OTTI CSABA – FEHÉR ANDRÁS

ADATKEZELÉSI SZABÁLYOK HATÁSA EGY SZERVEZET MUNKAERŐ- ÉS LÉTSZÁMGAZDÁLKODÁSÁRA

A szervezetek alapvető feladata a biztonságos munkakörnyezet és a törvényi munkafeltételek biztosítása a munkajogi szabályozások és rendelkezések betartásán keresztül. A munkáltató és munkavállaló kötelezettségeit, a szabadságolásokat, a munkarend tervezését vagy a munkaszerződési előírásokat egyaránt tartalmazzák a különböző munkajogi és adatvédelmi szabályozások. A „Piacvezérelt kutatás-fejlesztési és innovációs projektek támogatása" című pályázat[6] keretében integrált platformot fejlesztünk a vállalatok historikus adatokon alapuló prediktív létszámgazdálkodásához, aminek első lépése a személyi adatok védelmére irányuló rendelkezések áttekintése. A GDPR és a hazai adatkezelési és adatvédelmi szabályokat figyelembe véve megvizsgáljuk, milyen adatok használhatóak fel a szervezetek munkaerőpiaci előrejelzéséhez. A személyes adatok kezelésére a GDPR szabályait követve kiváló eszközrendszert biztosít az 5W módszertan, melyet cikkünkben a pályázati projektre specifikusan mutatunk be. Célunk egy olyan ismertető készítése, mely bemutatja a munkavállalók adatainak jogszerű felhasználását, és feltárja ezek alkalmazhatóságát az állományi előrejelzés gyakorlatában, továbbá a HR szakemberek módszertanként felhasználhatják általános GDPR elemzési és megfelelési célokra

Bevezetés

A munka világát rohamos mértékben befolyásolja a technológiai fejlődés, mely nem csupán a munkavállalók szükséges képességeit értékeli át, hanem a munkáltatók és a HR munkaügyi feladatait is. A technológiai fejlődéssel pedig, a munkajognak és a személyes adatok kezelésére vonatkozó szabályozásoknak is lépést kell tartaniuk. A digitalizáció átformálja a munkaviszonyokat és az igény a munkaidőnyilvántartás digitalizált és integrált rendszere iránt növekszik. A HR folyamatok automatizálása és integrált rendszerének kialakítása elsőbbséget élvez a technológiai fejlődés és az Ipar 4.0 okozta változások és kihívások követéséhez. Ezek a változások kihívások elé állítják a HR szakembereket, hiszen a hatásuk kiterjed a teljes munkaerő-piaci igények és kompetenciák alakulására (Szabó, et al., 2020) (Ferencz, 2019).

Tanulmányunkban egy teljes egészében magyar tulajdonú KKV példáján keresztül mutatjuk be egy integrált létszámgazdálkodásra alkalmas szoftver kidolgozására tett első lépéseket. A magyar tulajdonú középvállalkozás, a Login Autonom Kft. digitalizációs szoftvermegoldásokat és biztonságtechnikai hardveres megoldásokat kínáló vállalkozás, elsősorban multinacionális nagyvállalatok részére. A munkaidőnyilvántartás, és a nyilvántartáshoz szükséges, munkavállalók személyes

Otti Csaba főiskolai docens, Budapesti Metropolitan Egyetem, CEO, Login Autonom Kft.

Fehér András CEO, Login Autonom Kft.

[6] A 2020-1.1.2-PIACI-KFI-2021-00310 számú projekt az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2020-1.1.2-PIACI KFI pályázati program finanszírozásában valósult meg.

adatainak felhasználása jogi kérdéseket vet fel, ennek nyomán megvizsgáljuk első lépésben az ezeket szabályozó törvényeket és rendelkezéseket.

A cél, a bemutatott vállalkozás egy pályázati projekt keretében megvalósított HR szoftver létrehozásához szükséges munkajogi és adatvédelmi szabályok vizsgálata. A projekt keretében egy munkaerő-szükséglet tervezésére alkalmas szoftver kerül fejlesztésre, mely képes legfeljebb 2 hetes, de legalább 72 óránál nagyobb időintervallumon előrejelzést kínálni. Egy egységes, integrálható, egyszerű adatfelvételt és adatáramlást biztosító rendszer kialakítása lehetővé teszi a termeléssel foglalkozó vállalatok munkavállalóinak hatékonyabb létszámtervezését és kiküszöböli a „félretervezéssel" járó kieséseket a létszám tudatos, és szükséges mértékű túltervezésével. A vállalatoknak ezáltal nincs szükségük több, kevésbé integrálható, egy-egy területre fókuszáló rendszerek és szoftverek együttes használatára, hiszen a létrehozott szoftver önmagában alkalmas az állományi létszám megtervezésére oly módon, hogy a szükséges és megjelenő létszám között legfeljebb 1%-os eltérést eredményez.

A gyakorlati megvalósítás első lépése a szekunder kutatás, a szakirodalmi és szabályozási áttekintés. A munka törvénykönyve és adatvédelmi előírások figyelembevétele nélkülözhetetlen a jogszerű beosztástervezéshez, a munkavállalók jogainak alkalmazásához és a munkavállalók személyes adatainak jogszerű felhasználásához. Tanulmányunkban áttekintjük többek között a Munka Törvénykönyvében foglalt releváns előírásokat és a GDPR hatályos rendelkezéseit. A vizsgált adatokat felhasználva elkészítünk, egy a GDPR eszközrendszer által javasolt, adatfeldolgozást és a létszámgazdálkodással összefüggő adatfelhasználást elősegítő leltárt, mely útmutatóul szolgál a szoftver kidolgozásához, valamint általánosságban használható a vállalatok számára a személyi állomány adatvagyonának GDPR-nak megfelelő felméréséhez és kezeléséhez. Tanulmányunk alapvetően szekunder információk feldolgozását és szakirodalmi áttekintést tartalmaz, azonban a gyakorlat megvalósításra is javaslatokat tesz.

A munkaidő nyilvántartására és a munkavállalók személyi adatainak védelmére vonatkozó előírások áttekintése

A munkaidőnyilvántartás összetételének megértéséhez elengedhetetlen a munkaidővel kapcsolatos fogalmak áttekintése, jelen esetben csupán jogi szempontból vizsgálódunk. A munkaidő jogszerű számítása és annak nyilvántartása komplex feladat, figyelembe véve a Munka Törvénykönyvének rendelkezéseit. A munkaidő számításának problematikája és a definíciókkal kapcsolatos hiányosságok már korábban felmerültek a szabályozást vizsgáló kutatókban, a helyzetet pedig nehezíti, hogy az uniós megfelelőségi irányelvek és a magyar törvényi definíciók nincsenek teljes egészében összhangban. Az Európai Parlament és a Tanács 2003/88/EK irányelvében (továbbiakban irányelv) a munkaidő-szervezés egyes szempontjairól a munkaidőt úgy definiálja, mint az az időtartam, amely alatt a munkavállaló dolgozik, a munkáltató rendelkezésére áll, és tevékenységét vagy feladatát végzi a nemzeti jogszabályoknak és/vagy gyakorlatnak megfelelően. A 2012. évi I. törvény a munka törvénykönyvéről (továbbiakban Mt.) 86. § (1)e alapján a munkaidő a munkavégzésre előírt idő kezdetétől annak befejezéséig tartó idő, valamint a munkavégzéshez kapcsolódó előkészítő és befejező tevékenység tartama. Előkészítő és befejező tevékenységet jelentenek azok a feladatok, amelyet a munkavállalónak a munkájához kapcsolódóan külön utasítás nélkül, rendszeresen szükséges elvégeznie. Míg az Mt. a munkavégzésre előírt időként definiálja a munkaidőt, addig az EU irányelvben a munkavégzés puszta tényére koncentrál (Fodor, 2016) (Ferencz, 2019).

Az Mt. és az irányelv közötti alapvető definíciós és megfogalmazási hézagokat bizonyítja, hogy az irányelv egyes törvényi kötelezettségeit nem említi a Munka Törvénykönyve. Az irányelv a maximális heti munkaidőre vonatkozóan megszabja, hogy a hétnapos időtartamokban az átlagos

munkaidő, a túlórát is beleértve, ne haladja meg a 48 órát. A munkáltató naprakész nyilvántartást vezet az ilyen munkát végző valamennyi munkavállalóról; és a nyilvántartásokat az illetékes hatóságok rendelkezésére bocsátják, amelyek a munkavállalók biztonságával és/vagy egészségével kapcsolatos okok alapján megtilthatják vagy korlátozhatják a maximális heti munkaidő túllépését. Az Európai Bíróság továbbá rendelkezett arról is, ha a munkavállalók nem rendelkeznek állandó vagy szokásos munkavégzési hellyel, munkaidőnek minősül az az utazási idő, amelyet a munkavállalók a lakóhelyük, valamint a munkáltatójuk által kijelölt első és utolsó ügyfél közötti mindennapos utazással töltenek (Kártyás, et al., 2016) (Fodor, 2016).Az Mt. 86. § (2) bekezdése szerint nem minősül munkaidőnek a munkaközi szünet (készenléti jellegű munkakört kivéve), valamint a munkavállaló lakó- vagy tartózkodási helyéről a tényleges munkavégzés helyére, valamint a munkavégzés helyéről a lakó- vagy tartózkodási helyére történő utazás tartama (Poór & Mártonné, 2019).

Ezekből is kitűnik, hogy a hazai és európai uniós munkajog értelmezése, összeegyeztetése nehézkes és problematikus lehet, számos kérdést felvethet, melyekre folyamatos figyelmet fordítanak a munkajoggal foglalkozó szakemberek. A digitalizáció további nehézségeket vethet fel, hiszen a technológiai fejlődéssel nehezen tart lépést a munkajogi szabályozás és a munkajogi alapelvek. Az alapelvek alkalmazása mégis segítséget nyújt a rohamos technológiai fejlődés okozta nehézségek leküzdésében, mint a munkavállalóknak, mint a munkáltatóknak. A munkavégzés helyének megváltozásával, a koronavírus által okozott járványügyi veszélyhelyzetből kifolyólag a távmunka és a home office egyre gyakoribb alkalmazásával pedig még inkább szélesedik a munkajogi szabályozások és alapelvek áttekintésének szüksége (Herdon, 2021) (Mélypataki, 2020). Habár ez a két terület további lehetőségeket rejt magában, a tartalmi korlátok miatt jelen tanulmányban nem tárgyaljuk ezek problematikáját. A munkaidőnyilvántartás jogi szabályozásnak releváns tartalmi elemeit a munkaidővel kapcsolatos szabályozásokra korlátozzuk, hiszen — habár a munkavégzés helyének, és a munkaviszony teljesítésének szabályozása a munkavégzés szempontjából elengedhetetlen — azok teljeskörű alkalmazása a kutatás jelenlegi szakaszában és ebben a tanulmányban történő részletezésben nem kiemelt fontosságú.

Az Mt. szabályozza (Mt. 99. §), hogy a munkavállaló beosztás szerinti napi munkaideje - a részmunkaidőt kivéve - négy óránál rövidebb nem lehet. Kimondja továbbá, hogy a munkavállaló napi munkaideje legfeljebb tizenkét óra, heti munkaideje legfeljebb negyvennyolc óra lehet, a munkaidő beosztásba pedig beletartozik a rendkívüli munkaidő és az ügyelet teljes tartama is. A Mt. rendelkezik a rendkívüli munkaidőről és az ügyelet tartalmáról is (Mt. 56. és 57. cikke), teljes napi munkaidő esetén naptári évenként 250 óra, kollektív szerződés rendelkezése esetén pedig legfeljebb 300 óra rendkívüli munkaidő rendelhető el. Ezen felül önként vállalt túlmunkaként, a felek megállapodása esetén naptári évenként további legfeljebb 100 óra rendkívüli munkaidő rendelhető el. A munkavállaló beosztás szerinti napi vagy heti munkaidejét legfeljebb egy órával meghaladhatja, ha a téli időszámítás kezdete a munkaidő-beosztás szerinti munkaidőre esik, azonban a rendkívüli munkaidő kihasználása esetén az átlagos évi 250 munkanapra is eshet legfeljebb 1 óra rendkívüli munkavégzés (Ferencz, 2019) (Bankó, et al., 2020).

Az Mt. 92. §-a szerint, a teljes napi munkaidő nyolc óra. Ez a munkaidő csak abban az esetben emelhető 12 órára, ha a munkavállaló készenléti jellegű munkakört lát el, vagy a munkáltató, vagy a tulajdonos hozzátartozója. A munkavállaló munkaidejének mértékéről a felek szerződésben állapodnak meg, a munkaidőnyilvántartás jogszerű készítésénél is ez az irányadó. A munka- és pihenőidő nyilvántartásáról az Mt. 63. bekezdése rendelkezik, melyek közül a kiemelendő a 134. § (1). A paragrafus kimondja, hogy a munkáltató nyilvántartja a rendes és a rendkívüli munkaidőt, a készenlét, a szabadság és az önként vállalt túlmunka vagy kollektív szerződés alapján teljesített rendkívüli munkaidő tartamát. A munkaidő-nyilvántartás elektronikusan is vezethető, az Mt. nem kötelezi a munkáltatót a papír alapú nyilvántartása, azonban a nyilvántartásnak meg kell felelnie

a naprakészség követelményének, a munkavállaló saját beosztására, szabadságára vonatkozó adatai számára pedig hozzáférhető és ellenőrizhető legyen.

Az Mt. és az EU irányelve egyaránt tartalmazza a pihenőidőre vonatkozó szabályozást és alapelvet, az irányelv a napi pihenőidőt 24 órás időtartamonként 11 összefüggő órára határozza meg, erről hasonlóan rendelkezik az Mt. 104. § is. Azonban míg az irányelv a heti pihenőidőt hétnaponként 24 órás minimális, megszakítás nélküli pihenőidőként szabályozza, addig az Mt. 105. § hetenként két pihenőnap (heti pihenőnap) beosztását rendeli el, melyek egyenlőtlenül is beoszthatók (Prugberger, 2017).

A munkaidőt a munkáltató osztja be, azonban figyelembe kell vennie az egészséges és biztonságos munkavégzésre vonatkozó követelményeket és a munka jellegét. A munkáltató köteles a munkaidő-beosztást legalább egy hétre, a beosztás szerinti napi munkaidő kezdetét megelőzően legalább 168 órával korábban írásban közli a munkavállalóval, közlés hiányában az utolsó munkaidő-beosztás az irányadó. A munkaidő-beosztás módosítására — ha gazdálkodásában vagy működésében előre nem látható körülmény merül fel — a beosztás szerinti napi munkaidő kezdetét megelőzően legalább 96 órával korábban módosíthatja, azonban a munkavállaló is kérheti írásban a munkaidő-beosztás módosítását. Amennyiben a munkáltató a rendelkezésre állást megszablya, azt legalább 1 héttel korábban közölni kell a munkavállalóval, ettől rendkívüli, előre nem látható gazdasági esemény esetén szintén eltérhet. Az ügyelet tartama nem haladhatja meg a 24 órát, amelybe az ügyelet megkezdésének napjára beosztott rendes vagy elrendelt rendkívüli munkaidő tartamát be kell számítani (Mt. 50. bek.) (Bankó, et al., 2020) (Strihó, 2020).

Az Mt. irányadó szabályokat rögzített az adatkezelésre (Mt. 5/A. bek.), mely szerint a munkavállalótól csak olyan személyes adat kérhető, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy e törvényből származó igény érvényesítése szempontjából lényeges (Mt. 10. §). Az adatkezelésről pedig, a munkáltatónak írásban kell tájékoztatnia a munkavállalót. Az adatkezelésre vonatkozóan irányadó lehet az Mt. 52. § (1) bekezdésének a) pontja, mely szerint a munkavállaló köteles a munkáltató által előírt helyen és időben munkára képes állapotban megjelenni. Ez alapján a munkáltató ellenőrizheti, hogy a munkavállaló valóban megjelenik-e munkára képes állapotban. A munkavállaló biometrikus adatainak kezelésére is kitér az Mt. 11. §-a, így azok kezelésére akkor van lehetőség, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely vagy a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy törvényben védett jelentős érdek súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna. Itt pontosításra került, mit jelent a jelentősén védett érdek:

- a legalább „Bizalmas!" minősítési szintű minősített adatok védelméhez,
- a lőfegyver, lőszer, robbanóanyag őrzéséhez,
- a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez,
- a nukleáris anyagok őrzéséhez,
- a Btk. szerint legalább különösen nagy vagyoni érték védelméhez fűződő érdek.

A munkáltató nem használhatja és kezelheti a munkavállaló biometrikus adatait munkaidő-nyilvántartás céljából. A munkavállaló bűnügyi személyes adatait tekintve, a munkáltató azt abban az esetben kezelheti, ha a törvény vagy a korlátozó vagy kizáró feltételek (mint a munkáltató jelentős vagyoni érdeke, vagy a törvény által védett titok, érdek) szerint a munkáltató a betölteni kívánt vagy a betöltött munkakörben nem korlátozza vagy nem zárja-e ki a foglalkoztatást. A munkavállalók megfigyelésére alkalmas technikai eszközök munkahelyi alkalmazására vonatkozóan a Nemzeti Adatvédelmi és Információszabadság Hatóságának (NAIH) ajánlásait is figyelembe kell venni, mely olyan feltételeket fogalmaz meg, mint a kamera használata kizárólag munkavégzés

ellenőrzésére vagy az internet használat ellenőrzése kizárólag abban a helyzetben, ha a munkáltató a személyes célú használatot előre megtiltotta (NAIH, 2016).

Az elektronikus beléptető rendszerek esetén, irányadó szabályokat tartalmaz a 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban SzVMt.) jogszabály, amely rendelkezik arról, hogy elektronikus beléptető rendszer az erre vonatkozó megbízási szerződés alapján és akkor alkalmazható, ha a jogszabály vagy a terület használatára jogosult rendelkezése szerint a védett területre csak az arra jogosultak léphetnek be (SzVMt 32. §). A munkaidő-nyilvántartás esetében az elektronikus beléptető rendszer nem jelenti egyértelműen és nem azonos a munkavégzés kezdetével és befejezésével, hiszen a beléptető rendszer a munkahelyre való belépés és távozás időpontját rögzítik, nem számol a rendes vagy rendkívüli munkaidővel.

A munkáltató ellenőrizheti a munkavállaló magatartását, amennyiben az a munkaviszonnyal összefügg, de ezesetben is írásban kell tájékoztatni (Mt. 11. §/A). Az írásban történő, előzetes tájékoztatás fontos aspektusa a törvényi előírásnak, hiszen szorosan kapcsolódik az információs önrendelkezési joghoz és a magánszféra tiszteletéhez. Az Mt. nem konkretizálja, vagy definiálja, hogy a „munkaviszonnyal összefüggő magatartás" pontosan milyen cselekedetekre utal, arra sem tér ki, hogy a munkaközi szünet vagy a pihenőidő alkalmára értendő-e a rendelkezés. Az Mt. ezen rendelkezése nem tér ki arra, hogy a munkáltató ellenőrzése nem járhat az emberi méltóság megsértésével, azonban ebben az esetben is alkalmazni kell a Magyarország Alaptörvénye II. cikkéből és a 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban Ptk.) személyiségi jogot védő rendelkezéseiből adódó irányelveket. A munkavállalónak joga van a szabad vélemény nyilvánításához, azonban ez nem járhat a munkáltató hírnevének, gazdasági vagy szervezeti érdekének megsértésével (Poór & Mártonné, 2019).

Az Mt. továbbá rendelkezik arról is, hogy a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert a munkavállaló csakis a munkaviszony teljesítése érdekében használhatja, tehát a magáncélú használatot kizárja, kivéve, ha a felek nem állapodnak meg másban. A magáncélú használathoz külön megállapodás szükséges, ahol érdemes tisztázni a magáncélú használat jellegét és pontos feltételeit is. Ilyen esetekben, alkalmas lehet egy felhő-alapú rendszer használata, ahol elkülöníthetőek a munkáltatói adatok és akár távolról is hozzáférhetőek a munkáltató által (Bankó, et al., 2020).

Az Mt. az adatvédelemről leginkább kiegészítő, ágazati jellegű szabályokat tartalmaz, az adatvédelemről ennél pontosabban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról is rendelkezik. Az adatkezelés során a munkáltatónak figyelembe kell vennie:

- a **célhoz kötöttség elvét** (a munkáltatónak minden adatkezeléshez célt kell rendelnie, személyes adat csak akkor kezelhető, ha az lényeges, ha az adat kezelése nélkül a munkaviszony létesítése, fenntartása, megszűnése nem lenne lehetséges),
- a **szükségesség-arányosság elvét** (a munkáltatói ellenőrzésre irányul, mely csak akkor alkalmazható, ha egyértelmű, hogy az alkalmazni kívánt eszköz, módszer által az ellenőrzés útján a védeni kívánt munkáltatói érdekek, jogok sérelme megelőzhető és az emberi méltóság tiszteletben tartható, és az ellenőrzés a munkával összefüggésben történik. A munkahelyen is megilleti a magánélethez való jog a munkavállalót, mint az ebédlőben, pihenőhelyiségben, mosdóban és öltözőben) (NAIH, 2016) (Fehér, 2021).

Az adatkezelésre vonatkozó jogalapok esetében az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő

védelméről és az ilyen adatok szabad áramlásáról (továbbiakban GDPR) a mérvadó, mely a személyes adatok védelméről alaposabb rendelkezéseket kínál.

GDPR rendelkezések és eszközrendszerének alkalmazása

A GDPR a munkavállalói adatok kezelésére nem fogalmaz meg elkülönült, specifikus szabályokat így az általános rendelkezést kell alkalmazni ebben az esetben is. A GDPR rendeletét áttekintve, elsősorban két jelentős fogalmat érdemes figyelembe venni (GDPR 4. cikk):

- **személyes adat***:* azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
- **az érintett hozzájárulása***:* az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

Az ismertetett fogalmi meghatározások alapján elmondható, hogy személyes adatnak minősül a munkavállalóra vonatkozó minden információ, így a munkaidő nyilvántartáshoz felhasznált minden adat (a munkavállaló munkaidejének kezdete és vége, a munkaközi szünetek és a szabadság időtartama is). Az adatok azonban, az érintett szabad döntési lehetőségén alapuló hozzájárulásával használhatóak csak fel, ez nem vonatkozik azokra a személyes adatokra, amelyek szolgáltatására a jogszabály kötelez. A szabad döntési lehetőség a GDPR értelmezésében azt jelenti, hogy a személyes adatok felhasználása csak akkor jogszerű, ha az érintettnek az adatfelhasználásra, feldolgozásra vonatkozó kérelem elutasítása esetén nem jár semmilyen hátránnyal, az elfogadásáról szabadon és következmények nélkül dönthet. A szabad döntés jogát, pontosabban az önkéntes hozzájáruláson alapuló adatkezelést számos munkajoggal foglalkozó szakember tárgyalta már, hiszen egy munkaszerződés esetében nehezen elképzelhető, hogy a feltételek visszautasítása esetén ne járna a potenciális munkavállaló döntése bármilyen hátránnyal (Fodor, 2016). Ennek tárgyalása a tanulmányban nem kerül sorra, azonban említés szintjén fontosnak tartottuk érzékeltetni a problémát. A személyes adatok kezelésére vonatkozóan a GDPR is ismerteti a legfontosabb elveket (GDPR 5. cikk):

- jogszerűség, tisztességes eljárás és átláthatóság;
- célhoz kötöttség (az adatkezelés célját világosan, pontosan, egyértelműen és kellő részleteséggel kell meghatározni, mely során azonosíthatóak az adatkezelési műveletek);
- adattakarékosság (az adatok szükségszerűségre való korlátozását jelenti),
- pontosság;
- korlátozott tárolhatóság (az adatok azok céljának eléréséhez szükséges ideig való tárolását jelenti);
- integritás és bizalmas jelleg (a személyes adatok biztonságát jelenti a jogosulatlan és jogellenes eseményekkel szemben);
- elszámoltathatóság (az adatok megfelelésére vonatkozik).

Fontos elvárás, hogy a munkavállalók a saját személyes adataikhoz bármikor hozzáférhessenek, a személyes adatok kezelése számukra érthető és átlátható legyen (átláthatóság elve). A GDPR személyes adatok jogszerű felhasználására (GDPR 6. cikk) vonatkozóan több feltételt is megszabott,

amelyek közül legalább egynek teljesülnie kell. Ilyen az érintett hozzájárulása az adatok egy vagy több célú kezeléséhez, vagy az adatok felhasználása, ha a szerződés teljesítéséhez szükséges (jelen esetben beszélhetünk munkaszerződésről), esetleg az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez (jelen esetben ez jelenti a munkaviszony bejelentéséhez, társadalombiztosítási jogviszonyhoz, adózási szabályoknak megfelelő adatokat) szükséges.

Az EU tagállamok pontosabban kialakított szabályokat alkothatnak a jogszabályban vagy kollektív szerződésekben, hogy biztosítsák a jogok és szabadságok védelmét a munkavállalók személyes adatainak a foglalkoztatással összefüggő kezelése tekintetében (GDPR 88. cikk). Ezek a szabályok alkalmazhatók a munkaszerződés teljesítésére, vagy a munka irányítására, tervezésére és szervezésére. A munkáltató kötelessége, a papír alapú, és az elektronikus személyes adatok védelmének biztosítása, hozzáférést csak az arra kijelölt adatkezelő, és az érintett munkavállaló számára lehet biztosítani. Az elektronikus formában tárolt személyes adatokat többek között külső és belső tűzfalak, vírusvédelmi szoftverek, virtuális magánhálózatok (VPN), vagy behatolást jelző és megakadályozó csomagszűrő eszközök (IDS/IPS) alkalmazásával kell védeni.

A GDPR rendelkezései alapján – ahogyan azt a Mt. 11. § (1) pontja is kimondja – biometrikus adat csak szigorúan indokolt esetben használható fel, ilyen a vagyonbiztonság. Hasonló a helyzet az egészségügyi adatokkal is, melynek felhasználása szintén a GDPR 9. cikke szerinti kivételes esetekben lehetséges. A GDPR ösztönzi egyúttal a tanúsítási rendszerek, mint az ISO/IEC 27001 – Információbiztonsági Irányítási Rendszer (IBIR) alkalmazását, melyek által hatékonyabban lehet kezelni az adatbiztonságot (Otti & Rónaszéki, 2013).

A GDPR megfelelő alkalmazását, az adatfeldolgozáshoz és adatleltár készítését segíti elő az *5W (WHY, WHO, WHAT, WHEN, WHERE)* elv, mely egy egyszerűsített GDPR kompatibilis adatleltár. A leltár, habár nem jogi eszköz, mégis kiváló kiindulást jelent a személyes adatok kezeléséhez, feltérképezéséhez és azok jogalapjának áttekintéséhez. A GDPR alapelveit követve kínál a személyes adatok feldolgozásának folyamatát érintő legfontosabb kérdéseket, olyan alap útmutatót kínálva mely használható a személyes adatok feldolgozásának mélyebb és kockázatalapú kidolgozására. Az 5W elv az alábbi kérdéseket fogalmazza meg:

1. MIÉRT (WHY) kerülnek kezelésre a személyes adatok?
   Itt kerülnek részletezésre a személyes adatok felhasználásának okai és céljai, figyelembe véve a szervezeti tevékenység széleskörű területét pl. monitoring, személyzeti adminisztráció, áru vagy szolgáltatás nyújtás stb.

2 KINEK (WHOSE) a személyes adata kerül feldolgozásra?
   Az előző pontban azonosított okok és célok mentén, itt kerülnek azonosításra azok a személyek/csoportok, akiknek a személyes adatai kezelésre kerülnek pl. személyzet, ügyfelek stb.

3 MILYEN (WHAT) személyes adat kerül feldolgozásra?
   Itt kerül felsorolásra az összes rögzített vagy felhasznált személyes adat típus, az adatok forrásával és jogalapjával együtt pl. pénzügyi adatok, egészségügyi adatok, IP cím stb.

4 MIKOR (WHEN) kerül feldolgozásra a személyes adat?
   Itt kerül felsorolásra a személyes adatok megszerzésére, nyilvánosságra hozatalára és törlésére irányuló tevékenységek, mely során meg kell állapítani, hogy mikor válik elérhetővé a személyes adat, ki és miért férhet hozzá, valamint mennyi ideig kerül megőrzésre.

5 HOL (WHERE) kerül feldolgozásra a személyes adat?
Itt kerül részletezésre a személyes adatok feldolgozásának helye pl. külső szolgáltató, felhő alapú szolgáltatás (Isle of Man Information Commissioner, 2021).

A feltüntetett kérdések mentén kidolgoztunk egy leltárt a Login Autonom Kft. fent említett projekt céljának megfelelően a személyes adatok feldolgozását tekintve, felhasználva a tanulmányban vizsgált, jogszerűen feldolgozható adatok típusait, melyet az *1. táblázatban* szemléltetünk.

1. TÁBLÁZAT: GDPR-MEGFELELŐSÉGET BIZTOSÍTÓ ADATLELTÁR

MIÉRT	KINEK	MILYEN			MIKOR			HOL
		Típus	Forrás	Jog-alap	Feldolgo-zás	Keze-lés	Meg-őrzés	
Lét-szám-gazdál-kodás	Munka-erő	Név	Munkaidő nyilvántar-tás, jelenléti ív, munka-vállalói szerződés	GDPR 6. cikk, Mt. 10. §, Mt. 52. § (1)	Naprakészen, mun-kaidő-be-osztás vál-tozása ese-tén tárgyhó végéig	Adat-kezelő, adat-feldol-gozó, érin-tett	Nincs jogsza-bály-ban rögzí-tett idő-pont	belső IT szer-ver,HR szoft-ver
		Egyedi azo-nosító						
		Rendes napi munkaidő						
		Rendkívüli munkavég-zés						
		Szabadság						
		Fizetés nél-küli szabad-ság						
		Táppénzes állomány						
		Igazolt tá-vollét						
		Igazolatlan távollét						
		Készenléti idő						
		Ügyelet						

Forrás: saját szerkesztés (Isle of Man Information Commissioner, 2021, p. 18) alapján

A bemutatott táblázatban szereplő adatok gyűjteménye egy egyszerűsített útmutató a személyes adatok feldolgozásához. A táblázatban szereplő személyes adatok jelentik a létszámgazdálkodásra alkalmas HR szoftver input változóit. A személyes adatok kezelése során biztosítani kell az érintett munkavállalók számára:

- a tájékoztatáshoz való jogát (GDPR 13. és 14. cikk);
- a hozzáféréshez való jogát (GDPR 15. cikk);
- a helyesbítéshez és törléshez való jogát (GDPR 16. cikk);
- törléshez való jog (GDPR 17. cikk);
- a korlátozáshoz való jogát (GDPR 18. cikk);
- a tiltakozáshoz való jogát (GDPR 21. cikk);
- jogorvoslathoz való jogát (GDPR 77-82. cikkek).

A jelenlegi célhoz felhasznált személyes adatok megőrzésére vonatkozóan nem rögzít pontos határidőt a szabályrendszer, azonban ebben az esetben alkalmazható a Ptk. 6:22. §-a értelmében rögzített 5 éves általános elévülési idő, a munkavállaló szerződésben rögzített adatai pedig a munkaviszony megszűnéséig őrizhetőek.

A GDPR-nak megfelelően az érintetteket (ez esetben a munkavállalókat) számos jog illeti meg, például az adathordozhatósághoz és az elfelejtéshez (adattörléshez) való jog. A szervezetek kötelesek az adatok tárolását biztosítani, és korlátozni kell az EU-n kívülről származó adatokhoz való hozzáférést. Mindezen követelmények teljesítése megkívánja az alkalmazottak adatainak részletes feltérképezését, mely a digitális HR-rendszerektől a papíralapú archívumokig minden formátumot magában foglal. Az ismertetett szabályok és rendelkezések, valamint az 5W adatleltár segítségével kidolgoztunk egy egyszerű kérdéssort, amely lehetővé teszi az alkalmazottak adatainak, valamint a GDPR-megfelelőséghez szükséges folyamatok feltérképezését. Az útmutató azokat a zárt kérdéseket sorakoztatja fel, melyek segítenek a vállalkozás számára meghatározni a GDPR-ra való felkészültségében fennálló hiányosságokat:

- Van projektterv a GDPR megfelelésre?
- Tisztában van-e a felső vezetés a GDPR-ral kapcsolatos kockázatokkal és követelményekkel?
- Feltérképezte a DPO (adatvédelmi tisztviselő) szükségességét?
- Van jelenléte az EU-n kívül?
- Korlátozhatja az EU-n kívülről származó munkavállalói adatokhoz való hozzáférést?
- A munkavállalók adatait az EU-n kívül tárolják?
- Létrehoztak-e együttműködést a HR- és IT-csapatok a HR-rendszerek GDPR-megfelelőségének biztosítása érdekében?
- Feltérképezte az informatikai rendszert?
- Van áttekintése az összes munkavállalói adatról?
- Van alkalmazotti archívuma papír formátumban?
- Tárol alkalmazotti vagy fizetési adatokat elektronikus formában (pl. Excel)?

A zárt kérdésekre adott igen/nem típusú válaszok következtetni engednek a GDPR-megfelelőséghez szükséges adatfeldolgozási folyamat hiányosságaira.

Összefoglalás

A munkavállalók jogaihoz, a munkaidőnyilvántartáshoz, a munkaidő-beosztáshoz, valamint a munkavállalók személyes adatainak kezeléséhez kapcsolódó szabályok és rendelkezések áttekintése kiváló kiindulást jelent a pályázati projekt keretében megvalósuló létszámgazdálkodásra alkalmas HR szoftver jogi megfelelőségéhez. Habár a munkavállalók személyes adatainak kezeléséhez kapcsolódó szabályozások és törvények teljes körű, a téma minden területét lefedő ismertetése túlmutat e tanulmány keretein, az alapvető szabályozások bemutatásra kerültek. A feltérképezett tudás birtokában világossá vált, milyen alapvető követelményeknek kell megfelelni a munkaidőnyilvántartást és a munkavállalói személyes adatfeldolgozást tekintve. A kutatás lehetőség nyújt egy alaposabb, mindent átható GDPR-megfelelősséget teljes egészében lefedő szabályrendszer kidolgozásához, ugyanakkor jelen formájában jelentős segítséget nyújt a HR szakembereknek a GDPR szempontú adatvagyon feltérképezéséhez.

Irodalomjegyzék:

Bankó Z., Berke Gy., Kiss Gy., Kun A., & Petrovics Z. (2020). *Munkajog.* Dialóg Campus., Budapest.

Fehér A. (2021). Nagylétszámú termelővállalatok állományi rendelkezésre állása karakterisztikájának leírása ARIMA modellel. *Bánki Közlemények,* 4(1), 40-47.

Ferencz J. (2019). *Jogalkotás a munkaviszonyok szolgálatában.* Nemzeti Közszolgálati Egyetem, Budapest.

Ferencz S. J. (2019). Az átalakuló munkajog változásának jellege – A 24/7 jogi kihívásai. In: J. Glavanits, (szerk.) *A gazdasági jogalkotás aktuális lépései.* pp. 39-53.Dialóg Campus Kiadó, Budapest.

Fodor G. T. (2016). A Munka Törvénykönyve munka- és pihenőidő szabályozásának uniós jogi megfelelőségéről. *Magyar Munkajog,* 3(2) 21-36.

Herdon I. (2021). A munkavégzés helyének megváltoztatása – távmunka, „home office". In: *Mailáth György Tudományos Pályázat 2020 : Díjazott Dolgozatok.* pp. 650-706.Országos Bírósági Hivatal, Budapest.

Isle of Man Information Commissioner (2021). *Data protection compliance,* Barrantagh Fysseree UK.

Kártyás G., Répáczki, R. & Takács, G.(2016). *A munkajog digitalizálása,* Közösen a Jövő Munkahelyeiért Alapítvány, Budapest.

Mélypataki G. (2020). A munka digitalizálódása a munkajogi alapelvek tükrében. *Miskolci Jogi Szemle,* 5(3), 97-104.

NAIH (2016). A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről, Nemzeti Adatvédelmi és Információszabadság Hatóság, Budapest.

Otti Cs. & Rónaszéki P. (2013). Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész. *Detektor Plusz*, pp. 10-11.

Poór J. & Karoliny M-né (szerk.) (2019). *Emberi Erőforrás Menedzsment Kézikönyv.* 6.. Wolters Kluwer Hungary Kft., Budapest.

Prugberger T. (2017). A munkaidő, a pihenőidő és a szabadság új hazai szabályozásának megítélése a munkavállalói érdekek szempontjából. *Pro Futuro,* 7(2), 31-47.

Strihó K. (2020). A munkajog a digitalizáció világában. *Erdélyi Jogélet,* 3(4), 157-169.

Szabó, S., Némethy K., Csapó I., Poór J. & Balog K. (2020). A HR igény változásai a robotizáció és az Ipar 4.0 fejlődésének tükrében. In: Róka J. & Kiss F. (szerk.) *ANNALES.* pp. 186-214. Budapesti Metropolitan Egyetem, Budapest.

Jogforrások:

Európai Parlament és a Tanács 2003/88/EK irányelve (2003. november 4.) a munkaidő-szervezés egyes szempontjairól

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

2012. évi I. törvény a munka törvénykönyvéről

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Magyarország Alaptörvénye

2013. évi V. törvény a Polgári Törvénykönyvről

ANALISYS OF ACCESS POINTS WITH THE QUEUE MODEL FOR BIOMETRIC ACCESS CONTROL IN LARGE HEADCOUNT PLANTS

Csaba OTTI
University of Óbuda, Budapest, Hungary
otti.csaba@bgk.uni-obuda.hu

László HANKA
University of Óbuda, Budapest, Hungary
hanka.laszlo@bgk.uni-obuda.hu

ABSTRACT

The scaling of access control systems is usually done with respect to the life protection requirements regarding escape routes. At large headcount areas, the need for biometric identification arises from the security and business needs. Biometric systems can be characterized by probability variables, which can significantly affect the access process. Mathematically, access control is a discrete state space, stochastic process without memory, that can be described by a queue model. This study demonstrates the process model of access control systems and describes the mathematical model that allows for accurate planning and can ensure a successful introduction for access control systems.

KEYWORDS: access control system, biometry, queue model

1. Introduction

Waiting queues are found in every aspect of life. Waiting is a natural part of life – however unexpected or unreasonable queues can be a source of major discomfort for users. Parallelly to this, one of the most important tasks in creating a secure environment is to authenticate users for physical access into protected facilities and areas (Berek, 2014, pp. 19-24). Throughput calculations generally do not require serious mathematical modelling or designing – problems usually arise when either the access procedure is long due to the security level of the facility (metal detector gates, bag checking) or a large number of people arrive within a short timeframe. An increase in security level means a longer authentication time – which translates into an increased waiting time. The task of security experts is to find the optimal solution. Queue and mass serving models can serve as an adequate base to analyse access procedures and approximate their behavior thus making them plannable (Hillier & Lieberman, 2014). The purpose of this study is to create a MATAB program with which the properties of various scenarios can be examined, and also to analyse the results through a few examples. The study consists of the following parts: the 2. chapter describes the access process and its states. The 3. chapter introduces the queue model, and based on these, the 4. chapter develops the model of the access process. The 5. chapter details the mathematical model of the access process and demonstrates this through several calculation examples and the 6. chapter will summarize the study.

2. The Access Procedure

The access control system according to Bunyitai is a: *"Complex electromechanics-IT system, that – with the help of installed checkpoints – enables granting or denying personnel and vehicle access based on location, time and direction, while providing logging and tracking"* (Bunyitai, 2011, p. 18). The task of an access control system is to: *"Identify the person, determine the access right, document the event and control traffic"* (Bunyitai, 2011). The general elements of an access control system are readers: identifies the user arriving to the checkpoint. It can be password, card or biometry based – or a combination of them, controllers: they determine whether a user is eligible to access based on the code identified by the readers, APAS: The physical restrictive and mechanical devices controlled by the system and sensors that provide feedback. The controlled devices can be magnetic locks, holding magnets, turnstiles, turning crosses, revolving doors, automatic doors, etc. Sensors can be, or example infra gates, opening detectors or movement detectors. Finally, supervision software: This application serves as a control and display interface to the system settings, logs and handles the incoming signals from the hardware elements.

3. States of the Access Process

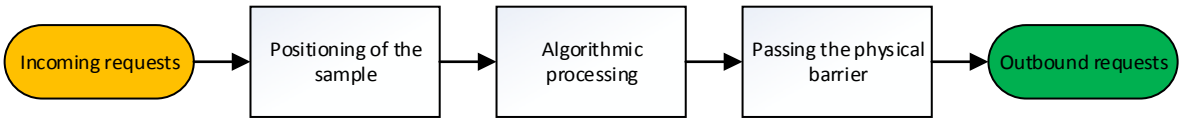


Figure no. 1: *The states of the access process*
(Source: Otti, 2015)

The states of the access process can be seen in the Figure no. 1. The properties of the individual stages are as such incoming requests: the employee or user arrives to the checkpoint and stands into the queue. Positioning the sample, when the user prepares for identification and presents their biometric sample to the sensor in order to gain access. An analogy to this for card-based access control is to touch the card to the reader. Algorithmic processing when the reader processes the sample and provides a successful or unsuccessful feedback signal. This step is only applicable for biometric systems, and this is the point where the probability nature of biometrics manifests – as it is never 100 % that a person can pass through the access point at the first try. The other consequence of this property – that also carries a security risk – is that an ineligible person gaining access can also not be ruled out by 100 %. This probability factor does not exist with card and PIN based systems. Passing the physical barrier, after a successful identification, the controller will signal the physical barrier to grant access. Outbound requests, when the user leaves the checkpoint. In an ideal environment, eligible people can always pass through the checkpoint, while attackers are always denied access, and as such, one must know the points where the system, in reality, may work differently. Incoming requests may face a queue. Positioning the sample can be unsuccessful: for example, the user places their finger on the sensor improperly, or maybe grows a beard and facial recognition systems will not recognize them, or drops the card etc. Algorithmic processing returns a bad result and requires a new attempt. The physical barrier does not work

properly, the door jams, the turnstile stops turning or the user uses it improperly – for example, tries to pass through too fast, jamming the barrier which will warrant another attempt.

4. Queue Model

Queues appear in various aspects of life, where access to a distributed resource is being served. Any system, where the customer is served with a limited resource, can be considered a queue system (Kleinrock, 1975). Example for such a system is a line in order to get ice-cream, a queue in the bank, the landing and maintenance queue for aircraft, data processing in a computer processor or even the students waiting for an exam. According to Pokoradi *"By queue, service systems, we mean a system where consumers arrive at random, the various requests wait for service, then depart"* (Pokorádi, 2008, pp. 173-175). Queue systems are also called Mass Service Systems. Queuing problems can be estimated, analysed and evaluated by analytic modelling or simulations. The analytic methods can be used with simpler queues, where the equations of the model can be easily obtained by simplifying certain aspects of the real process. In reality, however, it is very hard to describe such a system, because not all factors can be considered, or the equations obtained have a non-polinomial algorithmic processing time (Lovász, 2009, pp. 42-43). In these cases, an efficient examination method is simulation. That is done by simulating the operation of the system with a large element number and we derive conclusions from the results (Szeidl, 2009, p. 78). These systems have the following in common: the architecture of the system, incoming requests, waiting queues, servers, services, outbound requests.

Stochastic Process: It is not an uncommon issue in the technical sciences that the evolution of basic quantities required for analysis depends entirely on chance. These quantities typically describe the temporal and/or spatial changes of the analyzed factor. In this case, we can interpret quantities as a collective of probability variables belonging to the parameter. If the parameter set becomes a subset of the positive half-line, then can be considered as a time parameter or, in short, time. The set of real numbers is orderly, and as such the past and the future of the process can be interpreted. If we consider fixed value as present, then we can interpret as the future of the process, while is the past of the process (Pap & Szűcs, 2014, pp. 3-5).

Markov Process: We can describe a stochastic process as a Markov process, if the future states of the process are only influenced by the past states through the present states – or in other words, the process is without memory. For example, if five people stand at a turnstile access point, it doesn't matter that this state occurred because originally there were six people but one passed through or originally there were only three people and two more arrived. The access process can be considered a continuous, discrete state space Markov process – or in other words, a Markov chain. Every state in the system shows the number of people in queue and being served. The increase of waiting elements in the system is described by λ – arrival intensity, the decrease is described by μ – serving intensity. The base state of the system is that it is empty.

The Kendall Notation System: Kendall has published the general notations required to describe mass service systems in 1953. Based on this, the types of queue systems can be described if we know the incoming distribution, the properties of the queue and the service mechanism (Kendall, 1953, pp. 338-340). The purposes of this study are best served by the model of the book 'Basis of queuing theory' by

Sztrik (2011). The notations used to describe queuing systems are:

$$A / B / s / K / n / E$$

where:

– A = the distribution function of incoming request times.
– B = the distribution function of service times.
– s = the number of servers.
– K = the capacity of the system, or, in other words, the maximum number of requests that can stand in line.
– n = the amount of request sources.
– E = the basis of service.

The distribution functions (A, B) can be deterministic (D), exponential (M) or general (G). The capacity of the system (K) and the source of requests can be (n) finite or infinite – we generally use the latter. The basis of the service can be (E) FIFO (First In First Out), LIFO (Last In First Out), random or based on priority.

Terminology and Notation: The state of the system = the number of waiting elements in the queue.

– Queue length = the number of waiting elements that are waiting for the service to start.
– $N(t)$ = the number of elements waiting at *t (t ≥ 0)* point in time
– $P_n(t)$ = the probability of exactly *n* elements being present in the system at any given *t* moment.
– *s* = the number of parallel servers in the system.
– λ = incoming intensity per time unit.
– μ = service intensity per time unit.
– $\varrho = \frac{\lambda}{s\mu}$ = utilisation factor.

When a system is stable and set in (the queuing models – as this study does so as well – generally examine this state), then:

– P_n = is the probability, that exactly *n* elements are waiting in the system.
– $L = \sum_{n=0}^{\infty} nP_n$ = the number of elements waiting in the system.
– $L_q = \sum_{n=s}^{\infty}(n-s)P_n$ = expectable queue length.
– W = service time in the system with waiting time accounted for.
– W_q = time in the queue.

The following equations provide the connection between the above notations: $L = \lambda W$, called Little formula (Little, 1961, pp. 383-387), meaning: the average number of requests within the system is equal the incoming intensity times the average time spent in the system, where $L_q = \lambda W_q$ and $W = W_q + \frac{1}{\mu}$.

5. Model of the Access Process

Access control systems can be described as a multiple server, parallel service system. To further examine queue systems mathematically, we must put a number of restrictions in place in the conditions. These do not substantially influence the realisticity of the model, but if we must deviate from them, there are simulation methods to account for this (Law, 2015). The conditions will be accounted for using the Kendal notation. The distribution of the incoming requests is a Poisson distribution, the service time distribution is also exponential and the number of servers is *m* – a finite, natural number. The cardinality of the capacity of the system and the source of requests is infinite, the basis for service is FIFO. Based on this, the model of access control systems is: *M/M/s/∞/∞/FIFO*. In these cases, the last three parameters are usually not noted in writing – based on this, a one channel access control system is a *M/M/1*, a multi-channel is a *M/M/s model mass service system*. With the general sense of safety decreasing in the world, an ever-increasing need for authentic identification of users arises. The only technology that allows for identifying personally unique and preferably unfalsifiable properties is biometric identification. The current systems are by no means invulnerable, however, due to constant development, they fit an ever-growing standard of security and

convenience (Otti, 2016, pp. 251-253). Classification of biometric technologies: first of all, imaging-based technologies (fingerprint recognition, iris recognition, face recognition, vein recognition, hand geometry recognition, signature recognition), and also not (or not directly) imaging-based technologies (voice recognition, DNS test, behavior-based tests). The Figure no. 1 in chapter States of the access process shows "Positioning of the sample" and "Algorithmic processing" that are affected by biometric recognition. The queue model is modified by the service factor of the biometric devices. Service – in contrast to the traditional identification methods – is a probability variable, mostly affected by the FRR (False Rejection Rate) value of the system. ξ probability variable can be defined thusly: Let r be the number of users that within a given timeframe that are rejected by the system, if the enrolled number of users is n. If so, then ξ by definition has a binomial distribution:

$$P(\xi = r) = \binom{n}{r} p^r (1-p)^{n-r}; r = 0, 1, 2, \dots, n$$

The relative probability stochastically converges on p probability, if the number of observations n is increasing beyond all limits. If we wish to estimate this parameter, then the best method is Maximum Likelihood, that, in our case, is equal to the FRR itself. A more detailed deduction can be found in Hanka's publication (Hanka, 2013). From this definition of FRR – which our measurements confirm – comes that the probable run time for the algorithm is the highest in this case compared to any successful identification, since to establish a false rejection, the entire database has to be checked against the present sample (in 1:N identification, where no preselection exists with PIN or card), and the users must present the sample again, which means another full run of the identification cycle. These two factors increase the time required for a false rejection to around two- or threefold of a normal identification. This also means that the dispersion of service times is greatest for biometric identification, furthermore, FRR directly affects service performance, which is critical for access control and attendance tracking applications (Hanka & Werner, 2015, pp. 209-216).

The purpose of access control is typically tied to the operation of a physical barrier, however in high-security facilities, security methods beyond this are usually deployed. The Table no. 1 summarizes the typical elements and the service times given by the manufacturer versus the empirically obtained ones.

Table no. 1

The typical elements of an access process

Name	Service time (s)	Average (s)	μ (service/minute)	Notes
Card based identification	1-2	1,5	40	
PIN code	1-4	2,5	24	
Biometric identification	1-9	5	12	The large dispersion is due to FRR
Door	0-2	1	60	Magnetic lock, door holding magnet.
Turnstile, turning cross, fast gate	2-3	2,5	24	20-30 person/minute throughput
Turnstile, one person	3-10	6,5	9,23	
Guest registration	30 – 180	105	0,57	ID card checking, data recording, issuing the card, notifying escort.
Bag x-ray	30 – 150	90	0,67	
Metal detector gate	10 – 30	20	3	
Body search	20 - 60	40	1,5	

6. Mathematical Model of the System

The mathematic model was mainly developed based on the work of Hillier and Lieberman: "*Introduction to operations research"*. Beyond this, we also utilized *"The basis of queuing theory"* from János Sztrik, *"Queue Modelling and Simulation"* from Fischwick, and *"Development and introduction of access gate placement strategy demonstrated through a select number of metro stations"* from József Lukács (Hillier & Lieberman, 2014; Sztrik, 2011; Fishwick & Hyungwook, 2008; Lukács, 2014). In this article the access control system is considered as a queuing system. Customers are registered users in the system, and the service is the *"access"* it self. Consequently, the mathematical description of control system is given by the characteristic values of a queuing system. These essential values are the average number of customers in the system, expected queue length, the mean waiting time in the system, including service time, and the expected waiting time in the queue, denoted by L, L_q, W and W_q respectively. The value of these quantities is the most important question for the employer and for employees as well. These values depend on the mean arrival rate, and mean service rate, denoted by λ and μ respectively. These quantities are by definition the number of arrivals and the number of served customers per unit time respectively. The reciprocal of these values has illustrative meaning, these are mean interarrival time and mean service time respectively. In general, these rates may depend on the number of customers in the system, but it is acceptable, that considering an access control system, the arrival rate and the service rate is independent to the state of the system, in other words, to the number of customers, hence these quantities are constant. The following fundamental question is the number of channels in the system, which is denoted by s. Obviously, if the number of registered users is great enough, a single-server system is not satisfactory, consequently a multiple-server system is necessary. The appropriate number of channels is the fundamental question of this article, and is discussed below. Moreover, since arrivals and services are independent, it is also obvious that the interarrival time distribution and the service time distribution can be given by exponential distribution, so the $M/M/1$ and the $M/M/s$ model can be applied for the access control system. The state of the system is always given by the probability distribution $P_n(t)$, which denotes the probability of the event, that there are n customers in the system at time t. This distribution depends on t in general, but if the utilization factor, $\rho = \frac{\lambda}{\mu s}$ is less than 1, the system can reach the steady state condition, therefore the distribution in this case is independent to time, and expected values can be calculated. L, L_q, W and W_q are the interested expected values. The relationships between these expected values, and the simplest mathematical formulas at the same time are Little's formulas:

$$L = \lambda W;\ \ L_q = \lambda W_q;\ \ W = W_q + \frac{1}{\mu}.$$

If at least one of the four quantities are known, every other can be calculated using these equations. The mathematical formulas are much simpler if the calling population, in other words the number of registered users is infinity. But apparently, the size of the population is always finite, therefore the difference between finite and infinite mathematical model must be studied for the first time. Due to Little's formulas, it is enough for example focusing on L_q. For the single-server system, if the size of the population is infinity, L_q can be calculated using the following formulas:

$$P_0 = \left[\sum_{n=0}^{\infty}\left(\frac{\lambda}{\mu}\right)^n\right]^{-1} = 1-\rho;\quad P_n = P_0\rho^n;\quad L_q = \sum_{n=1}^{\infty}(n-1)P_n = \frac{\lambda^2}{\mu(\mu-\lambda)};\quad \rho = \frac{\lambda}{\mu}.$$

If the size of the population is finite, let it be N, then the difference is that the probability distribution P_n is obviously different and the sum in the definition of L_q is a finite sum:

$$P_0 = \left[\sum_{n=0}^{N}\left(\frac{\lambda}{\mu}\right)^n\right]^{-1};\quad P_n = P_0\rho^n;\quad L_q = \sum_{n=1}^{N}(n-1)P_n.$$

But these results can be given by much complicated formulas. For the multiple-server system, if the size of the population is infinity, L_q can be calculated using the following formulas:

$$P_0 = \left[\sum_{n=0}^{s-1}\frac{(\rho s)^n}{n!} + \frac{(\rho s)^s}{s!(1-\rho)}\right]^{-1};\quad P_n = \begin{cases}\dfrac{(\rho s)^n}{n!}P_0; & if \quad 0 \le n \le s\\ \dfrac{(\rho s)^n}{s!s^{n-s}}P_0; & if \quad s < n\end{cases};\quad L_q = \sum_{n=s}^{\infty}(n-s)P_n = \frac{P_0\rho(\rho s)^s}{s!(1-\rho)^2}.$$

where in this case $\rho = \dfrac{\lambda}{s\mu}$. If the size of the population is N, assuming that $N > s$, the difference is that the second term in the definition of P_0 must be replaced by the sum $\dfrac{(\rho s)^s}{s!}\sum_{n=s}^{N}\rho^{n-s}$, P_n can be calculated in the same way if $n \le N$, and the expected value of queue length is given by the following sum: $L_q = \sum_{n=s}^{N}(n-s)P_n$. The outcome of the calculations for the finite case is also much complicated. Comparing finite and infinite model, let's consider a hypothetic situation. Assume for example, that $\lambda = 7, \mu = 10$ and that the number of registered users is extremely low, for example N =10. It can be seen immediately, that difference between models is observable only if s =1. If $s \ge 2$ then the curves are practically coincided. Remarkable difference can be observed only if the number of channels is s = 1. But if the number of registered users is a few hundred, the single-server case is not satisfactory at all. Taking into consideration a situation, when the size of the calling population is 500, the mean arrival rate and mean service rate for a particular unit time is λ = 50 and μ = 70, the corresponding expected values can be seen in Tables no. 2 and no. 3.

Table no. 2

The expected values of customers in the system in case of infinite and finite model, if N = 500

	L		L_q	
channels	infinite	finite	infinite	finite
1	2.500000000000000	2.500000000000001	1.785714285714286	1.785714285714286
2	0.818713450292398	0.818713450292398	0.104427736006683	0.104427736006683
3	0.726443355119826	0.726443355119826	0.012157640834111	0.012157640834111
4	0.715690500989644	0.715690500989644	0.001404786703930	0.001404786703930
5	0.714433200854997	0.714433200854997	0.000147486569283	0.000147486569283
6	0.714299566011384	0.714299566011384	0.000013851725669	0.000013851725669
7	0.714286880352793	0.714286880352793	0.000001166067078	0.000001166067078

Table no. 3

The expected values of time in case of infinite and finite model, if N = 500

	W		W_q	
channels	infinite	finite	infinite	finite
1	0.050000000000000	0.050000000000000	0.035714285714286	0.035714285714286
2	0.016374269005848	0.016374269005848	0.002088554720134	0.002088554720134
3	0.014528867102397	0.014528867102397	0.000243152816682	0.000243152816682
4	0.014313810019793	0.014313810019793	0.000028095734079	0.000028095734079
5	0.014288664017100	0.014288664017100	0.000002949731386	0.000002949731386
6	0.014285991320228	0.014285991320228	0.000000277034513	0.000000277034513
7	0.014285737607056	0.014285737607056	0.000000023321342	0.000000023321342

Subsequently if the size of calling population is a few hundred and if the finite model is applied for modelling, the obtained data are exactly equal to corresponding data obtained in the infinite model. Therefore, the infinite queuing model can be applied for modelling an access control system in which there are finite number of registered users. Characteristic values of a queuing system depend on the utilization factor as well. Using formulas for L_q and applying Little's formulas, the correspondence can be illustrated. Figure 2 depicts the dependence of L and W on the utilization factor for various numbers of channels using logarithmic y-scale, for a particular value of mean arrival rate ($\lambda = 10$).

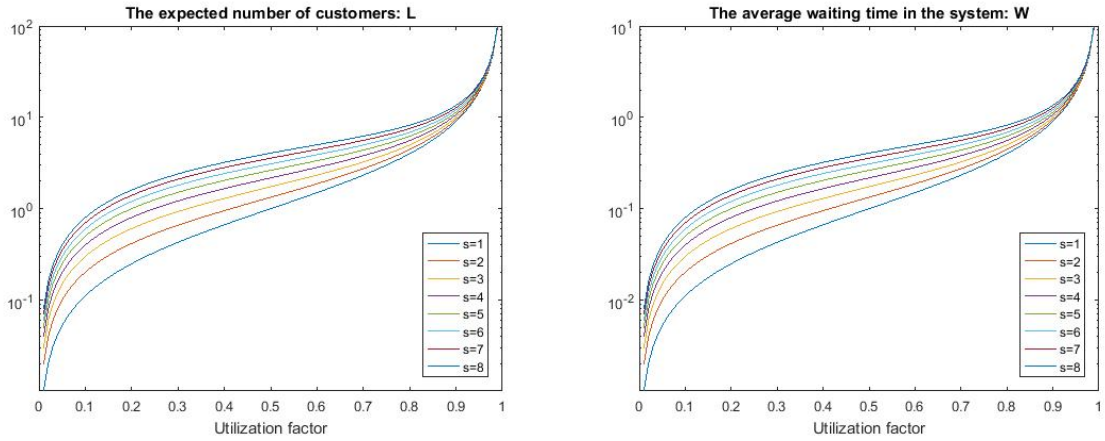


Figure no. 2: *The expected number of customers in the system (left) and the average waiting time in the system, including service time (right)*
(Source: own edit)

Due to Little's formulas, $\lambda W = L$, hence the relationship between W and L only a constant factor, the shape of curves above are similar. These relationships can be used for planning an access control system. For example, if there is a requirement for the waiting time in the system, the planner can determine for instance the appropriate number of channels. Taking into consideration a real problem, assume that in a particular access control system, the average service time is 13s. The number of customers is known between 6:00 a.m. and 7.00 a.m. According to observations, the average number of users between 6:00 to 6:20 were 185, between 6:20 to 6:40 were 275 and between 6:40 to 7:00 were 202. Therefore, the unit time in this case is 20min. Since the average service time is 13s, the mean service rate is $\mu = \frac{1200}{13} = 92.3$. Since the system has steady state probability distribution only if the utilization factor is less than 1, taking

into account the maximal number of arriving customers, the number of channels must satisfy the following inequality:

$$\rho = \frac{\lambda}{s\mu} = \frac{275}{93.1 \cdot s} < 1 \Rightarrow s \geq 3$$

Therefore at least 3 channels must be applied in the system. The requirement is that, the average waiting time must be less than 1 minute. Using these data, L, L_q, W and W_q can be computed if s is at least 3. The outcome of calculations can be seen on Figure no. 3.

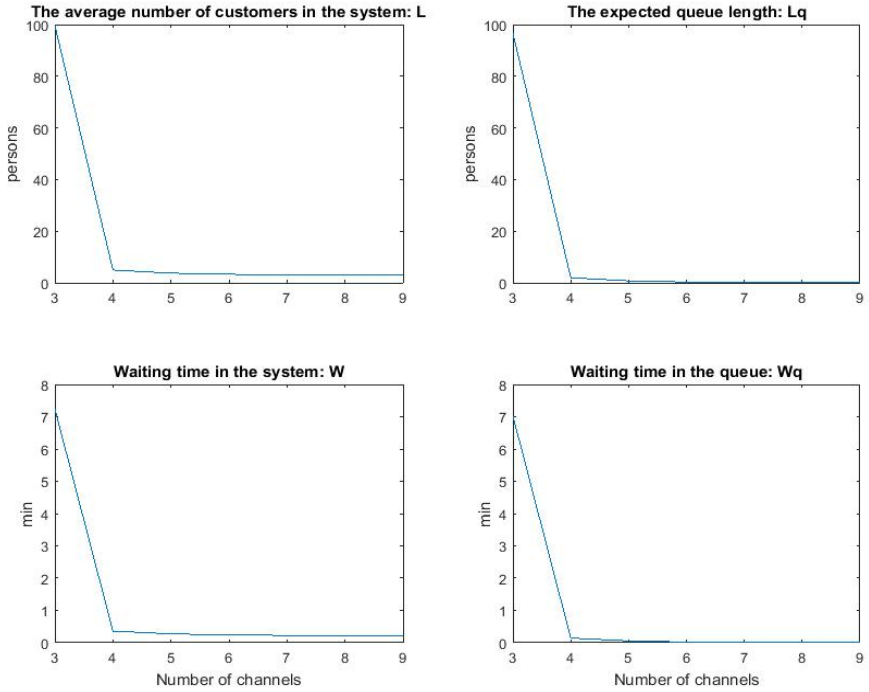


Figure no. 3: *Characteristic values for the system given by parameters: λ =275, μ = 92.3, T = 20 min.*

It can be seen that if the number of channels is 3, then either the waiting time in the system or the waiting time in the queue is approximately 7 minutes, which is unacceptable for the employees. But if the number of channels is at least 4, these waiting times are less than 1 minute. Moreover, it is also obvious, that if s is at least 4 the time functions and the queue length function are approximately constant functions, consequently s = 4 the optimal decision. The growing number of channels won't improve the characteristic values, every expected value practically stays the same. Table no. 4 comprises the calculated data for this particular case.

Table no. 4

The characteristic values of the system for various channels if λ =275, μ = 92.3, T = 20 min

number of channels	L (persons)	L_q (persons)	W (min)	W_q (min)
3	99.5432	96.5638	7.2395	7.0228
4	4.9559	1.9765	0.3604	0.1437
5	3.7471	0.7677	0.2725	0.0558
6	3.3011	0.3217	0.2401	0.0234
7	3.1072	0.1278	0.2260	0.0093
8	3.0261	0.0466	0.2201	0.0034
9	2.9950	0.0155	0.2178	0.0011

The remaining question can be the following. The actual number of customers is random; therefore, it can be described by a probability distribution. The average number of the customers can be seen in Table no. 4. But these data are *"only"* expected values of a probability distribution. The question can be the probability of the event, that there are a specified number of customers. Table no. 5 comprises these probabilities and Figure no. 4 illustrates these probabilities graphically.

Table no. 5

The probability of the event that there are n customers in the s-server system

	n = 0	n = 1	n = 2	n = 3	n = 4	n = 5	n = 6	n = 7	n = 8	n = 9	n = 10
s = 3	0.0015	0.0046	0.0068	0.0068	0.0067	0.0067	0.0066	0.0066	0.0065	0.0065	0.0065
s = 4	0.0389	0.1160	0.1727	0.1716	0.1278	0.0952	0.0709	0.0528	0.0393	0.0293	0.0218
s = 5	0.0477	0.1422	0.2119	0.2104	0.1567	0.0934	0.0556	0.0332	0.0198	0.0118	0.0070
s = 6	0.0500	0.1490	0.2220	0.2205	0.1642	0.0978	0.0486	0.0241	0.0120	0.0059	0.0030
s = 7	0.0506	0.1508	0.2247	0.2231	0.1662	0.0990	0.0492	0.0209	0.0089	0.0038	0.0016
s = 8	0.0508	0.1513	0.2253	0.2238	0.1667	0.0993	0.0493	0.0210	0.0078	0.0029	0.0011
s = 9	0.0508	0.1514	0.2255	0.2240	0.1668	0.0994	0.0494	0.0210	0.0078	0.0026	0.0009

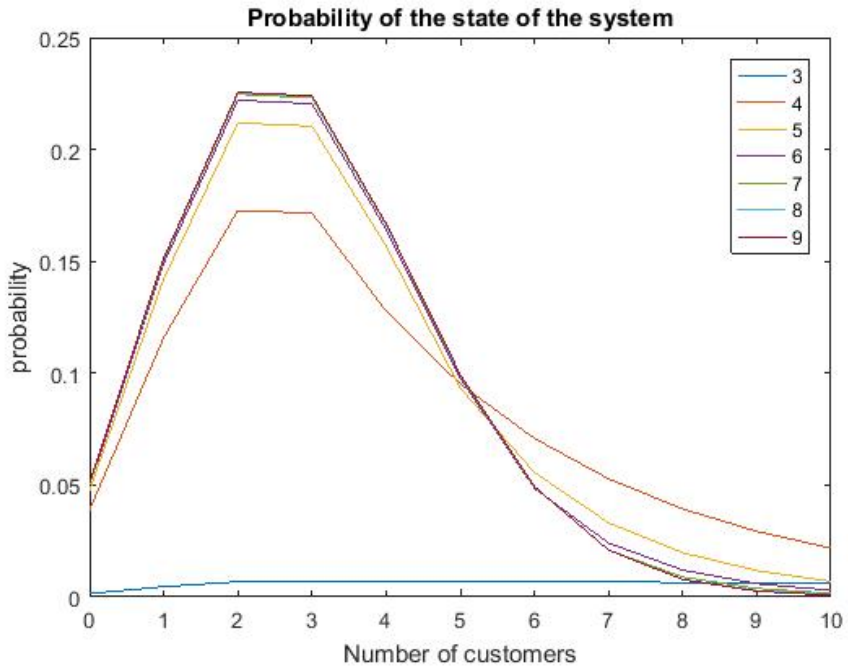


Figure no. 4: *The probability of the particular state of the system*

7. Summary

The study demonstrated a useful method for constructing a stochastic model with a Markov chain for access control systems and new analysis methods based on said method. We can state, based on the results of this study, that this analysis method is suitable for ensuring quality and supporting business decisions through the design phase of biometric or generic access control systems. The goal of the authors is to ensure successful introduction of access control projects for high headcount facilities with respect to business and security requirements and standpoints, to create process- and system analysis methods through mathematical simulation, and – by using case studies – to demonstrate its practical usability. These goals are fulfilled, and in practice, the designing engineers of access control systems are given a new and powerful methodology that is useful in practice.

REFERENCES

54/2014. (XII. 5.) *BM Decree on the National Fire Protection Regulations* (2014). Budapest: National Legislation.

Berek, L. (2014). *Security Systems*. Budapest: National University of Public Service.

Bunyitai, A. (2011). Location and role of access control systems in asset protection. Budapest: *Hadmernok, VI.(4.),* 17-25.

Fishwick, P. A., & Hyungwook, P. (2008). *Queue Modeling and Simulation. In Principles of Modeling and Simulation: A Multidisciplinary Approach.* New Jersey, USA: John Wiley & Sons, Inc.

Hanka, L. (2013). Applications for using binomial distribution in functioning identification systems, the application of maximum likelihood principle. *Spring Technical Symposium*, Budapest, Hungary: University of Obuda.

Hanka, L., & Werner, G. (2015). Using the Beta-Binomial Distribution for the Analysis of Biometric Identification. *13th International Symposium on Intelligent Systems and Informatics: Proceedings,* 209-216, Subotica, Serbia.

Hillier, F. S., & Lieberman, G. J. (2014). *Introduction to Operations Research.* New York, USA: McGraw-Hill Higher Education.

Hungarian Standards Institution. (2015). MSZ EN 60839-11-2:2015. *Alarm systems and electronic security systems. Part 11-2.: Electronic access control systems. Application Guidelines*. Budapest: Hungarian Standards Institution.

Kendall, D. G. (1953). Stochastic processes occurring in the theory of queues and their analysis by the method of imbedded Markov chain. *Annals of Mathematical Statistics, Vol. 24, Issue 3*, 338-354.

Kleinrock, L. (1975). *Queueing Systems Volume 1: Theory.* New York: Wiley - Interscience.

Law, A. M. (2015). *Simulation Modeling and Analysis. 5th Edition.* Tucson, Arizona, USA: McGrow-Hill .

Little, J. D. (1961). A proof of the queuing formula: l = λw. *Operations Research, Vol. 9(3),* pp. 383-387, available at: http://fisherp.scripts.mit.edu/wordpress/wp-content/uploads/2015/11/ContentServer.pdf

Lovász, L. (2009). *Complexity of Algorithms.* Budapest: ELTE, Institute of Mathematics.

Lukács, J. (2014). *Develop and present an access gate placement strategy through a few selected subway stations*. Budapest: BME Budapest University of Technology and Economics.

Otti, C. (2015). Classification of biometric access control systems based on real-time throughput. *Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates*, Bratislava, 63-71.

Otti, C. (2016). Biometric Systems User Pattern Positioning Issues. *DOSZ, Spring Wind Conference,* 251-260, Budapest.

Pap, G., & Szűcs, G. (2014). *Stochastic processes.* Szeged, Hungary: STE Institution of Bolyai, Stochastic Department.

Pokorádi, L. (2008). *Modeling of systems and processes.* Debrecen, Hungary: Campus Kiado.

Szeidl, L. (2009). *Mass Service.* Budapest, Hungary: University of Obuda, Institute of Informatics.

Sztrik, J. (2011). *Basics of queuing theory.* Debrecen, Hungary: University of Debrecen.

HADMÉRNÖK

XII. Évfolyam 2. szám – 2017.június

BELÉPÉSI PONTOK MEGHATÁROZÁSA MARKOVI MODELLEL, NAGY LÉTSZÁMÚ ÜZEMEK BIOMETRIKUS BELÉPTETÉSÉNÉL

DETERMINATION OF ACCESS POINTS WITH THE MARKOV MODEL FOR BIOMETRIC ACCESS CONTROL IN LARGE HEADCOUNT PLANTS

OTTI CSABA

(ORCID: 0000-0002-9266-639X)

otti.csaba@bgk.uni-obuda.hu

Absztrakt

A beléptető rendszerek méretezése jellemzően a menekülési útvonalakra vonatkozó életvédelmi szempontok szerint történik. Nagy létszámú beléptetési helyeken az ezen túlmutató biztonsági és üzleti igények miatt sokszor felmerül a biometrikus azonosítás igénye. A biometrikus rendszerek működése valószínűségi változókkal jellemezhető, amely jelentősen képes befolyásolni a belépési folyamatot.
Matematikai szempontból a belépetés egy diszkrét állapotterű, emlékezet nélküli sztochasztikus folyamat, így az Markov lánccal írható le.
Jelen tanulmány bemutatja a beléptető rendszerek folyamatmodelljét, valamint számítási eljárásokat ad meg a tervezéshez amellyel biztosítható a bevezetési projekt sikeressége.

Kulcsszavak: *beléptetés, beléptető rendszer, biometria, sorbanállás, markov lánc*

Abstract

The scaling of access control systems is usually done with respect only to the life protection rules pertaining escape routes. However, in the case of access points with a large traffic, further business and security requirements point towards biometric identification. Operation of such systems can be characterised by probability variables that can affect the access procedure significantly.
From a mathematical standpoint, access control is a discrete state space stohastic process without a memory and thus can be described with a Markov chain.
This study will first demonstrate the process model of access control systems and then provide calculation processes to aid the design of such systems which can ensure the success of their introudction.

Keywords: *access control, access control system, biometrics, queuing, Markov chain.*

A kézirat benyújtásának dátuma (Date of the submission): 2017.04.11.
A kézirat benyújtásának dátuma (Date of the submission): 2017.05.16.

BEVEZETÉS

A beléptető rendszerek biztonsági felhasználása természetessé vált a vállalati alkalmazásokban. Általában különösebb megfontolást és méretezést [1, p. 59§ (8)] – a menekülési útvonalakon szükséges előírásokon túlmenően - nem igényelnek ezek a rendszerek. Problémák ott merülnek fel ahol vagy hosszadalmas a beléptetési procedúra az objektum biztonsági fokozata miatt (fémkereső kapu, csomagátvizsgálás) vagy nagy létszám érkezik rövid idő alatt[1]. A belépési folyamat egyes lépései jól azonosíthatók és becsülhető az időtartamuk, azonban biometrikus beléptetés esetén valószínűségi változóval leírható [2, p. 69] tevékenységet viszünk a rendszerbe, mely működési bizonytalansága komoly kockázatot jelent a teljes rendszerbevezetés sikerességének összefüggésében. Ezért fontos, hogy kidolgozásra kerüljön egy olyan eljárás, amely az üzleti és biztonsági kérdésekre [2, p. 64] egyértelmű, megbízható válaszokat szolgáltat már a tervezési szakaszban.

Jelen tanulmány tudományos megközelítéssel vizsgálja a beléptető rendszereket, amelyek egy objektumba történő személybeléptetés a belépés előkészítésére, az ellenőrzési feladatokra, az azonosításra, és az APAS (Access Point Actuators and Sensors - Beléptetőpont működtetett szerkezetei és érzékelői)[2] működtetésére épülő sztochasztikus folyamatként írhatók le [3]. A belépési folyamat modellvizsgálatával megállapítható, hogy a távozások függetlenek a múltbeli eseményektől, az csak a vizsgált időpont állapotától függ, ez alapján matematikailag Markov folyamatnak tekinthető és sorbanállási modellel leírható [4, pp. 156-158].

A publikáció célja a fenti üzemeltetéselméleti, valószinűségszámitási, matematikai modellezési, valamint műszaki diagnosztikai munkák tudományos eredményeinek, módszereinek összegzése és a kitűzött specifikus alkalmazás a beléptetési folyamatainak sorbanállási modellel történő leírása, illetve gyakorlati alkalmazásuknak vizsgálata.

A tanulmány az alábbi részekből áll: a 2. fejezet a beléptetési folyamatot és állapotokat mutatja be. A 3. fejezetben ismertetésre kerül a sorbanállási modell, majd az előzőek alapján a 4. fejezetben kidolgozásra kerül a beléptetési folyamat markovi modellje. Az 5. fejezet példákat mutat be az alkalmazásra, a 6. fejezet összegzi a tanulmányt.

A BELÉPTETÉS

A beléptető rendszer Bunyitai szerint: „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.” [5, p. 18] A beléptető rendszer feladata pedig : „a belépő azonosítása, a belépési jogosultság megállapítása, az esemény dokumentálása, valamint az áthaladás szabályzása.”

A beléptető rendszerek általános felépítése:

- Olvasók: az azonosítási ponthoz érkező felhasználót azonosítja. Lehet kódos, kártyás, biometrikus vagy ezek kombinációja.
- Vezérlők: az olvasó által azonosított kódról dönti el, hogy az adott helyen és időben jogosult-e a belépésre a felhasználó.
- APAS: A rendszer által vezérelt fizikai korlátozó és mechanikus eszközök, illetve érzékelők tartoznak közéjük. A vezérelt eszközök lehetnek: mágneszár, ajtótartó mágnes, forgóvilla, forgókereszt, forgókapu, automata ajtó, stb. Érzékelők például infrakapu, nyitásérzékelő vagy mozgásérzékelő.

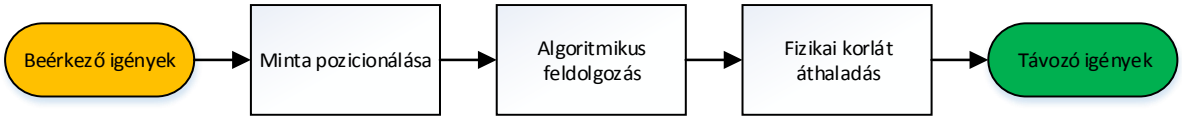
[1] A két jelenség együttes fellépésére jó példa a repülőtér, de ott meg azért nem probléma, mert az emberek kivárják a sorukat, akár több órás várakozási idővel is. Ez nyilván nem elfogadható egy munkahelyi beléptetésénél.

[2] Például egy mágneszár, forgóvilla vagy nyitásérzékelő.

– Felügyeleti szoftver: a rendszer és felhasználói beállítások kezelésére, valamint a rendszer begyűjtött jelzéseinek feldolgozására, naplózására, tárolására szolgáló alkalmazás.

A beléptetési folyamat állapotai

A beléptetési folyamat állapotait a **1. ábra** mutatja be.



1. ábra: A beléptetési folyamat állapotai; forrás: [2]

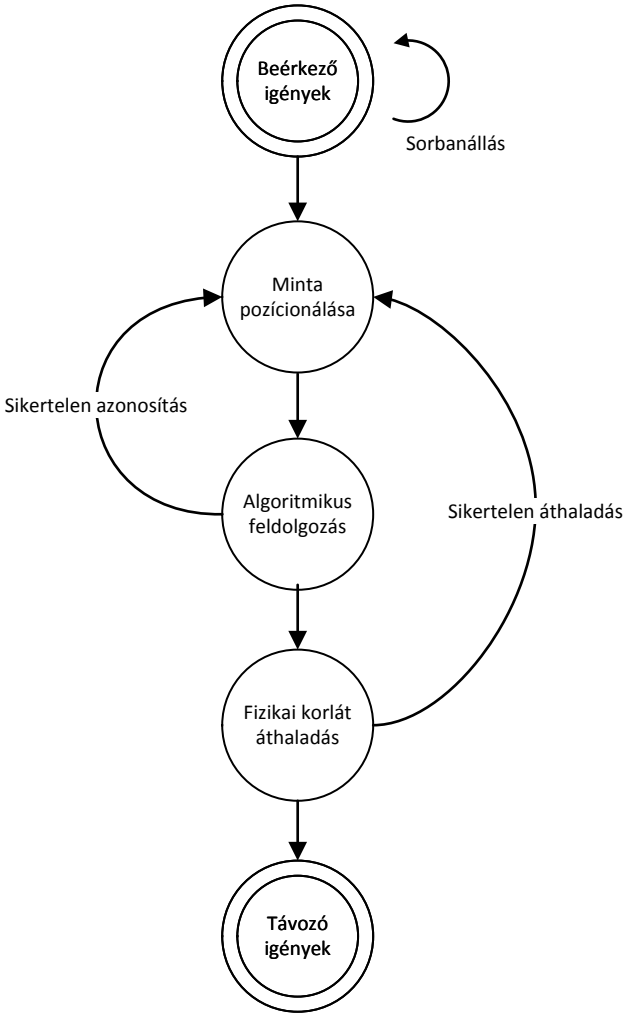
Az egyes állapotok leírása és jellemzői:

– Beérkező igények: A dolgozó vagy felhasználó megérkezik az áthaladási ponthoz és sorbanáll.
– Minta pozícionálása: A felhasználó felkészül az azonosításra és biometrikus mintáját a szenzornak bemutatja, hogy áthaladhasson. Analóg módon értelmezhető a kártyás beléptetésnél a kártya olvasóhoz történő érintése.
– Algoritmikus feldolgozás: A prezentált mintát feldolgozza az olvasó és sikeres vagy elutasított jelzést ad. Ezt a lépést csak a biometrikus rendszereknél értelmezzük, és itt tapasztalható meg a biometria valószínűségi jellege, mivel soha nem 100%, hogy egy jogosult személy elsőre át fog tudni haladni az azonosítási ponton. Másik következménye a tulajdonságnak - ami biztonsági kockázatot hordoz magában -, hogy az sem biztos 100%-ig, hogy egy jogosulatlan nem jut át. Ez a valószínűségi jelleg kártyás vagy PIN kódos rendszereknél nem áll fenn.
– Fizikai korlát áthaladás: A sikeres azonosítást követően a vezérlő jelet ad a fizikai korlátozó elemnek, hogy az áthaladást tegye szabaddá.
– Távozó igények: a felhasználó elhagyja az azonosítási pontot.

Egy ideális környezetben a jogosultak mindig át tudnak haladni az azonosítási ponton, a támadókat pedig mindig elutasítja a rendszer, ezért ismerni kell azokat a pontokat, ahol a valóságban ettől eltérően működhet a rendszer.

– A Beérkező igények lépésnél sorbanállás lehetséges.
– A Minta pozícionálása lehet sikertelen, például: nem jól teszi oda az ujját az ujjnyomat azonosító szenzorra, szakállat növeszt és emiatt nem működik az arcfelismerő, elejti a kártyát, stb.
– Az algoritmikus feldolgozás rossz eredményt ad vissza és újra kell próbálkozni.
– A fizikai korlát nem működik megfelelően, beragad az ajtó, nem fordul át a korlát vagy a felhasználó használja rosszul az eszközt, például túl gyorsan lép be a villához, ami emiatt megszorul és újra kell próbálkozni.

Ezek alapján a belépési folyamat leírható egy, a **2. ábra** látható irányított gráffal.



2. ábra: Belépési folyamat gráfja; forrás: saját.

SORBANÁLLÁSI MODELL

Sorbanállási rendszerek az élet számos területén előfordulnak, ahol kiszolgálás történik valamilyen elosztott erőforrás hozzáféréséhez. Bármely rendszer, ahol a vevő kiszolgálása véges erőforrással történik, tekinthető sorbanállási rendszernek. [6] Ilyen rendszerekre példa egy fagyizóban a fagyira várakozás, egy banki sor, a repülőgépek leszállási és karbantartási kiszolgálása, a számítógép processzorának adatfeldolgozása vagy akár a vizsgára várakozó hallgatók is.

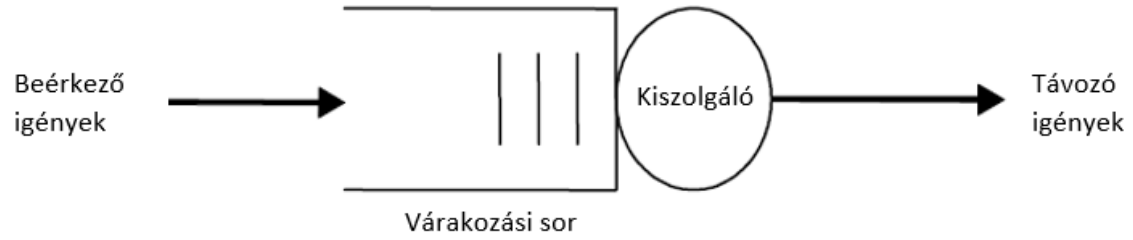
Pokorádi szerint *„Sorbanállási, kiszolgálási rendszeren olyan rendszert értünk, amelybe a fogyasztók véletlenszerűen érkeznek be, az eltérő igényeik kielégítésére várnak, majd a kiszolgálásuk után távoznak.”*. [4, pp. 173-175] A sorbanállási rendszereket Tömegkiszolgálási Rendszernek is szokás nevezni. A sorbanállási problémákat analitikus modellezéssel vagy szimulációs eljárásokkal lehet becsülni, elemezni és értékelni. Az analitikus eljárás egyszerűbb sorbanállási rendszereknél használható, ahol a valóságos folyamat feltételeinek szűkítésével egyszerűen előállíthatók a modell egyenletei. A valóságban sokszor nagyon nehéz leírni egy ilyen rendszert, mert nem vehető figyelembe minden tényező vagy olyan bonyolult egyenlet keletkezik amely algoritmikus futásideje nem polinomiális idejű. [7, pp. 42-43] Ezekben az esetekben hatékony vizsgálati eljárás a

szimulációs módszer. A működési elve az, hogy a rendszer működést szimuláljuk nagy elemszámmal és ezek eredményeiből vonjuk le a következtetéseket. [8, p. 78]

Ezekben a rendszerekben közös:

- A rendszer felépítése.
- Beérkező igények.
- Várakozási sorok.
- Kiszolgálók.
- Kiszolgálás.
- Távozó igények.

A 3. ábra a legegyszerűbb sorbanállási rendszert ábrázolja sematikusan.



3. ábra: Legegyszerűbb sorbanállási rendszer, forrás: [8]

Sztochasztikus folyamat

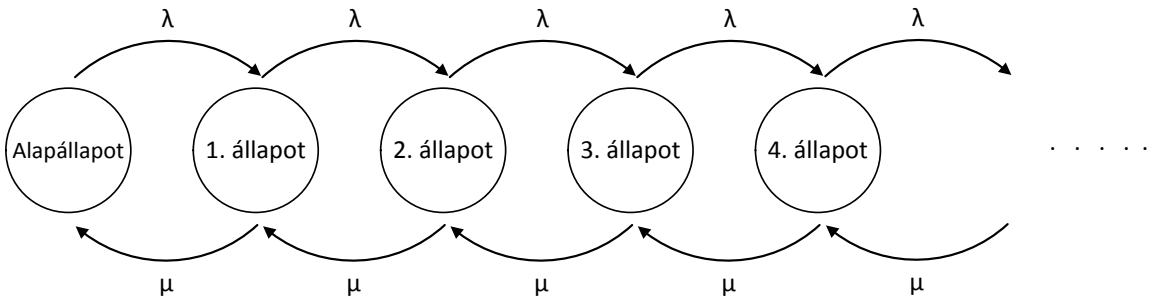
A műszaki tudományok területén sokszor előfordul az a helyzet, hogy az analízishez szükséges alapvető mennyiségek $\{X(t), t \in T\}$ alakulása a véletlenen múlik. Ezek a mennyiségek jellemzően a vizsgált tényező idő és/vagy térbeli változásait írják le. Ekkor az $\{X(t), t \in T\}$ mennyiségeket értelmezhetjük a T paraméterhez tartozó valószínűségi változók együtteseként. Ha T paraméterhalmaz a pozitív félegyenes $T \subseteq [0, \infty)$ részhalmaza lesz, akkor t tekinthető időparaméternek, röviden időnek. A valós számok halmaza rendezett, ezért értelmezhető a folyamat múltja és jövője. Ha jelen időpillanatnak tekintjük $t \in T$ rögzített értéket akkor értelmezhető az $\{X(s): s > t\}$ folyamat jövője, az $\{X(s): s < t\}$ pedig a múltja. [9, pp. 3-5]

Markov folyamat

Markov folyamatnak nevezzük azokat a sztohasztikus folyamatokat, amelyek jövőbeli állapotait a folyamat múltja csak a jelen állapoton keresztül befolyásolja, más szóval a folyamat emlékezet nélküli. Ha például egy forgóvillás beléptető kapunál öten állnak sorban, akkor mindegy, hogy az úgy alakult ki, hogy hatan voltak és egy áthaladt, vagy hárman voltak és ketten még érkeztek hozzá.

A beléptetési folyamat tekinthető folytonos idejű, diszkrét állapotterű Markov folyamatnak, más néven Markov láncnak.

A 4. ábra egy egy kiszolgálós sor, diszkrét állapotterű Markov lánc reprezentációját mutatja be.



4. ábra: Egy csatornás Markov lánc; forrás: saját.

Minden állapot a rendszerben várakozók és aktuálisan kiszolgálásra kerülők darabszámát jelenti. A rendszerben várakozók számának növekedését a λ - érkezési intenzitás, a csökkenésüket pedig a μ - kiszogálási intenzitás írja le. A rendszer alapállapota az, hogy senki nincs a rendszerben.

Kendall jelölésrendszere

A tömegkiszolgálási rendszerek leírásához szükséges általános jelölésrendszert Kendall publikálta 1953-ban. E szerint a sorbanállási rendszerek típusai akkor írhatók le, ha ismerjük a beérkezési eloszlást, a sor tulajdonságait és a kiszolgálási mechnaizmust. [10, pp. 338-340] Jelen dolgozat céljait legjobban Sztrik „A sorbanállási elmélet alapjai" című könyvének modellje szolgálja ki. [11] A sorbanállási rendszerek jellemzésére használható jelölésrendszer:

$$A / B / m / K / n / E$$

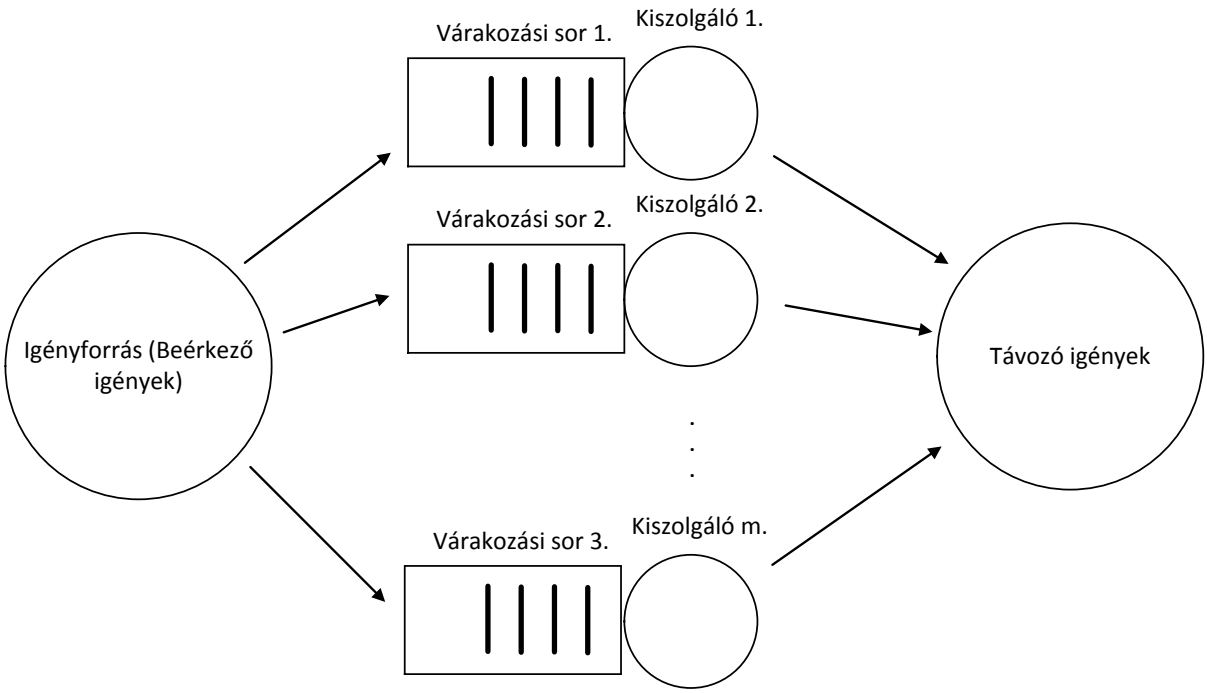
ahol:

- A - a beérkező igények idejének eloszlásfüggvénye.
- B: a kiszolgálási idők eloszlásfüggvénye.
- m: a kiszolgálók száma.
- K: a rendszer befogadóképessége, azaz a kiszolgálóegységben és a várakozási sorban tartózkodó igények maximális száma.
- n: az igényforrás számossága.
- E: a kiszolgálás elve.

Az eloszlásfüggvények (A,B) lehetnek determinisztikus (D), exponenciális (M) vagy általános (G) típusúak. A rendszer befogadóképessége (K) és igényforrása (n) lehet véges vagy végtelen, általában ez utóbbit alkalmazzuk. A kiszolgálás elve (E) lehet FIFO (First In First Out – az elsőként beérkező kerül először kiszolgálásra), LIFO (Last In First Out – az utolsóként beérkező kerül elsőként kiszolgálásra), véletlenszerű vagy prioritásos.

A BELÉPTETÉSI FOLYAMAT MODELLJE

A beléptető rendszerek általában több kiszolgáló egységből álló párhuzamos kiszolgálóegységes rendszerként írhatók le, grafikusan az **5. ábra** mutatja be általános formában.



5. ábra: Több kiszolgálós beléptető rendszer modellje; forrás: saját.

A sorbanállási rendszerek matematikai tárgyalásához szükséges, hogy néhány megszorítást tegyünk a feltételekben. Ezek érdemben nem befolyásolják a modell valósághűségét, azonban ha mégis el kell ezektől térnünk, akkor valamilyen szimulációs eljárás használható a modellezésre. [12] A feltételeket Kendall jelölésrendszere alapján vesszük sorra. A beérkező igények eloszlásfüggvénye Poisson eloszlású, a kiszolgálási idők eloszlásfüggvénye szintén exponenciális, a kiszolgálók száma m – véges, természetes szám, a rendszer befogadóképessége és az igényforrás számossága végtelen, a kiszolgálás elve FIFO. Ez alapján a beléptető rendszerek modellje: *M/M/m/∞/∞/FIFO*. Ilyen esetekben az utolsó három paramétert nem szokás kiírni, ez alapján egy egy csatornás beléptető rendszer *M/M/1*, egy több csatornás *M/M/m* tömegkiszolgálási rendszerrel modellezhető.

A biometrikus beléptetés

A világban tapasztalható biztonságérzet csökkenésével párhuzamosan egyre nagyobb az igény a felhasználók hiteles azonosítására. Egyedül a biometrikus azonosítás az a technológia, amely az emberek egyedi, lehetőség szerint megmásíthatatlan és hamisíthatatlan tulajdonságait vizsgálja. A jelenlegi rendszerek sem sebezhetetlenek, azonban a folyamatos fejlesztéseknek köszönhetően egyre magasabb biztonsági és kényelmi elvárásoknak felelnek meg. [13, pp. 251-253]
Biometrikus technológiák csoportosítása:

- Képalkotás alapú technológiák
  - Ujjnyomat azonosítás
  - Írisz azonosítás
  - Arc azonosítás
  - Erezet azonosítás
  - Kézgeometria azonosítás
  - Aláírás vizsgálat
- Nem (vagy nem közvetlenül) képalkotással dolgozó technológiák

- Hangazonosítás
- DNS vizsgálat
- Viselkedés alapú vizsgálatok

A 0-es fejezet 1-es ábráján látható beléptetési folyamatban a biometrikus azonosítás a „Minta pozícionálása" és az „Algoritmikus feldolgozás" lépéseket befolyásolja. A sorbanállási modellt a biometrikus eszközök kiszolgálási tényezője módosítja. A kiszolgálás – ellentétben a hagyományos azonosítási eljárásokkal – valószínűségi változó, mely legnagyobb mértékben a a rendszert jellemző FRR (False Rejection Rate – Hibás elutasítási arány) értéktől függ. Definiálható ξ valószínűségi változó a következő módon: Legyen egy adott időszakban az n db regisztrált felhasználó egyszeri belépése esetén r azok száma akiket a rendszer elutasít. Ekkor ξ definíció szerint binomiális eloszlású:

$$P(\xi = r) = \binom{n}{r} p^r (1-p)^{n-r}; r = 0, 1, 2, \dots, n \quad (1)$$

A relatív gyakoriság sztochasztikusan konvergál a p valószínűséghez, ha a megfigyelések száma, n minden határon túl növekszik. Amennyiben ezt a paramétert szeretnénk becsülni, akkor a legjobb becslés a vizsgált esemény relatív gyakorisága (Maximum Likelihood), ami esetünkben éppen az FRR értékkel egyezik meg. Részletes levezetése Hanka Matematikai módszerek a biometriában 1. publikációjában megtalálható. [14]
Az FRR definíciójából következik – amit a méréseink is alátámasztanak -, hogy

- az algoritmus futási idejének várható értéke a legmagasabb bármilyen sikeres azonosításhoz képest, mivel a téves elutasítás megalapozott meghozatalához a teljes adatbázist végig kell vizsgálni (1:N azonosításnál, azaz amikor nincs előválasztás PIN kóddal vagy kártyával), valamint
- a felhasználónak újra kell a mintát prezentálnia, ami a teljes azonosítási ciklus megismétlését jelenti.

Ez a két tényező a hibás elutasításos azonosítás idejét a normálhoz képest körlbelül két – háromszorosára növeli.
Fentiekből következően a biometrikus eszközök kiszolgálási idejének a legnagyobb a szórása, továbbá az FRR-től közvetlen függ a kiszolgálási idő, amely kritikus a beléptető és munkaidő nyilvántartó alkalmazásoknál. [15, pp. 209-215]

Mérőszámok

A modellalkotás célja, hogy képesek legyünk meghatározni a rendszert jellemző mérőszámokat amelyek leírják a teljesítményét. [11] [16] [17]

Jelölés	Leírás	Megjegyzés
n	Beérkező igények száma	
s	Kiszolgált igények száma	s = $(s_1, s_1, s_1, \dots)$ sorozat, ahol $s_i$az i. ügyfél kiszolgálási idejét jelenti.
T	A vizsgált időintervallum	

1. táblázat: Jelölések

Megnevezés	Képlet	Leírás
Beérkezési intenzitás	$\lambda = \frac{n}{T}$	Beérkező igények száma időegységenként
Kiszolgálási intenzitás	$\mu = \frac{s}{T}$	Kiszolgált igények száma időegységenként
Kihasználtsági tényező (M/M/1)	$\varrho = min\left\{\frac{\lambda}{\mu}; 1\right\}$	A konvergencia feltétele. A gyakorlatban ez azt jelenti, hogy a maximális kiszolgálási kapacitásán működik a rendszer.
Rendszerben tartózkodók átlagos száma (M/M/1)	$N_{\text{á}} = \frac{\varrho}{1-\varrho}$	
Átlagos sorhossz (M/M/1)	$N_S = \frac{\varrho^2}{1-\varrho}$	Fő
Átlagos várakozási idő	$t_{\text{á}} = \frac{N_{\text{á}}}{\lambda}$	

2. táblázat: Egy kiszolgálós beléptető rendszer mérőszámai

Megnevezés	Képlet	Leírás
Beérkezési intenzitás	$\lambda = \frac{n}{T}$	Beérkező igények száma időegységenként
Kiszolgálási intenzitás	$\mu = \frac{s}{T}$	Kiszolgált igények száma időegységenként
Kihasználtsági tényező (M/M/m)	$\varrho = \frac{\lambda}{m * \mu}$	
Egy kiszolgáló egység kihasználtsága (M/M/m)	$a = \frac{\lambda}{m*\mu} = \frac{\varrho}{m} < 1$	
Átlagos sorhossz (M/M/m)	$N_S = P(0)\frac{\left(\frac{\lambda}{\mu}\right)^m}{m!}\frac{a}{(1-a)^2}$	Fő
Rendszerben tartózkodók átlagos száma (M/M/m)	$N_{\text{á}} = \varrho + N_s$	
Átlagos várakozási idő	$t_{\text{á}} = \frac{N_{\text{á}}}{\lambda}$	

3. táblázat: Több kiszolgálós beléptető rendszer mérőszámai

A MÓDSZER ALKALMAZÁSA

A beléptetés funkciója jellemzően valamilyen fizikai korlát működtetéséhez kapcsolódik, azonban kiemelt biztonságú objektumokban ezeken túlmenően további biztonsági lépések is beiktatásra kerülnek. A **4. táblázat** összefoglalja a jellemző elemeket és azok gyártók által megadott illetve valós rendszerekben tapasztalt kiszolgálási idejét.

Megnevezés	Kiszolgálási idő (s)	Átlag (s)	μ (kiszolgálás /perc)	Megjegyzés
Kártyás azonosítás	1-2	1,5	40	
PIN kód	1-4	2,5	24	
Biometrikus azonosítás	1-9	5	12	A kiszolgálási idő nagy szórását az FRR okozza.
Ajtó	0-2	1	60	Mágneszár, ajtótartó mágnes.
Forgóvilla, gyorskapu, forgókereszt	2-3	2,5	24	20-30 ember/perc átbocsátási képesség.
Forgókapu, személyzsilip	3-10	6,5	9,23	
Vendég regisztráció	30 - 180	105	0,57	Személyi igazolvány vizsgálat, adatrögzítés, kártyakiadás, kisérő értesítése
Csomagröntgen	30 – 150	90	0,67	
Fémdetektor kapu	10 – 30	20	3	
Kézi átvizsgálás	20 - 60	40	1,5	

4. táblázat: Belépési folyamat jellemző elemei

Példa egy csatornás beléptetésre

Tekintsünk egy forgóvillás, az adott időszakban egy irányban üzemeltetett belépési pontot, ahova a felhasználók kártyás azonosítással léphetnek be. A kiszolgálás átlagos ideje kártyás azonosítás + forgóvilla működés = 4 s, ebből az egy perces kiszolgálási intenzitás $\mu_{1\ perc}$= 60s / 4s = 15. A dolgozók reggeli beérkezési eloszlása azt mutatja, hogy a legtöbb ember 7 és 8 óra között lép be. Az adatok 15 perces felbontásban állnak rendelkezésre. Ekkor a kiszolgálási intenzitás normalizálható a kiértékelés T időtartamára, ami 15 perc, azaz $\mu_{15\ perc}$= 225. A számításoknál figyelembe kell venni, hogy az eredményeket szintén a vizsgált 15 perces intervallumra kell normálni.

Időintervallum	15 perces beérkezési intenzitás (λ)	Kihasználtsági tényező (ϱ)	Átlagos sorhossz (N_S)	Átlagos várakozási idő percben
7.00 – 7.15	50	0,222	0,063	0,086
7.15 – 7.30	100	0,444	0,356	0,12
7.30 – 7.45	150	0,667	1,333	0,2
7.45 – 8.00	215	0,956	20,54	1,5

5. táblázat: 1 csatornás beléptetési számítás

Példa több csatornás beléptetésre

Egy termelő vállalatnál az az elvárás, hogy a dolgozók a beléptetési folyamatban 5 percnél többet ne várakozzanak. A beléptetést kártyával és biometriával tervezik megvalósítani. Hány forgókapura van szükség, hogy az üzleti igényt kielégítő rendszer valósuljon meg?

A rendszer kiszolgálási ideje:

	Forgókapu működési idő:	6,5 s
	Kártyás azonosítás:	1,5 s
+	Biometrikus azonosítás:	5 s
	Összesen:	13 s

A belépési adatok 20 perces felbontásban állnak rendelkezésre, a műszakváltás 6 és 7 óra között zajlik le, ekkor kritikus a rendszer működése. A 20 perces kiszolgálási intenzitás csatornánként $\mu_{20\ perc}$= 1200s / 13s = 92,3.

A dolgozók be és kilépései ugyanazon forgókapukon történnek, ezért a a két adathalmazt összesíteni kell. A méretezést a legnagyobb terhelésű időszakra kell elvégezni, ez 6.20 és 6.40 között következik be, ekkor λ = 275 fő érkezik a rendszerbe. Ekkor:

$$\varrho = \frac{\lambda}{m*\mu} < 1 \tag{2}$$

egyenletnek teljesülnie kell, amiből adódik, hogy 3 csatornát legalább be kell állítani a rendszerbe, így $\varrho = 0{,}993$ értékű lesz a kiszolgálási intenzitás. A formulákat 3 csatornára alkalmazva $N_S = 183{,}4$ fő az átlagos sorhossz, az átlagos várakozási idő $t_{á} = 13{,}5$ perc lesz, ami nem elfogadható, ezért növelni kell a csatornák számát. Ha 4 forgóvilla kerül telepítésre, akkor az átlagos várakozási idő kevesebb, mint fél perc időtartamban alakul.

KÖVETKEZTETÉSEK

A tanulmány bemutatta a beléptető rendszerek Markov lánccal történő sztochasztikus modellje felállításának egy jól alkalmazható eljárását, valamint az erre épülő elemzésének egy új módszerét. A tanulmány során kapott eredmények alapján kijelenthető, hogy kidolgozott elemzési eljárás alkalmas a biometrikus beléptető rendszerek bevezetésének tervezési fázisban történő minőségbiztosítására, az üzleti döntések támogatására.

A szerző célja a nagylétszámú beléptetési objektumok üzleti és biztonsági szempontok alapján történő projekt bevezetései sikertelenségének elkerüléséhez létrehozott matematikai szimuláción alapuló folyamat-, és rendszerelemzési eljárások kidolgozása, valamint – esettanulmányok felhasználásával – gyakorlati alkalmazási lehetőségeinek bemutatása.

FELHASZNÁLT IRODALOM

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

[2] OTTI, Cs: *„Classification of biometric access control systems based on real-time throughput,"* in Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates, Bratislava, 2015.

[3] MAGYAR SZABVÁNYÜGYI TESTÜLET, *MSZ EN 60839-11-2:2015. Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek,* 2015.

[4] POKORÁDI L.: *Rendszerek és folyamatok modellezése,* Debrecen: Campus, 2008.

[5] B. Ákos, *„A beléptető rendszerek helye és szerepe a vagyonvédelemben,"* Hadmérnök, %1. kötetVI., %1. szám4., pp. 17-25, 2011.

[6] KLEINROCK L.: *Queueing Systems Volume 1*: Theory, New Yor: Wiley - Interscience, 1975.

[7] LOVÁSZ L.: *Algoritmusok Bonyolultsága,* Budapest: ELTE, Matematikai Intézet, 2009.

[8] SZEIDL L.: *Tömegkiszolgálás,* Óbudai Egyetem, Neumann János Informatikai Kar, 2009.

[9] S. G. PAP Gy.: *Sztochasztikus folyamatok,* Szeged: Szegedi Tudományegyetem, Bolyai Intézet, Sztochasztika Tanszék, 2014.

[10] K. D. G., *„Stochastic processes occurring in the theory of queues and their analysis by the method of imbedded Markov chain," Annals of Mathematical Statistics,* pp. 338-354, 1953.

[11] SZTRIK. J.: *A sorbanállási elmélet alapjai*, Debrecen: Debreceni egyetem, Informatikai Kar.

[12] LAW, A. M.: *Simulation Modeling and Analysis*. 5th edition., Tucson, Arizona, USA: McGrow-Hill , 2015.

[13] OTTI Cs: *„Biometrikus rendszerek felhasználói minta pozicionálásának kérdései"* in *DOSZ, Tavaszi Szél 2016*, Budapest, 2016.

[14] HANKA L.: „A Binomiális Eloszlás Alkalmazási Lehetoségei Ujjnyomat Azonosító Rendszerek Vizsgálatában, A Maximum Likelihood Elv Alkalmazása" in *TAVASZI BIZTONSÁGTECHNIKAI SZIMPÓZIUM 2013, ÓBUDAI EGYETEM*, Budapest, 2013.

[15] WERNER, G. Á., HANKA, L.: „Using the Beta-Binomial Distribution for the Analysis of Biometric Identification," in *SISY 2015 : IEEE 13th nternational Symposium on Intelligent Systems and Informatics: Proceedings*, Subotica, Szerbia, International Symposium on Intelligent Systems and Informatics, 2015, pp. 209-216.

[16] PAUL, H. P.; FISHWICK A.: *„Queue Modeling and Simulation,"* in *Principles of Modeling and Simulation: A Multidisciplinary Approach*, John Wiley & Sons, Inc, 2008.

[17] LUKÁCS J.: *Beléptető kapu elhelyezési stratégia fejlesztése és bemutatása néhány kiválasztott metróállomáson keresztül,* Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, 2014.

POLISH JOURNAL OF MANAGEMENT STUDIES
Otti Cs., Kolnhofer-Derecskei A.

2018
Vol.17 No.2

INTRODUCTION TO THE BIOMETRIC ACCESS CONTROL SYSTEMS FOR MANAGERS: WHICH ERROR INDICATOR MATTERS IN THE SELECTION?

Otti Cs., Kolnhofer-Derecskei A.[*]

Abstract: The managers in the business sector have to face security management issues on a daily basis and the present article analyses and discusses one of its segments, namely the biometric systems. The decision-maker is presented with a number of professional data before the implementation of such a system, although the opinion of the final user will be determinant regarding the use of the system. Following the dual engineer-manager approach, the present study first introduces the biometric systems through the engineering metrics and concepts because the decision-maker learns the errors of the system through these indices. The research also highlights the fact, that the final user is far less sensitive. However, it is a principal factor in all the security investments whether the users are able and willing to use the system properly. It is even more so in case of biometric access control systems because the algorithms operate with probabilities and the users can never be sure that they are recognized with 100% accuracy. The error values provided by the manufacturers of biometric systems are not available and because these are algorithmic data, the difference can be of several orders of magnitudes between the actually measured results. The article publishes the results of a quantitative research and determines the users' individual subjective acceptance threshold regarding the errors of access control systems. On the basis of this, the biometric systems could be evaluated from the users' point of view as well.

Key words: FRR, biometrics, user acceptance

DOI: 10.17512/pjms.2018.17.2.17

Article's history:
Received February 15, 2018; *Revised* May 7, 2018; *Accepted* May 26, 2018

Introduction

The relevance of the examined topic could be supported by the recent implementation of GDPR; however, we do not discuss the legislation of data handling because our research focuses on another segment of security management, namely the biometric access control systems. The selection and introduction of such a system belongs to the competence of senior executive management. These managers, however, mostly get the information based on the error indicators tested by engineers. The aim of the present article is to review the basic concepts in order to get a better understanding of this area. It should also be

[*]**Csaba Otti, MSc.**, Óbuda University, DonátBánki Faculty of Mechanical and Safety Engineering; **Anita Kolnhofer-Derecskei, PhD,** assistant professor at Óbuda University, Keleti Faculty of Business and Management
✉ Corresponding author: otti.csaba@bgk.uni-obuda.hu
✉derecskei.anita@kgk.uni-obuda.hu

highlighted that the users are much more receptive; the error indicator they perceive is different by orders of magnitude from the technical error values of the system. First, however, it is briefly explained why it is important to deal with this topic in the field of management. As it is discussed by Peltier in his book: "an overall security program helps the enterprise meet its business objectives or mission by protecting its physical or financial resources". (Peltier, 2016)In order to achieve this, it is inevitable that the decision-makers (security personnel) are well trained and knowledgeable in technical sciences, too. It should be added - as Sennewald and Baillie also underlines - that "the security division is accountable for the employees" (Sennewald and Baillie, 2015).

These days there are an increasing number of articles and research dealing with the issues of security management (Kliestik et al., 2018, Belás et al., 2017; Kuril, 2018; Limba and Šidlauskas, 2018). Soomro et al provide an excellent summary of the professional literature sources. Their study highlights the interdisciplinary cooperation of engineering and management sciences (Soomro et al., 2016). One of the main areas of security management – besides IT security - is the physical security; the main elements of which are: the mechanical protection, electronic protection and manned protection. One of the basic tasks of providing security is to ensure that only the authorised staff can have access to the given facilities, persons or information (Oláh et al., 2017, Oláh et al., 2018). The major part of security systems is focusing on this task. There are three types of basic technologies in the field of automatic identification (access control systems): knowledge based (PIN code, password); asset-based (card, phone) or biometric identification (a physical characteristic). (Otti, 2016; Piotrowska et al., 2017)The automated, electronic biometric identification has gone through an enormous development in the last fifty years. The law enforcement authorities have an increasing demand to be able to identify people quickly and credibly, practically anywhere. Parallel with this, it is more and more necessary in all the areas of life to identify users and entrants and to authenticate their access. On the other hand it is fairly obvious that the users' acceptance towards these technologies or devices has a key role in the success of implementation and everyday usability. (Dillon and Morris, 1996)

In the research first of all those civil biometric applications were identified where the biometric identification was crucial in terms of operation: these are the staff entry and attendance recording systems in companies with high number of employees. (Otti, 2016) It is regarded crucial because - due to the high number of staff - the system should be quick and should have a low false rejection rate (FRR) value. The majority of almost 100 biometric systems, that have been implemented in Hungary in the last 20 years and examined in our research, failed. Even in our days the success depends only on „sheer luck". Having analysed this phenomenon we started to test biometric devices in ABI (Applied Biometrics Institute) in 2010. By examining any device of any supplier it was revealed that the FRR data provided by the supplier were different from the actual values by several orders of magnitude. The primary reason for this was that the suppliers provide the results of

algorithmic or – in other words – technological tests and they do not calculate with users, implementation or environmental conditions. The next question that came to us was: how could there exist any successful biometric system at all? Or approaching it from another angle: can it be decided about a biometric device during the tender whether it is going to function properly or not?
Therefore we turned to the users and asked them how they perceived this issue. The hypothesis was that the people would accept higher False Rejection Rate even by 2-3 orders of magnitude as serviceable. In the expert and focus group examinations carried out in the previous phases of research (Otti, 2017). We elaborated the set of questions, which the quantitative research was based on. The present study analyses the questions and summarises the results on the basis of 653 responses.

Literature: Characteristics of Biometric Systems

Hereinafter the technical parameters of biometric access control systems are summarised in a nutshell. On the basis of the related ISO standard (ISO/IEC, 2006) andShimon's article Biometrics in Identity Management: Concepts to Applications (Shimon, 2011)the biometric devices are basically sample recognising systems and in general they consist of subsystems as it can be seen in Figure 1.

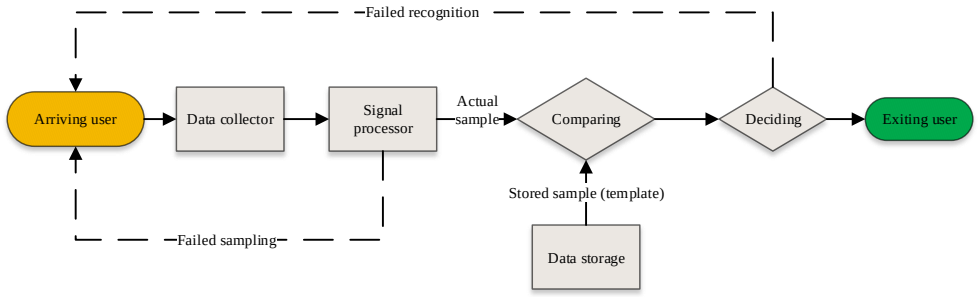


Figure 1. Subsystems of a general biometric device

The data collecting subsystem is responsible for taking the biometric sample of the user. The errors entered into the system at this point would run through the whole identification process. The task of the sign processing subsystem is to extract those features from the samples, which make them unique. The data storage stores the collected and coded biometric data for later comparison. These data are also called templates in biometrics. The storage can be central (on one computer or server) or local (e.g. on a smart card or individual media device). The Regulation (EU) 2016/679 practically bans the central storage of biometric data from users. The comparing subsystem compares two samples and creates a similarity score. This score indicates the certainty that the stored template and the sample taken are from one and the same person. The biometric identification systems are always probability-based; therefore 100% match would never exist. As opposed to this, in

case for example a cryptographic or password-based system the successful identification always requires 100% match. Since the meeting of a person and a sensor can never be exactly the same twice, therefore the system generates a similarity score instead of a simple „yes" or „no" response. The decision-making subsystem compares the generated similarity score to a preliminary determined limit in order to decide about the success or failure of identification. But sometimes there are errors. The control and identification errors can be traced back either to matching (false match or false non-match) or sampling errors (sampling failed, entering into system failed). When these basic errors lead to a decision-making error, it can be due to several different factors, for example the number of comparisons required; decision-making policy or simply whether the identification was positive or negative. (Jain et al., 2004; Androniceanu, 2017a)

A biometric identification system can generate two types of errors (1) It can produce false match of biometric samples from two different persons and identify them as match (False Match: the index in references is FMR - False Match Rate or FAR - False Acceptance Rate) (2) Two measurements from the same person are identified as belonging to two different persons (False Non-match: the index in references is FNMR – False Non Match Rate or FRR – False Rejection Rate).

There is a trade-off curve in every system between the false match rate (FMR) and the false non-match rate (FNMR). If the system is configured in a way that it is less sensitive to confusing factors and has better acceptance of the users' samples, the FMR will be increasing; if more secure settings are created, then the FNMR will be higher (Androniceanu, 2017b). ROC (Receiver Operating Characteristics) and DET (Detection Error Trade-off) curves are generally used to describe the performance of biometric systems ((Springer, 2013; Horváth and Kovács, 2013).

The references do not offer any (or they offer more) commonly used and accepted definitions of indices characterizing biometric systems. Mostly the ISO/IEC 19795 standards of 2006 and 2012 are applied. (ISO/IEC, 2006; ISO/IEC, 2012) Here we do not detail all of them only we focus FRR because that has important significance in practice. The False Rejection Rate is seemingly a secondary index in the field of biometric identification. This may be the case because FAR (False Acceptance Rate) is far more „terrifying" in terms of security, as it means that non-authorised persons (impostors) may enter the protected area. It is true in many applications, but in the area of physical security, in case of mass occupancy establishments (entry and attendance register; more than 300 employees) there has not been any application in Hungary in the last 20 years where this factor dominated. It is easy to prove if mathematical risk analysis methods are used;as well as the time and success of entering the users is an important aspect in the implementation (Michelberger and Horváth, 2017).

On the basis of the professional literature sources we have processed, estimating, measuring and providing FRR was almost always limited to technological results – which is not surprising as this is the only test type, which can be controlled well, can be run on a large mass sample and is able to set up a clear order among the

algorithms. The manufacturers would indicate these FRR values on the specification of their devices, usually in the 0.00001% - 0,01% range.(Hanka and Werner, 2015)
Examining the results of scenario tests and tests under live conditions, it has been concluded that in reality the users meet false rejection in the 1%-70% range. It means that the difference can be at least 2 or even 6 (!) orders of magnitude between the promise in the specifications and the actual results. Since the values in the specifications cannot be measured in the practice, this leads to two outcomes in the decision-making regarding a security investment: (1) The devices of all the manufacturers meet the requirements. (2) It cannot be decided which system is more suitable for the given task. Therefore the decision points are shifted and other aspects - for example the price –are given priority.

Scenario FRR Tests (Research 1)

On the basis of the related ISO standards regarding the testing of biometric systems as well as own methodological developments, the same conditions were created for the scenario tests as those with which the users meet in real life. Such as for example the dependence on light conditions in case of a face recognition device, with the testing of which it can be exactly determined how a device installed outdoor would behave under the sunlight at different times of the day. (ISO/IEC, 2012)As it has been expected, the FRR values deteriorate when the circumstances are deviating from the ideal. The difference between devices and the decision about usability of each device depends on how quickly and to what extent the results are deteriorating. (Kovács et al., 2012)
Procedures that are as close to real conditions as possible have been elaborated enabling the accurate documentation of conditions and circumstances of tests in order to ensure reproducibility: (1) Positioning sensitivity: the perfectly positioned sample is rotated and shifted and the changes in FRR are measured. (2) Measuring throughput in relation to enrolled users and samples. (3) Contamination of the sample: for example a wet finger. (4) Distortion of the sample: for example a wounded finger or a ring. (5) Effects of environmental changes: lighting, temperature, and humidity. (Stan and Li, 2015)
Hanka's publication (2013) gives an excellent summary for the analysis of statistical backgrounds of FRR measurements. In this work Hanka confirms and expands Doddington's rule of 30 on biometric fingerprint identifying systems. The rule says that to be 90% confident that the p probability is within ± 30% of the relative frequency calculated on the basis of experiences, there must be at least 30 errors. In the current case the p probability is the FRR value and – according to the principle - 30 errors should be measured in order to accept the given FRR level. It means that 300,000 events or tests should be made for the FRR=0.01% measurement of an average biometric device. This is virtually impossible to carry out. Yet we got interpretable results in the reality; the best example for this is the FRR dependence of a fingerprint identifying equipment on the number of enrolled

samples. According to the measurement methodology, the nominal user capacity (500 people) was filled up with 50-person increments and 300 measurements were made in every measurement points. The results can be seen in the following figure.

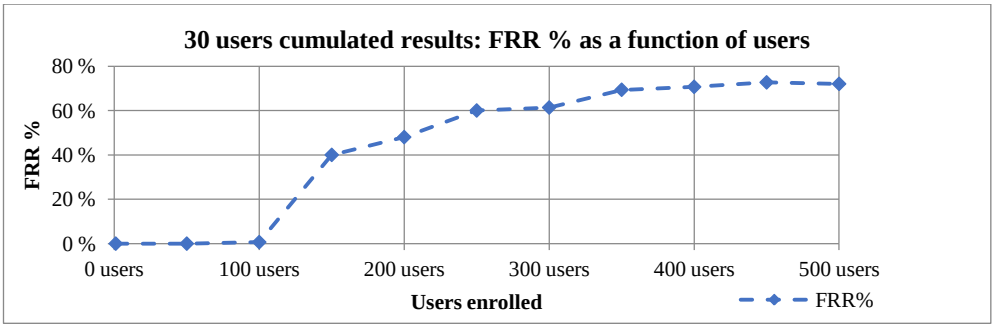


Figure 2. Results of face recognition scenario test. FRR% as a function of enrolled users

The implementation of such a device is a rather costly investment. Nazareth and Choi also examined this; using a system dynamics model, their study evaluates alternative security management strategies through an investment and security cost lens, to provide managers guidance for security decisions. (Nazareth and Choi, 2015)When ranking the systems, the technical specifications of the system as well as other aspects should also be considered. Regarding the success of implementation and use, the opinion of the final users is very important. They may perceive the false rejection as "the door is stuck". How do they interpret this and with what error values would they still feel the system acceptable? These questions are discussed in the next chapter.

Users' Acceptance (Research 2)

The subject of research in this chapter is the final user, who is tested with the methods of social science, through their introspective responses given to hypothetical, imaginary situations. The objective of the current research is to survey when and to what extent the people regard a biometric access control system usable in relation to the number of their failed entries. Previous study (Otti, 2016) helped to define the spontaneous responses, experiences and feelings of people. Due to this, the biometrics relates was taken out from the definition, then the access control system, too. Then it was simplified to a stage that the question was about passing through a door, which is sometimes stuck and cannot be opened. In this example the number of failed entries can be interpreted in an analogous way but it is not trivial, which value it corresponds with. Finally, the FRR value is chosen because it contains the algorithmic FMR and FTA (Failure To Acquire) values but it does not include the FTE Failure to Enrol rate, which cannot be modelled. The question was as follows: *„Imagine that you have to go through a*

door in your workplace/school 5 days a week, four times a day. This door usually works well, but ……. (frequency of door jam) times it is stuck and you have to try again to open it. To what extent do you regard the door usable?"

The hypotheses drafted in our research are as follows:

H1: There is a correlation between the frequency of being rejected and the presumed usability of the system.

H2: The acceptance threshold of people is higher by several orders of magnitude than the FRR False Rejection Rate provided by the manufacturer for the device.

If the hypotheses can be confirmed then – on the one hand - the values based on the scenario tests can be validated statistically; on the other hand the usability of the system can be actually predicted in the given application.

The frequency of door jams is determined as a function of the number of entries and the following units were used (1) once a day (the most frequent) (2) once a week (3) once a month (4) once a year.If we presume that the respondent goes through the gate in question every weekday at least four times (2 entries and 2 exits), then calculating with 20 workdays per month on average it means 960 passes per year, therefore the relative frequency of being stuck per year is as follows (1) 25% in case of one jam per day (2) 5.415% in case of one jam per week (3) 1.25% in case of one jam per month (3) 0.104% in case of one jam per year.The presumed usability was measured on a four-stage semantic differential scale using the following stages: (1) unusable (2) less usable (3) usable (4) perfectly usable. Both criteria mean data measured on ordinal scale. The following statistical methods were used in the analysis: descriptive statistics; interval estimation (with 90% confidence interval, which was justified by Doddington's rule that is used for the evaluation of biometric systems); cross table analysis (with α=0,05 significance test); non-parametric hypothesis tests (again p = 0,95), and regression analysis.

Methodology

The data were collected in March and April 2017 among the students of the Óbuda University (446 persons, 60.8% of the respondents) and the members of MENSA Hungar IQ (197 persons, 26.8% of the respondents), as well as students from other universities (91 persons, 12.4% of the respondents). Our choice of target group is justified by two reasons: on the one hand the students on the campuses of the Óbuda University already meet and use access control gates on a daily basis, and, on the other hand, they will form an organic part of the labour market, where – according to our experiences – the majority of enterprises and all the large-scale companies use similar access control systems. Out of the students of Óbuda University, 390 persons are studying at the Donát Bánki Faculty of Mechanical and Safety Engineering; they not only meet such systems but also study about them. Some of the respondents (497 persons) are already employed, typically in areas where they encounter such systems. A questionnaire was used in the research, the content of which was partly based on former research (Otti, 2016), partly on review of professional literature sources. Since the respondents had to assess the issue of

being rejected at the door not in a real but in an imaginary, hypothetical situation, the questionnaire was tested several times. Following the data cleansing, responses from n=734 respondents were processed. This number of elements was further reduced to 653, which covered those respondents who answered all the questions. The distribution of respondents was the following: By gender 74.4% (486 persons) were male and 25.6% (167 persons) were female; it is due to the profile of Óbuda University.
As the sampling was not based on random selection and our aim was to increase the number of sample elements, therefore our sample has high element number but cannot be regarded as representative from all aspects.

Results

There is a significant correlation (sig. $p < 0.05$) between the frequency of being rejected and evaluation of usability. The lower is the frequency of rejections, the higher is the satisfaction. The quantifiable value of correlation by Pearson correlation is $R = 0.543$, which is a moderately strong correlation.

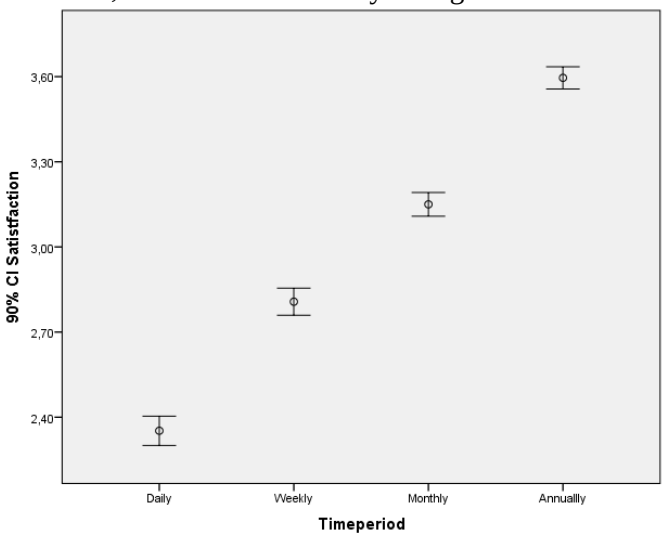


Figure 3. Averagesatisfaction of respondents as a function of the frequency of rejections, with 90% confidence interval

If the time unit is examined not on an ordinal but on a ratio scale, that is the frequency of rejections is examined in the above described percentage (relative) distribution, the value will be very similar ($R = - 0.479$, the negative value is justified by the fact that the lower is the frequency of being held up, the higher is the user's satisfaction). This moderately strong significance of the correlation enables to fit a regression function on the data. During the fitting, the frequency of rejections was examined in the percentage of time unit. The best fit could be observed in case of the logarithmic function, which is demonstrated on Figure 4

below. The value of constant is 2.1054, which means that there is a neutral reaction to the stuck door, which decreases the value of the usability of the device by increasing the frequency of rejections. In this case, one per cent growth in the frequency of being stuck (1% of four-a-day passes, 960 times a year) will lead to decline in the users' usability sense by 0.224 unit (considering on the above described 4-stage scale). We should realise a strong similarity between Figure 2 and Figure 4 that failures curves are similar but the acceptance levels differ.

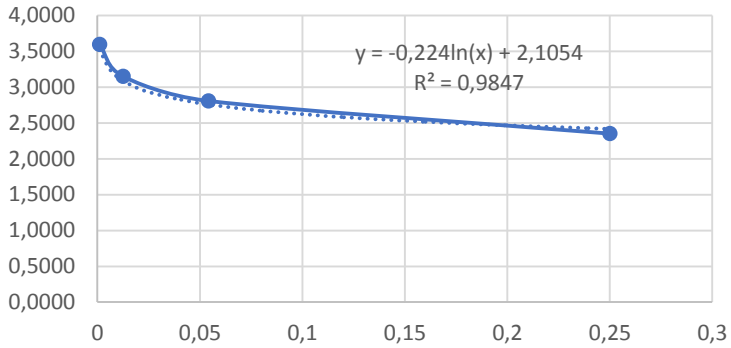


Figure 4. Regression function fit on the general satisfaction level of the respondent as function of the frequency of rejections (X axis: relative frequency of rejections per year, Y axis: degree of usability/satisfaction level)

The examination has confirmed the H1 hypothesis, which assumed that there is a correlation between the frequency of rejections and the presumed usability of the system. Moreover, this correlation is strong enough to fit a logarithmic regression function on it. It should be repeated, however, that the explanation power (Rsquared) is 0.295, which means that the frequency of rejections explains the satisfaction of the user only to an extent of about 30%. Therefore the question arises, what else can affect the user's satisfaction. During the survey, in addition to the demographic characteristics, the users were also asked about their workplace satisfaction. The reason for this was that the respondents were deliberately not given the questions in sequential order; therefore the questions put between responses decreased the saturation and maintained the interest of the respondent. (1) How do you feel now? (2) How satisfied are you with the information received for your work/studies? (3) How much would you recommend your current workplace/school to others?

Again the answers could be given to this on a semantic differential scale. Although it could be interesting, but the present article does not cover the one-by-one analysis of responses given to these questions; only those overlaps are discussed, where the user's actual general mood and their feelings towards their work had an impact on the usability value we examined. The general device satisfaction level was examined in the comparison; and the significant correlations (sig. $p < 0,05$)

that were found had the following features: (1) those who felt better and marked a higher value on this scale, evaluated the device as more usable in general (Cramer value 0.179); (2) the more the respondent felt that they receive substantial information, the more satisfied they were with the device (Cramer value 0.179); (3) in this case the direction of the relation (cause and effect relation) was not identified but there was a significant correlation between the device satisfaction and the degree of recommendation (Cramer value 0.161). The strongest correlation was in case of information; in another question, the ratio of predictability was indicated as the main source of stress in the workplace. This indicates that education and appropriate information flow may reduce uncertainty and by thisimprove the feelings towards and acceptance of the device. It is obvious that the correlation is everywhere significant but very weak, therefore the explanatory power of the above model would only be weakened by these factors in case of applying a multifactor regression model, therefore we accept the two-factor model.
According to hypothesis H2, the acceptance threshold of users is higher by several orders of magnitude than the false rejection rate (FRR = 0,01%), which is usually provided on the datasheets. There is an approximately 3% FRR belonging to the 3.00 „Usable" value on Figure 4. Therefore hypothesis H2 has been confirmed, too.
Cavusoglu et al got similar outcomes from testing the security awareness of organizational users. They regarded the appropriate training in the early phase and later the prudent control as the most important elements in the implementation of such a system. (Cavusoglu et al., 2015)

Summary and Conclusions

Peltier (2016) systematizes those features, which should be considered before the implementation of security-assisting systems. (Peltier, 2016) Focusing on the users, the present research compared the acceptance rate (usability index) given by them and the technical parameters of the system. Both the technological and organisational aspects are critically important, but both of these are closely related to people. As our research has also concluded, the individual users are less sensitive than the certified FRR. As the sense of security is decreasing, more and more security and biometric systems are implemented all over the world. The acceptance by the users is closely related to their ability to use the system.
Two hypotheses were tested in the present article:
H1: There is a correlation between the frequency of being rejected and the presumed usability of the system. ACCEPTED
The system may reject the final user during the access control for several reasons. The final user, however, would not perceive the FRR value at all, for them the door is stuck and they cannot enter. They cannot achieve their objective; therefore they will not be satisfied with the system. Nevertheless, this rejection rate will still be lower even with a much more frequent failure to enter than what could be regarded acceptable on the basis of the technical parameters.

H2: The acceptance threshold of people is higher by several orders of magnitude than the FRR False Rejection Rate provided by the manufacturers for the device. ACCEPTED

Both hypotheses have been confirmed and thus it has been proved that the actual FRR values measured in scenario tests can be evaluated in this range. Under given security conditions it should be determined what value of user acceptance would be suitable for business decision-makers and the biometric access control systems should be calibrated to this value.

Discussion

Managers have a great responsibility in choosing, implementing and ensuring the successful use of the appropriate device. In the selection phase, besides knowing the technical parameters, the satisfaction of final users with the device can be achieved with further support. It has also been revealed that education and information flow can significantly improve acceptance, which base on a properly designed knowledge transfer system. 'However, a properly designed transfer system is a prerequisite for effective knowledge transfer in an intra-organizational network, which can assist in the generation of competitive advantage.' (Sroka et al., 2014)On the other hand, the security management approach is an innovation approach, similar to the social innovation approach, which says that the enterprise engagement in that kind of activities "may provide the background conditions for the creation of additional profit opportunities while generating social value; the possibility of obtaining tax benefits from government; and the receipt of benefits from the public and private sectors (mainly by involving the additional investment capital)."(Shpak et al., 2017)

The acceptance of the technology by the users can be clearly observed in the course of implementing an ERP or HRIS system. By quantifying that the people still typically accept an approximately 3-5% inconvenience; this value presumably can be applied in the implementation of management support systems and software and in case of organisational development projects, too. Our results can also be used in employee journey mapping analyses. It means that without training and improving the commitment to the given system this degree of inconvenience is still accepted by the employees without any significant decline of satisfaction.

At a fundamental level, our study provides managers with clear findings regarding acceptance of security and helps to decide about that kind of investment. This article also advises managers to adopt a more holistic approach to information security management to include: management participation from top-level management and the involvement of strategic decision makers to the thorough understanding of the technical parameters of devices. However, the motivations of users, their human nature; in other words, the soft factors in addition to the hard, technical factors will also have an important role. This has been highlighted by Safa and Von Solms, too: "now we can say that information security knowledge sharing, information security collaboration, and complying with information

security organizational policies and procedures are organizational aspects of information security that should be taken into the consideration by both academics and practitioners." (Safa and Von Solms, 2016)

Acknowledgements

 *Supported By the ÚNKP-17-4/I. New National Excellence Program of the Ministry of Human Capacities*

References

Androniceanu A. 2017a, *The three-dimensional approach of Total Quality Management, an essential strategic option for business excellence*, "Amfiteatru Economic", 19(44).

Androniceanu A. 2017b, *Hospital management based on the relationship between doctors and patients*, "Administratiesi Management Public", (29).

Belás J., Mišanková M., Schönfeld J., Gavurová B., 2017, *Credit risk management: financial safety and sustainability aspects*, "Journal of Security and Sustainability Issues", 7(1).

Cavusoglu H., Cavusoglu H., Son J.-Y., Benbasat I., 2015, *Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources*, "Information & Management" , 52(4).

Dillon A., Morris M., 1996, *User acceptance of new information technology: theories and models*,"Annual Review of Information Science and Technology", 31.

Hanka L., 2013, *A Doddington-féle 30-as szabály, biometrikus rendszerek megbízhatóságának statisztikai elemzése*, Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest: Óbudai Egyetem.

Hanka L., Werner G., 2015, *Using the Beta-Binomial Distribution for the Analysis of Biometric Identification*, IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY).

Horváth T., Kovács T., 2013, *Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén*,[In:]Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest: Óbudai Egyetem.

ISO/IEC, 2006, ISO/IEC 19795-1 *Information technology — Biometric performance testing and reporting* — Part 1: Principles and framework, Svájc.

ISO/IEC, 2012, ISO/IEC 19795-6:2012(E). *Information technology — Biometric performance testing and reporting* — Part 6: Testing methodologies for operational evaluation, Svájc.

Jain A.K., Fellow A.R., *Prabhakar S., 2004, An Introduction to Biometric Recognition*, "EEE Transactions on Circuits and Systems for Video Technology", 14(1).

Kliestik T., Misankova M., Valaskova K., Svabova L., 2018, *Bankruptcy prevention: new effort to reflect on legal and social changes*, "Science and Engineering Ethics", 24(2).

Kovács T., Otti C., Milák I., 2012, *A biztonságtudomány biometriai aspektusai*,[In:]A biztonság rendészettudományi dimenziói: Változások és hatások, Pécs: Magyar Rendészettudományi Társaság.

Kuril J. 2018, *Public administration for safe and secure environment: case of Slovak Republic*, "Entrepreneurship and Sustainability Issues", 5(3).

Limba T., Šidlauskas A., 2018, *Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook*, "Entrepreneurship and Sustainability Issues", 5(3).

Michelberger P., Horváth Z., 2017, *Security aspects of process resource planning*, "Polish Journal of Management Studies", 16(1).

Nazareth D., Choi J., 2015, *A system dynamics model for information security management*, "Information & Management", 52(1).

Otti C., 2016, *Comparison of biometric identification methods*,IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara.

Otti C., 2017, *Why does it fail to operate?*[In:]Thinking Together: The economy in practice,Budapest: Óbudai Egyetem.

Oláh J., Karmazin Gy., Pető K., Popp J., 2017, *Information technology developments of logistics service providers in Hungary*. "International Journal of Logistics Research and Applications", 21(3), 332-344.

Oláh, J., Zéman, Z., Balogh, I., & Popp, J. 2018,*Future challenges and areas of development for supply chain management*, "LogForum", 14(1).

Peltier T.R., 2016, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, CRC Press.

Piotrowska A., Polasik M., Piotrowski D., 2017, *Prospects for the application of biometrics in the Polish banking sector*, "Equilibrium. Quarterly Journal of Economics and Economic Policy", 12(3).

Safa S.N., Von Solms R., 2016, *An information security knowledge sharing model in organizations*, "Computers in Human Behavior", 57.

Sennewald C.A., Baillie C., 2015, *Effective Security Management*, Elsevier: Butterworth-Heinemann.

Shimon M.K., 2011, *Biometrics in Identity Management: Concepts to Applications*, Norwood: Artech House.

Shpak N., Satalkina L., Sroka W., Hittmar S., 2017, *The Social Direction of Enterprises' Innovation*, "Polish Journal Of Management Studies", 16(1).

Soomro Z.A., Shah M.H., Ahmed J., 2016, *Information security management needs more holistic approach: Aliterature review*, "International Journal of Information Management", 36(2).

Springer, 2013, *Security and Privacy in Biometrics*, Springer London Heidelberg New York Dordrecht: Springer.

Stan Z., Li A.K., 2015, *Encyclopedia of Biometrics - Second Edition,* Springer New York Heidelberg Dordrecht London : Springer.

Sroka W., Cygler J., Gajdzik B., 2014, *The Transfer of Knowledge in Intra-Organizational Networks: A Case Study Analysis*, Organizacja, 47(1).

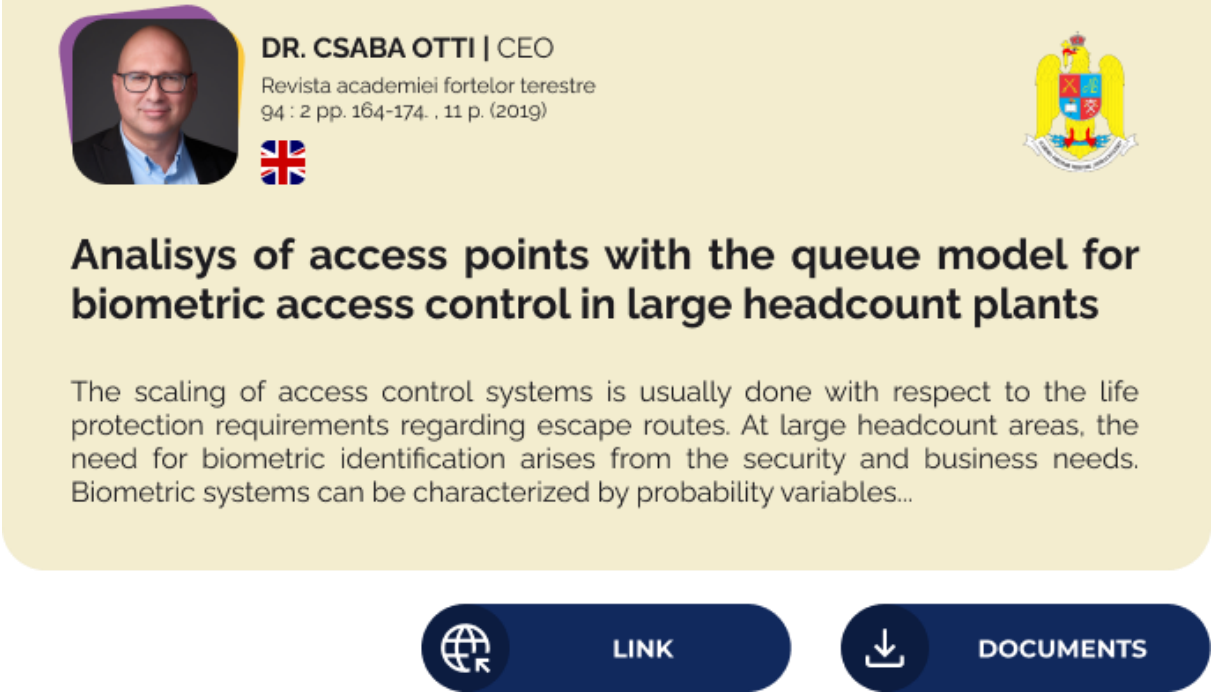
WPROWADZENIE DO SYSTEMÓW KONTROLI DOSTĘPU BIOMETRYCZNEGO DLA MENEDŻERÓW: KTÓRE WSKAŹNIKI BŁĘDU MAJA ZNACZENIE W WYBORZE?

Streszczenie: Menedżerowie w sektorze biznesowym codziennie muszą stawiać czoła problemom związanym z zarządzaniem bezpieczeństwem, a niniejszy artykuł analizuje i omawia jeden z jego segmentów, a mianowicie systemy biometryczne. Decydent otrzymuje szereg profesjonalnych danych przed wdrożeniem takiego systemu, chociaż opinia ostatecznego użytkownika będzie decydować o korzystaniu z systemu. Zgodnie z dualnym podejściem inżynier-menedżer, obecne badanie najpierw wprowadza systemy biometryczne poprzez metryki inżynierskie i koncepcje, ponieważ decydent poznaje błędy systemu poprzez te wskaźniki. Badanie podkreśla również fakt, że końcowy użytkownik jest znacznie mniej wrażliwy. Jest to jednak główny czynnik we wszystkich inwestycjach w bezpieczeństwo, niezależnie od tego, czy użytkownicy są w stanie i chcą prawidłowo korzystać z systemu. Tym bardziej w przypadku biometrycznych systemów kontroli dostępu, ponieważ algorytmy działają z różną dokładnością, a użytkownicy nigdy nie mogą być pewni, że są rozpoznawani ze 100% dokładnością. Wartości błędów dostarczone przez producentów systemów biometrycznych nie są dostępne i ponieważ są to dane algorytmiczne, różnica może wynosić kilka rzędów wielkości między faktycznie zmierzonymi wynikami. Artykuł publikuje wyniki badania ilościowego i określa indywidualny, subiektywny próg akceptacji użytkowników dotyczący błędów systemów kontroli dostępu. Na tej podstawie systemy biometryczne mogłyby być oceniane również z punktu widzenia użytkowników.
Słowa kluczowe: FRR, biometria, akceptacja użytkownika

生物识别访问控制系统为经理介绍：哪些错误指标在选择？

摘要：商业领域的管理者必须每天面对安全管理问题，本文将分析和讨论其中的一个细分领域，即生物识别系统。尽管最终用户的意见将决定系统的使用，决策者在实施此类系统之前会收到大量专业数据。继双工程师-管理者方法之后，本研究首先通过工程度量和概念介绍生物特征系统，因为决策者通过这些指标了解系统的误差。该研究还强调了这样的事实，即最终用户的敏感度要低得多。然而，这是所有安全投资的主要因素，无论用户是否能够并愿意正确使用系统。在生物识别访问控制系统的情况下更是如此，因为算法以概率运行，并且用户无法确定它们以100%的准确度被识别。由生物统计系统制造商提供的误差值不可用，并且因为这些是算法数据，所以实际测量结果之间的差异可以是几个数量级。文章发表定量研究的结果，并确定用户对访问控制系统错误的个人主观接受阈值。在此基础上，还可以从用户的角度评估生物识别系统。
关键词：FRR，生物特征识别，用户接受度

Research



DR. Csaba Otti | CEO

Adatkezelési szabályok hatása egy szervezet munkaerő- és létszámgazdálkodására

- Absztrakt (-): -
- Nyelv: magyar
- Link: https://www.metropolitan.hu/upload/c161b94e18ad3277c1c58f01f7279a63e33dce9d.pdf
- Kiadó/kiadás: ÚJ MUNKAÜGYI SZEMLE 3 : 2 pp. 38-47. Paper: 2677 1306 , 10 p. (2022)

Analisys of access points with the queue model for biometric access control in large headcount plants

- Absztrakt (EN): The scaling of access control systems is usually done with respect to the life protection requirements regarding escape routes. At large headcount areas, the need for biometric identification arises from the security and business needs. Biometric systems can be characterized by probability variables, which can significantly affect the access process. Mathematically, access control is a discrete state space, stochastic process without memory, that can be described by a queue model. This study demonstrates the process model of access control systems and describes the mathematical model that allows for accurate planning and can ensure a successful introduction for access control systems.
- Nyelv: angol
- Link: https://www.armyacademy.ro/reviste/rev2_2019/Otti_RAFT_2_2019.pdf
- Kiadó/kiadás: Revista academiei fortelor terestre / Land forces academy review 94 : 2 pp. 164-174. , 11 p. (2019)

Introduction to the biometric access control systems for managers: which error indicator matters in the selection?

- Absztrakt (EN): The managers in the business sector have to face security management issues on a daily basis and the present article analyses and discusses one of its segments, namely the biometric systems. The decision-maker is presented with a number of professional data before the implementation of such a system, although the opinion of the final user will be determinant regarding the use of the system. Following the dual engineer-manager approach, the present study first introduces the biometric systems through the engineering metrics and concepts because the decision-maker learns the errors of the system through these indices. The research also highlights the fact, that the final user is far less sensitive. However, it is a principal factor in all the security investments whether the users are able and willing to use the system properly. It is even more so in case of biometric access control systems because the algorithms operate with probabilities and the users can never be sure that they are recognized with 100% accuracy. The error values provided by the manufacturers of biometric systems are not available and because these are algorithmic data, the difference can be of several orders of magnitudes between the actually measured results. The article publishes the results of a quantitative research and determines the users' individual subjective acceptance threshold regarding the errors of access control systems. On the basis of this, the biometric systems could be evaluated from the users' point of view as well.
- Nyelv: angol
- Link: https://pjms.zim.pcz.pl/resources/html/article/details?id=174959
- Kiadó/kiadás: Polish Journal of Management Studies 17 : 2 pp. 197-210. , 14 p. (2018)

Belépési pontok meghatározása markovi modellel, nagy létszámú üzemek biometrikus beléptetésénél

- Absztrakt (HU): A beléptető rendszerek méretezése jellemzően a menekülési útvonalakra vonatkozó életvédelmi szempontok szerint történik. Nagy létszámú beléptetési helyeken az ezen túlmutató biztonsági és üzleti igények miatt sokszor felmerül a biometrikus azonosítás igénye. A biometrikus rendszerek működése valószínűségi változókkal jellemezhető, amely jelentősen képes befolyásolni a belépési folyamatot. Matematikai szempontból a belépetés egy diszkrét állapotterű, emlékezet nélküli sztochasztikus folyamat, így az Markov lánccal írható le. Jelen tanulmány bemutatja a beléptető rendszerek folyamatmodelljét, valamint számítási eljárásokat ad meg a tervezéshez amellyel biztosítható a bevezetési projekt sikeressége.
- Absztrakt (EN): The scaling of access control systems is usually done with respect only to the life protection rules pertaining escape routes. However, in the case of access points with a large traffic, further business and security requirements point towards biometric identification. Operation of such systems can be characterised by probability variables that can affect the access procedure significantly. From a mathematical standpoint, access control is a discrete state space stohastic process without a memory and thus can be described with a Markov chain. This study will first demonstrate the process model of access control systems and then provide calculation processes to aid the design of such systems which can ensure the success of their introudction.
- Nyelv: magyar
- Link: http://hadmernok.hu/172_03_otti.pdf
- Kiadó/kiadás: Hadmérnök 12 : 2 pp. 22-33. , 12 p. (2017)

Comparison of biometric identification methods

- Absztrakt (-): 2016 ieee 11th international symposium on applied computational intelligence and informatics (saci)
- Nyelv: angol
- Link: https://m2.mtmt.hu/gui2/?mode=browse&params=publication;3051270
- Kiadó/kiadás: Budapest, Magyarország : IEEE (2016) 412 p. pp. 339-344. , 6 p.