekintve a nagyméretű fém tárgyak vagy azonos frekvencián működő eszközök közelsége zavart okozhatnak az olvasásban.

Előnyei: Nincs fizikai érintkezés az olvasóval, nincs kopás, elhasználódás. Egyszerű érintés útján lépnek kontaktusba a forgalomszabályozó, illetve egyéb olvasó berendezésekkel. A bankkártyákkal együtt hordható a levéltárcában vagy pénztárcában, lehetőségünk van arra is, hogy fényképet, azonosítót, vagy feliratokat helyezünk el rajtuk. Ezzel az elektronikus ellenőrzés mellett vizuális ellenőrzésre is módunk van, ami további felhasználási lehetőségeket biztosít a beléptető kártyának.

¹³ Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személy azonosítási eljárásai biztonságtechnikai szempontból, Hadmérnök , VI. évfolyam 1. szám, 2011 március, ISSN 1788-1919 , 2011. 09. 01.

Hátrányai: A kártyát mindig magunknál kell tartanunk, azt elveszíthetjük, vagy akár el is lophatják tőlünk. Ebben az esetben a kártya azonnali letiltása, és másik kártya igénylése szükséges.

Ujjnyomat azonosítás és a Karon található ujjnyomat azonosító eszköz (Suprema Bioentry Plus)

Francis Galton óta tudjuk és alkalmazzuk, hogy ujjunkon lévő bőr gyűrődéseiből (fodorszálak) kialakult mintázat egyedi és életünk során nem változik. Ez a mintázat – az ujjnyomat – 18 hetes korban alakul ki és a későbbiekben csak a kéz méretbeli változásait követi. Megjegyzendő, hogy az égés, vágás, kopás, marás, stb. során esetlegesen értékelhetetlenné vált mintázat legkésőbb 14-40 napon belül regenerálódik (kivéve, ha mély a sérülés, ekkor viszont egyedi heg képződik).

Az ujjnyomat-típusok lehetnek: boltozat, hurok vagy örvény mintájúak, azonosításhoz a jellegzetes pontjait vizsgáljuk. Ilyen jellegzetes pontok az elágazások, végződések, keresztezések, szigetek, horgok, hidak, stb. Egy ujjnyomaton megközelítőleg 100 jellegzetes pont található. A legtöbb ország 12 (Magyarország 10) sajátossági pont egyezését egyértelmű személyazonosításnak tekint. 12 sajátossági pont és azok egymáshoz viszonyított helyzetének ismétlődése – Osterburg számításai szerint – $1:1,25 \cdot 1020$ valószínűségi.

Ujjnyomat-azonosításkor a berendezés vizsgálja, hogy az ujj élő-e, ez legegyszerűbben az ujjbegy hőmérsékletének és/vagy felületi nedvességének mérésével végezhető. Az ujjnyomat-azonosítók képrögzítőinek főbb típusai és működésük röviden:

Optikai: az ujjat egy LED világítja meg, a képződött kép egy prizmán és egy lencserendszeren jut a CMOS vagy CCD érzékelőhöz.

Kapacitív: a fodorszálak és a bőrredők közti eltérő kapacitást detektálja.

Nyomásérzékelős: a szenzor alatt piezo-elektromos nyomásérzékelő mátrix található, ami detektálja a fodorszálakat.

Hőérzékelős: a redők és a völgyek közti hőmérséklet-különbségek mérésén alapszik.

Ultrahangos: ultrahangot sugároz az ujjra, a visszaverődő hullámokból alkotja a képet.[12][13][14]

Suprema Bioentry Plus ujjnyomat olvasó

Az ujjnyomat azonosító eszközök az egyik leginkább elterjedt biometrikus beléptető azonosítók. Az eszköz keskeny kialakítása miatt kis helyen elfér, könnyen szerelhető. Nagy olvasási sebességgel rendelkezik és könnyen beilleszthető a beléptető rendszerbe.

A készülék ujjlenyomat felismerési folyamata

Az ujjlenyomat redőkből és völgyekből áll. A redő a kiemelkedő csík az ujjlenyomatban, míg a völgy a rés két redő között. Mindenkinek az ujján eltérő mintát alkotnak a redők és völgyek. Az ujjlenyomat felismerés titka éppen ezekben az egyedi mintázatokban rejlik.

Az ujjlenyomat érzékelő szenzorok kétdimenziós ujjlenyomat képet hoznak létre, különböző technológiával. Az érzékelés módjától függően, a szenzorok optikai, kapacitív vagy hőérzékelő kategóriába oszthatók.

Az ujjlenyomat minta numerikus adatok gyűjteménye, amelyek egy ujjlenyomat jellemzőit írják le. Az ujjlenyomat minták a BioEntry Plus memóriájába kerülnek elmentésre, és innen olvassuk ki őket az azonosításkor.

A személyi szabadság megőrzése miatt a Suprema ujjlenyomat olvasók nem mentik el magukat az ujjlenyomatról alkotott képeket, csak a belőlük képzett numerikus adatokat, amelyek az azonosításhoz tökéletesek, de nem lehet belőlük rekonstruálni az egyén ujjlenyomatát. A bevitt nyomat mellé lehetőség van RFID kártyát felvenni, ezzel is növelve a biztonságot. Szükség esetén csak RFID kártyaolvasóként is működtethető a Suprema ujjnyomat azonosító.

Az alábbiakban az eszköz műszaki adatai olvashatóak. A készülékben 128 belépési csoport és 128 időtáblázat hozható létre. Memóriáját tekintve elmondható, hogy 4 MB flash memóriával és 8 MB RAM-al rendelkezik. Olvasója 500 dpi felbontású, mellyel rendkívül részletesen tudja a képet bevinni, így is elősegítve a minél pontosabb azonosítást. Olvasási sebességét tekintve elmondható, hogy 2000 nyomatot képes leolvasni 1 másodperc alatt azon túl 5000 nyomat tárolására képes. Két darab kimenettel rendelkezik az ajtók nyitásához. Processzoráról elmondható, hogy 400MHz-es, 8 bites. A készülék színes ledkijelzővel és több hangszínű hangjelzővel ellátott.

Az olvasó tápfeszültsége 12 V, áramfelvétele maximum 250 mA. Méretei: 160 mm magas, 50 mm széles és 37 mm vastag. Csatlakozás PC-hez Cat5 kábellel, protokollja RS485. Az itt leírt műszaki adatokat az alábbi táblázat tartalmazza.



5. kép Suprema Bioentry Plus ujjnyomat azonosító készülék, Készítette: A Szerző

Tápfeszültség	12V
Áramfelvétel	Max. 250mA
Olvasó felbontása	500 dpi
Ujjnyomat tárolási kapacitás	5000 db
processzor	400 MHz, 8 bit

méretei	Magassága	160mm
	Szélesség	50 mm
	Vastagság	37 mm
Csatlakoztatási PC-hez	Cat5	
Kommunikációs interfész	RS485	
Multicolor kijelző	van	
Multi tone hangjelző	van	
Olvasási sebesség	1 másodperc alatt 2000 nyomat	

4. Számú táblázat: Suprema Bioentry Plus ujjnyomat azonosító műszaki adatai,
Készítette: A Szerző, a Supream Bioentry Plus temékkatalógusa alapján

A tenyérerezet azonosítás

A tenyér erezet azonosítás technológiáját a Fujitsu cég fejlesztette ki. A technológia ötvözi az ujj és tenyérnyomat azonosítás biztonságosságát és az olvasási egyszerűséget.

A kézben levő erek elrendeződése egész életünk során azonos marad, s személyenként egyedi képet mutat. Az olvasás hatékonyságát nem befolyásolja a szennyezett bőr, a külső sérülések, a bőrszín valamint az anyajegyek. A szkennelés során a gép a tenyér érhálózatának képét rögzíti, ebből egy úgynevezett sablont generál, majd ezt a generált sablont menti el. A beléptetés során a már tárolt mintát veti össze a gép a belépés során beolvasottal, s engedélyezi vagy megtagadja az áthaladást. Személyenként az ellenőrzés nem haladja meg az 1 másodpercet. A Karon a Fujitsu által gyártott INTUS 1600 került telepítésre.

INTUS 1600 tenyérerezet azonosító berendezés



6. kép INTUS 1600
tenyérerezet olvasó,
Készítette: A Szerző

Az alábbiakban olvasható a készülék működési elve. A tenyér 3-8 cm távolságban kell tartani a készülék fölött. Az olvasás során a berendezés abszorpciós infravörös fénnel világítja meg a tenyér, mivel míg az oxigéndús vér visszaveri az infravörös fényt addig, az oxigénhiányos vér elnyeli azt. Az érzékelő készít egy képet az infrafény által kirajzolt érhálózatról, s szoftvere segítségével ebből egy körülbelül 0,8-3 kB nagyságú fájlt generál és menti azt úgy, hogy azt valamilyen más azonosító segítségével az adott személyhez köti. Az így mentett file-t a későbbiek során az összehasonlításhoz mintaként használja. Rendkívül nagy pontosság és a biztonság jellemzi: FAR: 0.000 08%, FRR: 0,01%.

Az érintésmentes olvasási technológiájának köszönhetően, higiénikus megoldás. A család, a gép megtévesztése gyakorlatilag lehetetlen. A készülék teljes mértékben integrálható egyéb hozzáférési és munkaidő-nyilvántartási megoldásokkal is. Továbbá nagy előnye a készüléknek, hogy a kézerezet minta mellé lehetőség van PIN kód bevitelére is, így növelve a biztonságot.

Az olvasó műszaki adatai a következők. Az olvasó részt tekintve, az érzékelőt egy polikarbonát kupola védi a környezeti hatásokkal szemben. A Magic Eye kijelző egy RDB led kijelző, mely színének változtatásával jelzi aktuális állapotát a felhasználó számára, úgy, hogy ha az azonosítás rendben van zöldre vált, ha elutasítja az áthaladást (azonosítás nem megfelelő) akkor piros színűvé válik. Az eszköz PC-hez való csatlakoztatása Cat5 kábellel vagy USB-vel lehetséges. Környezeti működési hőmérséklet tartománya +5 °C és +40 °C között van, ezen értékektől való eltérés esetén a hibamentes működést nem garantálja a gyártó. IP minősítése IP30, vagyis kis méretű szilárd tárgyak ellen védett, de víz elleni védelemmel nem rendelkezik az érezetolvasó.

A készülékház 300 mm magas, 140 mm széles, 71 mm vastag, anyagát tekintve fehér alumínium (RAL 9006). A berendezés szabotázs védelemmel ellátott. A vezérlő logikája egy digitális bemenettel és egy digitális kimenettel rendelkezik. Olvasási sebessége kevesebb, mint 1 másodperc. Az itt olvasható műszaki adatokat táblázatos formában az alábbi táblázat tartalmazza.

Érzékelője	Magic Eye (RGB)	
Méretei	Magasság	300mm
	Szélesség	140 mm
	vastagság	71 mm
Anyag	Fehér alumínium, polikarbonát kupola	
Szabotázs védelem	van	
Vezérlő logika	1 digitális bemenet	
	1 digitális kimenet	
PC-hez való csatlakoztatás	Cat5, USB	
Környezeti működési hőmérséklet	+5 ° C ... +40 ° C.	
IP minősítés	IP30	
Beolvasott adatokból képzett file mérete	0,8-3 kB	
Olvasási távolság	3-8 cm	
Olvasási sebessége	<1 másodperc	
FAR	0,00008%	
FRR	0,01%	

**5. számú táblázat: INTUS 1600 tenyérerezet azonosító műszaki adatai,
Készítette: A Szerző, az INTUS 1600 gyártói katalógusa alapján**

2.3.3 A rendszerfelügyeletet ellátó szoftver

A Karon a Roger cég által kifejlesztett felügyeleti rendszer (Roger Access Control System, röviden RACS) került telepítésre. A proximity kártyák rendszerbe való felvitele, azok nyomon követése, egyéb tevékenységek végzése ezzel a szoftverrel történik. A következőkben a szoftver kártyakezelési funkciói és az áteresztési pontokhoz kapcsolódó lehetőségeket tárgyalom csak. A szoftver a következő felhasználói csoportokat különbözteti meg:

- MASTER,
- KULCS korlátlan (ID 1...49),
- KULCS korlátolt (ID=50...99),
- NORMÁL,
- NORMÁL (ID above 1000),
- Select ID.

A felsorolt csoportok közül a NORMAL csoportokat használják csak. Mivel a felhasználók száma meghaladja az 1000 fő-t így az 1001. és e feletti felhasználók a NORMAL (ID above 1000) csoportba kerülnek.

A profilok létrehozásánál miután a csoportok kiválasztottuk a program a következő adatokat kéri:

- Keresztnév,
- Vezetéknév,
- Kártya érvényességének kezdete,
- Lejárat időpontja,
- Kártya száma.

Minden egyes profil esetén a felvitelkor ki kell pipálni az „érvényes felhasználó” checkboxot, ennek elmulasztása esetén a kártya nem kerül érvényesítésre.

A felhasználói profilokkal kapcsolatos tevékenységek:

- Törlés,
- Monitoring,
- Szerkesztés,
- Nyomon követés,
- Események naplózása, visszaolvasása,
- Szűrés.

Ugyan a szoftver képes az ujjnyomatok kezelésére is, de a Karon elhelyezett ujjnyomat olvasó készülékek saját szoftvere lett feltelepítve, ez a Suprema Biostar program.

Az alábbiakban ezt a kezelőfelületet ismertetem a teljesség igénye nélkül. Új felhasználó felvétele esetén az alábbi adatokat szükséges megadni:

- Név,
- csoport,
- telefonszám,
- e-mail cím,
- jelszó,
- felhasználó típusa.

A felsorolt adatok beírása után történhet az ujjnyomat felvétele, ez a rendszerben kiválasztott olvasóval történik. Minden felhasználó esetén egy ujjról kell mintát felvenni.

Ez esetben is lehetőség van a felhasználók nyomon követésére, törlésére, egyéb műveletek végzésére.

Ahogy az már a korábbi alfejezetben olvasható volt a Karon tenyérerezet azonosító készülék van elhelyezve. A nyomatok felviteléhez és kezeléséhez egy harmadik program van használatban, ez az INTUS PS szoftver. Az alábbiakban ismertetem a nyomatok felvételével kapcsolatos paramétereket. Ezek a következők:

- Jogosultsági időszak
- Csoport
- Felhasználó neve
- Minta választása: a minta lehet Normal – ha csak a kézerezet kerül tárolása –, illetőleg lehet Small – a kézerezet mellett RFID kártya is tárolásra kerül
- PIN kód rendelése a profilhoz

A felhasználói profilokkal kapcsolatos tevékenységek a következők:

- Törlés,
- Monitoring,
- Szerkesztés,
- Nyomon követés,
- Események naplózása, visszaolvasása,
- Szűrés.

2.4. Az egyes eszközök működési sebessége, fellépő hibák, áteresztési számítások

Ebben az alfejezetben a már bemutatott eszközök működési sebességeit és a működésük során tapasztalt hibákat elemzem. Áteresztési számítást készítek a forgókeresztekre. A Karon levő beléptető rendszer üzemeltetését a kari Őrszolgálat végzi. A szolgálat tagjaival folytatott konzultáció során úgy nyilatkozott a felelős személy, hogy a lengőkapuval kapcsolatban nem tapasztaltak hibát.

Az ujjnyomat olvasó olvasási sebességét tekintve 2 másodperc. Az ujjnyomat olvasó 70%-os hibaaránnal dolgozik, sajnos okát ez idáig még a gyártó sem tudta megmondani, így a készülék leszerelésre fog kerülni. A tenyérerezet olvasó olvasási sebessége kevesebb, mint 1 másodperc, a használata során kellemetlenséget okozhat, ha nem megfelelően helyezi rá a tenyerét a felhasználó – a tenyér nem pontosan az a része kerül az olvasó fölé, amely rész mintaként fel lett véve- az olvasó elutasítja az áteresztést.

Az alábbiakban a Karon beszerelésre került Gunnebo márkajelzésű forgókeresztek áteresztéssel kapcsolatos adatai láthatóak táblázatos formában. A következőkben a forgókeresztre készített

A következőkben a forgókeresztekre készített áteresztési számolás látható:

Áteresztő képessége	25 fő /perc
Áthaladási idő	5 sec
Olvasási idő	0,5 sec
Követési idő	1 sec
Áteresztési idő	3-5 sec

6. számú táblázat Gunnebo BA forgókereszt adatai
Készítette: A Szerző, saját mérések alapján

A felhasznált képlet a következő:
$$N_a = \frac{N_{\text{áh}} \times T_a}{T_m}$$

ahol N_a az áteresztési pontok száma, T_m a mintavételezési idő, $N_{\text{áh}}$ az áthaladók száma és T_a az áteresztés ideje.

Mivel a Karra járó hallgatók között van más karról érkező és levelezős hallgató is így az áteresztési számításomban csak a Karra járó hallgatókkal és az ott dolgozókat vettem figyelembe. Fontos még megemlíteni, hogy a számításom során a 2011/2012-es tanév órarendje alapján – a tantermek befogadó képessége szerint- a keddi napot figyelve történt a

hallgatók számának kalkulációja. Azért ezt a napot emeltem ki, mert ezen a napon van a legtöbb óra az intézményben azon túl figyelembe kellett venni a hallgatók azon tulajdonságát miszerint a hét elején nagyobb valószínűséggel látogatják az órákat, mint a hét második felében.

Időpont	Hallgatók és óratartók száma
8-9:40	480 fő + 8 fő
9:50-11:30	595 fő + 10 fő
11:40-13:20	759 fő + 17 fő
13:30-15:10	775 fő + 14 fő
15:20- 16:05	275 fő + 6 fő

7. táblázat Hallgatók eloszlása időrendben a 2011/2012. tanév első félévének Keddi napján, Készítette: A Szerző, az egyetem 2011/2012. első félévi órarendje alapján

Ahogy az a 7. táblázatban látható a keddi napot tanórák alapján osztottam fel. Mivel a tanórák 90%-a kétszer 45 perces így a vizsgált időintervallumok is 90 percesek. A táblázatban szereplő hallgatói létszámok a termék befogadó képessége alapján lett kiszámítva. Az óraadók száma a tantermek száma alapján lett számítva. A keddi napon a Karon megforduló hallgatók és tanárok számát – nem beleértve a többi óraadót akik esetlegesen egyéb tevékenység miatt vannak az épületben- összeadva 2939 főt kapunk.

Az említett 2939 fön kívül az épületbe napi szinten lép be 23 fő, akik különböző adminisztrációs tevékenységet folytatnak az intézetekben, így ők napi szinten vannak jelen. A 2939 főt és a 23 főt összegezve 2962 főt kapunk. Meg kell még említeni a kiszolgáló személyzetet – beleértve a portait, a büfé azon kívül a takarító személyzetet – amely még plusz 10 főt jelent. Így elmondhat, hogy a keddi napon a 2011/2012-es félévben 2972 fő lép be a nap folyamán. Figyelembe véve az esetleges megbetegedéseket, késéseket és azt feltételezve, hogy a 2939 hallgatóból nem mindegyiküknek kezdődik tanórája 8 órakor, az áteresztési számításom során a hallgatóknak csupán a 80 %-át veszem figyelembe. Ennek következtében a reggel 7:30 és 8:00 között az épületbe belépők száma 2384 fő.

A 2384 főnek három forgókereszten van lehetősége áthaladni. Az eszközök egyenkénti áteresztési sebessége 40 fő / perc. Tehát elosztva a 2384 főt hárommal, 798 főt kapunk.

A kapott összeget elosztva 40 fővel megkapjuk, hogy az említett 2384 fő 13 perc alatt léptethető be az intézménybe. Mivel az eszközök áteresztési ideje 3-5 másodperc között van azon kívül a követési idejük 0,5 másodperc, 13 perces áteresztési időhöz hozzá kell adnunk

4,3 percet – 5 másodperc + 0,5 másodperc / fővel számolva – így a végleges eredmény 17,3 perc lesz. Itt természetesen feltétezem, hogy minden személy rendelkezik belépési azonosítóval illetve, hogy mindhárom kereszten ez idő alatt csak befelé haladás történik.

Ebben a fejezetben részletes ismertetőt adtam a Kar személyi beléptető rendszerének feladatairól azon túl mint működésük mind műszaki adataik alapján átfogóan bemutattam az intézményben használt eszközöket. A 2.4-es alfejezetben olvasható az elhelyezett forgókeresztek áteresztési számítása és az ezen adatokból a működési sebességre való következtetés.

3. A VIZSGÁLT RENDSZER ELŐNYEINEK ÉS HÁTRÁNYAINAK ÖSSZEHAISONLÍTÁSA

Ebben a fejezetben a már bemutatott rendszer előnyeire és hátrányaira rávilágítok annak érdekében, hogy a megfelelő ismeretek birtokában lehessen megvizsgálni a jelenlegi működési hatékonyságot, illetve a jövőbeni esetleges módosításokhoz megfontolandó javaslatokat nyújtsak.

3.1. A Karon elhelyezett rendszer előnyeire és hátrányaira való rávilágítás

Ebben az alfejezetben a beléptető rendszer előnyeit és hátrányait elemzem, mind biztonsági, mind használhatósági szempontból. Részletes ismertetőt adok a biztonsági résekről, azok rendszerre gyakorolt hatásáról.

3.1.1. Előnyök

Ahogy az már többször említésre került, a Karon a kar anyagi helyzetéhez képest a lehető legmodernebb eszközök lettek felszerelve. Ennek következtében az alapképzésben tanuló had – és biztonságtechnikai mérnökök illetve a mesterképzésben részt vevő biztonságtechnikai mérnököknek lehetőségük van ezen berendezések megismerésére és használatára, mely hozzájárul jövőbeni szakmájuk „testközelből” való megismeréséhez, az eszközök és eljárási módok elsajátításához. A már említett rendszer többi részével is megismerkedhetnek, többek között a zárt láncú kamerarendszerrel azon túl a hátsó bejáratnál található gépjármű-beléptető rendszerrel is. Lehetőségük van a biztonságtechnika szakos hallgatóknak kötelező szakmai gyakorlatukat szakmai felügyelet alatt a Karon tölteni. Előnyként említhetők a biometrikus azonosító berendezések, hisz biztonsági szempontból ezek a készülékek nyújtják a legnagyobb biztonságot „átverhetetlenségük” szempontjából. Ezen modern eszközök még nem terjedtek el széles körben hazánkban, így elmondható, hogy a Kar tartja a lépést a technológiai fejlesztésekkel, kihasználva annak előnyeit és értékeit. Megemlítendő a rendszer „elrettentő” hatása, mivel ha egy idegen belép az épületbe, szembe találja magát a zárt forgóvillákkal és kapukkal ennek következtében esetleges rossz szándékától hamar elállhat, megkönnyítve ezzel a biztonsági szolgálat munkáját és rendeltetése szerint megóvva az épületben található értékeket, továbbá a zárt láncú kamerarendszer által készített felvételek segítségével könnyebben azonosítható a jogtalan belépő.

3.1.2. Hátrányok

Hátrányként első sorban a rendszer áteresztő képességét emelném ki, hogy az már olvasható volt a 2.4. fejezetben hirtelen nagy ember mennyiség esetén az áteresztési idő jócskán a kívánt érték felett teljesít, lelassítva a be- és kihaladást, továbbá negatívumnak tekinthető az áthaladást szabályzó eszközök elhelyezése. Tekintettel az épület adottságaira elmondható, hogy a felszerelt kapuk megfelelő helyre kerültek beépítésre, ugyanakkor a forgókeresztek száma az áthaladók számát tekintve nem kielégítő. Egyébiránt fontosnak tekinthető még az áthaladási idő szempontjából az a tény, hogy a hallgatók a három kapuból az esetek nagy részében csupán kettőt használnak a ki vagy bejutásra – ez az a két eszköz, amelyek az aula irányában vannak elhelyezve. Hasonlóképpen problémát okoz, hogy a már említett két kaput mind be, illetőleg mind kifelé haladásra használják, aminek következtében torlódás lép fel a kapuknál. Egyébiránt ki kell emelnem, a korábban már említett ujjnyomat olvasók olvasóhibáját – túl nagyszámú téves elutasítási arány –, amely jellemzően nagy mennyiségű felvett ujjnyomat esetén jelentkezik – a tapasztalatok alapján 500 felvett profil után kezd érezhetően lassulni az olvasás, míg 1000 bevitt nyomat esetén az olvasási idő 0,3-0,8 másodpercet is igénybe vehet. A másik biometrikus olvasónál ugyancsak jelentkezik olvasási hiba, abban az esetben, ha a felhasználó a tenyerének nem a tárolt mintájának pontosan megfelelő részét helyezi az olvasó fölé, ez megfigyeléseim során többször előfordult.

Másik fontos szempontként emelném ki azt a biztonsági rést, amelyet a forgókeresztek szabadon futó üzemmódja hordoz magában. A beszerelt kapukat tekintve elmondható, hogy az illetéktelen bejutás könnyen véghezvihető. Mivel a forgókereszteken való áthaladás során csupán befelé menet szükséges az azonosítás, míg kifelé haladás irányába a keresztek szabadon futó üzemmódban működnek. Így lehetőség van a kapuk kifelé való 90° elmozdítására a befelé haladás során, azaz be lehet jutni a lengőkapu mellett, ehhez hozzájárul még a lengőkapu zárt állapotban való 6,5 cm-es kilengése is, melyet már nagyon kis erővel elmozdítható. Mindezek következtében, ha az Őrszolgálat nem elég figyelmes vagy a behatoló kellőképpen rafinált, könnyedén bejut az épület belsejébe a rendszert kijátszva.

Szükséges itt megemlítenem, hogy a kétállványos forgókereszt hátoldalán, illetve a falra szerelt forgókereszt fölött a falra rögzítve, jól látható helyen vannak elhelyezve a karok leejtését előidéző nyomógombok. Így ha valaki meg tudja figyelni, hogy a nyomógomb, mely a villák közvetlen környezetében, illetőleg magukon a villákon helyezkednek el a karokat

nyitott helyzetbe állítja, könnyedén átjut a rendszeren, hisz megnyomja a gombot és már bent is van az épületben.

Kisebb hiányosságnak tekinthető, hogy a beléptető rendszer nem egy, hanem három szoftvert használ az azonosító eszközök felvitelére, ez több program kezelésének megtanulását jelenti az Őrszolgálat tagjai számára, azon túl pedig lassítja a profilok felvételének időtartamát. Mindezekon túl kiemelten kell kezeljem a hátrányok között a hallgatók nem megfelelő tájékoztatását – az Egyetem nem minden hallgatója lett informálva arról, hogy a Karon a beléptető rendszer üzembe lett helyezve és a továbbiakban hogy tudnak az épületbe belépni. Ez a hiányosság napi szintű problémát okoz mind a tájékozatlan hallgatók számára mind pedig az Őrszolgálat számára.

3.2. Következtetések, javaslatok

A rendszer elemeinek és működésének vizsgálata után – az előnyök és a hátrányok számbavételét követően – összességében megállapítható, hogy a rendszer feladatának eleget tesz, miszerint ellenőrizhetőek, nyilvántarthatóak és követhetőek az áthaladó személyek. Sajnálatos módon azonban a rendszerrel kapcsolatban több olyan tényező merül fel, amely a már említett feladatának végrehajtását nehezíti. Mindezek kezelésére a biztonsági struktúra esetleges jövőbeni átszervezéséhez, racionalizálásához a következő javaslatokat tenném meg. A kapuk tekintetében megfontolandó lenne a jelenleg működő három helyett négy darabra bővíteni az eszközök számát, a jelenleg felszerelt lengőkapuk helyére – egy plusz kereszt kerülne az aula bal oldalára. Mivel az épületen belül valamint az épületbe gyakori rendszerességgel szállítanak nagy méretű csomagokat – többek között elektronikai eszközöket és egyéb az intézetek számára érkező vagy általuk küldött egyéb csomagokat. Szükséges lenne teljes testes kapuk beszerelése, amellyel kivédhető lenne az illetéktelenek lengőkar melletti bejutása.

Abban az esetben, ha nincs mód új kapukat venni és beszereltetni, a lengő és a forgókapu közé térelválasztó elem beépítésével ugyancsak elkerülhető lenne a kar visszafelé való forgatásával való jogtalan bejutás.

Ahogy az már korábban említésre került, komoly problémákat és torlódásokat okoz, hogy nincs szabályozva a ki- és bejutás áramlásának iránya. Ennek kezelésére az aulával szemben állva jobb oldalra eső két kaput lehetne a bejutásra, míg a baloldalra esőt a kijutásra használni, meggyorsítva ezzel a legforgalmasabb időpontokban az áthaladást.

Az ujjnyomat-olvasók tekintetében az informatikai erőforrások emelése lenne szükséges a hatékony és megfelelő sebességű működés érdekében. Ugyancsak előnyt jelentene, ha használható lenne az ujjnyomat-olvasó kártyaazonosító egysége a meglévő proxy kártyák felismertetését, hiszen ezek működése jóval gyorsabb, mint a kapuk egységei. Komoly biztonsági kockázatot jelent a kapuk felett, jól látható módon elhelyezett gombok, melyek a lengőkapu karjait függőleges helyzetbe helyezik. Ennek csökkentése érdekében a nyomógombokat rejtve kéne elhelyezni, laikus számára nem észrevehetően.

Fontos lenne továbbá, ha nem csak a befelé, hanem a kifelé való haladás esetén is azonosítaniuk kellene magukat a használóknak, ezzel még követhetőbbé téve az épületben tartózkodókat.

A kar hallgatóinak és munkatársainak tájékozottsága megfelelő mértékű, azonban a levelező tagozatra, valamint az Egyetem más karra járó hallgatóinak esetén ez nem mondható el. Teljeskörű tájékoztatásra lenne szükség a fentebb felsorolt csoportok körében, mely megvalósítható lenne az összes kar első évfolyamainak esetében a beiratkozáskor, a felsőbb évfolyamra járókat körüzenetben kellene értesíteni. Ennek tartalmaznia kellene a rendszer működésének leírását, illetve nem a Karra járók és ott dolgozók bejutásának lehetőségeit.

Ugyancsak jelentősen növelhető lenne a biztonság, ha a kari levelezős és a többi hallgató és alkalmazott csak vendégkártya felvételét követően juthatna be az épületbe. Ennek megvalósítása a portaszolgálat bevonásával lenne elérhető, vagyis amikor egy belépni kívánó személy az épületben érkezik, leadja diákigazolványát, megkapja ideiglenes kártyáját, majd kijutáskor visszaadja azt. Külsősök esetében kísérővel lehetne csak az épületbe jutni, amelyet vagy a portaszolgálat biztosít vagy olyan személy, akihez az illető érkezett. Mindezekkel csökkenthető lenne az épületbe való illetéktelen bejutások száma.

A beléptető kártya vásárlás esetén is megfontolandó lenne az azonosítás, ez megvalósítható lenne a vásárló által bemutatott érvényes diákigazolvánnyal vagy a Tanulmányi Osztály által kiadott hallgatói listával, amelyen ellenőrizhető az adott személy hallgatói státusza is. Könnyen ellenőrizhetővé tenné a hallgatókat, ha a tanulmányi rendszer segítségével történne a kártyavásárlás nyilvántartása, így nem csak kiszűrhetőek az illetéktelenek hanem, amint a hallgató végez a képzésen nem csak személyes adatlapja, hanem belépési profilja is törlésre kerülhetne. Szintén ide kapcsolódó probléma, hogy névre szólnak a kártyák, amely helyett lehetne a Neptun kódokat alkalmazni, ezzel is növelve a személyes adatok védelmét.

Összességében véve a fentebb felsorolt javaslatok részben kis ráfordítással is megoldhatóak lennének, ezzel tovább csökkentve a rendszerben felmerülő biztonsági réseket.

A nagyobb anyagi terhet jelentő beruházások lehetősége mindenképp növelné a hatékonyságot, ugyanakkor ez a kar költségvetésére komoly terhet róna.

Ebben a fejezetben az olvasó részletesen megismerhette a Karon levő beléptető rendszer előnyeit és hátrányait valamint elolvashatta az ezzel kapcsolatos következtetéseimet és fejlesztési javaslataimat.

BEFEJEZÉS

Dolgozatomban bemutattam a Karon működő beléptető rendszert, annak elmeit és működését. Annak érdekében, hogy átlátható legyen az ismertetés, röviden bemutattam a beléptető struktúrákhoz tartozó alapfogalmakat, az azonosítási lehetőségeket és eszközöket, továbbá az áteresztést szabályozó elemeket és a felügyeleti rendszert, valamint az ezekkel kapcsolatos problémákat, előnyöket.

Nagy hangsúlyt kívántam fektetni – magának a rendszernek a bemutatása mellett – annak hatékonyságára, kiemelve az előnyöket és a működés során fellépő nehézségekre. Saját mérések segítségével rá kívántam világítani a biztonsági résekre és a hatékonyságot akadályozó tényezőkre, továbbá javaslatokat fogalmaztam meg ezek orvoslására.

Fontosnak tartom, hogy a Kar, mint közintézmény és oktatási egység, kiemelt biztonságot szavatoljon az ott tanulók és dolgozók számára, melynek elérésében fontos szerepet játszik a már ma is működő biztonsági struktúra. Ennek további fejlesztése nem csak azért javasolt, hogy lépést lehessen tartani a fejlődő technika vívmányaival, ezáltal a kari hallgatók ismeretei és gyakorlati tapasztalatai is bővíthetők legyenek, hanem hogy folyamatos és magas szintű biztonságot lehessen garantálni az ott tartózkodók számára.

A megfogalmazott javaslataimmal a rendszert működtetők és a költségvetést biztosító kari vezetés számára kívántam ötleteket nyújtani a későbbi fejlesztésekhez, mely reméljük, hogy a közeljövőben megvalósításra kerülhet.

IRODALOMJEGYZÉK

[1] Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személy azonosítási eljárásai biztonságtechnikai szempontból, Hadmérnök , VI. évfolyam 1. szám, 2011 március, ISSN 1788-1919 , 2011. 09. 01.

[7] IButton: Maxim , <http://www.maxim-ic.com/products/ibutton/ibuttons/>, 2011. 08. 27.

[8] Berényi Richárd: Biometrikai azonosító rendszerek TDK dolgozat, <http://mycite.omikk.bme.hu/doc/4233.pdf>, 2011. 08. 29.

[9] Szabó Máté Dániel: BIOMETRIKUS AZONOSÍTÁS ÉS ADATVÉDELEM, <http://www.szabomat.hu/tanulmany/biometria.pdf>, 2011. 08. 30.

[10] Habil Dr. Kovács Tibor: Biometrikus azonosítás alapjai elektronikus jegyzet

Géher Károly: Híradástechnika, 2001, Budapest, Műszaki Könyvkiadó, ISBN: 963-16-0173-0

Dr. Házma István: Híradástechnika II.,2005., Budapest, BMF

BME Híradástechnikai Tanszék tanszéki munkaközösség: Információ közlése és feldolgozása, 1986., Budapest, Tankönyvkiadó

Andrew S. Tannenbaum: Számítógépes hálózatok, 2003, Budapest, PANEM KTF., ISBN: 9789635453849

Dr. Csernoch János: Rádiófrekvenciás átvitelek, 2002, Budapest, BMF

Dr. Lukács György: Vagyonvédelmi Nagykönyv, 1996, Budapest, CEDIT Információtechnikai Kft., ISBN: 963 8180 39 0

Információ – biztonság: 1997, Budapest, CEDIT Kft.

Allaga Gyula: Kártyás rendszerek, 1997, Budapest, PRÍM Kiadó, ISBN: 963-04-7789-0

Pálffy Zoltán: RFID és biztonság Detektor Plusz 2010/5-6, ISSN: 06006

Filkorn József: Beléptető rendszerek üzemeltetése a gyakorlatban, Detektor Plusz magazin 2010.-17. évfolyam 3-4. szám, ISSN: 06006

Dr. Lukács György: Vagyonvédelmi rendszerek I-II. ppt előadás, 2010. 04. 14.

Szádeczky Tamás: Vagyonvédelmi rendszerek II. előadásjegyzet, 2011. 02. 22.

RACS kezelői útmutató

Suprema Biostar kezelői útmutató

INTUS PS kezelői útmutató

Utassy Sándor: Komplex vagyonvédelmi rendszerek biztonságtechnikai kérdései PhD értekezés, http://193.224.76.4/download/konyvtar/digitgy/phd/2009/utassy_sandor_thu.pdf, 2011. 09.01.

Integrált Biometrikus Azonosító Rendszerek Irodalomkutatás kötet: Budapesti Műszaki és Gazdaságtudományi Egyetem Méréstechnika és Információs Rendszerek Tanszék, oldweb.mit.bme.hu/research/search/downloads/ibar/Irodalomkutatatas.pdf, 2011. 08.29.

Gunnebo SlimStile BA forgókereszt:

http://www.tablázat.hu/images/upload/products/pds_slimstile.ev_1.1_en.pdf, 2011. 08.27.

Gunnebo SlimStile BA forgókereszt falra szerelhető változat:

http://smp.hu/WEBSET_DOWNLOADS/651/CCEC%20PDS%20SlimStile%20BA%20UK%201_hu.pdf, 2011. 08. 27.

Suprema Bioentry

Plus:http://www.supremainc.com/eng/bbs/bbs/download.php?bbs_code=10022&bbs_cate=1&filename=BioEntry_Plus.pdf&file_no=109, 2011. 09. 02.

Intus 1600: http://pcs.com/uploads/tx_nppcsproducts/INTUS_1600_presentation_P_en.pdf, 2011. 08. 29.

Wanzl termékkatalógus: <http://www.wanzl.hu/default.asp?oid=150&lid=Hu&navid=551382> oldalon található pdf formátum, 2011. 09.03.

TÁBLÁZATJEGYZÉK

1. Számú táblázat: Gunnebo SlimStile BA forgókereszt műszaki adatai, Készítette: A Szerző, a Gunnebo SlimStile BA termékkatalógus alapján
2. Számú táblázat: Wanzl lengőkapu műszaki adatai, Készítette: A Szerző, a Wanzl termékkatalógus alapján
3. Számú táblázat: RFID kártyák csoportosítása, Készítette: A Szerző

4. Számú táblázat: Suprema Bioentry Plus ujjnyomat azonosító műszaki adatai, Készítette: A Szerző, a Supream Bioentry Plus termékkatalógus alapján
5. Számú táblázat: INTUS 1600 tenyérerezet azonosító műszaki adatai, Készítette: A Szerző, az INTUS 1600 termékkatalógus alapján
6. Számú táblázat: Gunnebo SlimStile BA forgókereszt adatai, Készítette: A Szerző, saját mérések alapján
7. Számú táblázat: Hallgatók eloszlása időrendben a 2011/2012. tanév első félévének Keddi napján, Készítette: A Szerző, a Kar 2011/2012. első félévének órarendje alapján

KÉPJEGYZÉK

1. kép: Gunnebo SlimStile BA forgókereszt, lábon álló kivitel, Készítette: A Szerző
2. kép: Gunnebo SlimStile BA forgókereszt, falra szerelhető kivitel, Készítette: A Szerző
3. kép: Wanzl lengőkapu, Készítette: A Szerző
4. kép: Wanzl lengőkapu 2, Készítette: A Szerző
5. kép: Suprema Bioentry Plus ujjnyomat azonosító, Készítette: A Szerző
6. kép: INTUS 1600 tenyérerezet olvasó