Óbudai Egyetem

Doktori (PhD) értekezés

A pénzintézeti biztonság fogalma, eredete, jelene, jövője, a paradigmaváltás feltételei és jelentősége

Fialka György

Témavezető: Prof. Dr. Kovács Tibor

Biztonságtudományi Doktori Iskola

Budapest, 2016

Szigorlati bizottság:

Elnök: Prof. Dr. Berek Lajos egyetemi tanár, ÓE

Tagok: Dr. Simon Ákos (külső)

Dr. Kiss Sándor (külső)

Nyilvános védés teljes bizottsága:

Elnök: Prof. Dr. Pokorádi László, egyetemi tanár, ÓE

Titkár: Dr. Szűcs Endre, egyetemi adjunktus, ÓE

Tagok: Dr. Simon Ákos (külső)

Dr. Christián László, egyetemi docens, NKE

Dr. Nagy Rudolf, egyetemi adjunktus, ÓE

Bírálók: Dr. Kiss Sándor (külső)

Prof. Dr. Berek Lajos, egyetemi tanár, ÓE

Nyilvános védés időpontja:

2016. június 28.

TARTALOMJEGYZÉK

FELHASZNÁLT IRODALMAK…F1-F8

BEVEZETÉS

A tudományos probléma megfogalmazása

Doktori értekezésem a biztonság fizikai és elektronikai eszközrendszereit, fejlődését a humánbiztonság kapcsolódó feladatait, valamint a pénzintézeti műveletek működő biztonsági folyamatait, illetve ezek kölcsönös, egymásra ható, működtetésével kapcsolatos feladatokat elemzi. Az ezekből leszűrhető konzekvenciák és korunk új innovációs technológiai lehetőségei alapján keresem a védelem paradigmaváltásának lehetőségeit a bankok fizikai biztonságának növelése érdekében.

A pénzintézetek biztonsága több, egymásba épülő és egymást kölcsönösen feltételező biztonsági rendszer védelmi hatása és a környezeti behatások változása mentén állandóan módosuló képet mutatva formálódik. A technikai fejlődés mechanikai, elektronikai, a tudományos előrelépés biológiai és kémiai eredményei, valamint a humán kutatások idevonatkozó következtetései és a jogi szabályozásokból fakadó lehetőségek egyaránt megjelennek és beépülnek a fejlesztési folyamatokba. A változások hajtómotorja a bekövetkezett támadásokból leszűrhető konzekvenciák alapján megfogalmazódott újabb prevenciós igény, amely a védelem különféle variációs szükségleteit formázza meg - jelen esetben a pénzintézetek részére.

A bűncselekmények - függően a támadás célpontjától: az intelligens csalási folyamatoktól a legdurvább erőszakos rablási cselekményekig - széles sávban mozognak. Talán az erőszak természete, veszélye és végeredménye miatt nagyobb hangsúlyt kap a bankrablási cselekmények elhárítására fordított energia. A bankrablások, mint e csoport kiemelkedő bűncselekményei, folyamatos fejtörést okoznak a biztonsági szakembereknek. Ellenük technikai, szabályozási és pszichikai eszközök együttes alkalmazása mentén érhetünk el csak érdemi eredményeket.

A biztonságtechnika legújabb termékeinek - amelyeket a pénzintézetek ez idáig is teljességükben alkalmaztak - vonatkozásában elérve azok fejlettségének lehetséges csúcsát paramétereik javításával, megbízhatóságuk fokozásával, valamint fizikai méreteik csökkentésével lehet számolni.

Megítélésem szerint a védelmi logika (figyelembe véve a törvények biztosította kereteket) jelenleg egy jól indokolható passzív koncepciót követ, és kevés figyelem összpontosul a megelőző aktív beavatkozási, akadályozási módszerek fejlesztésére, bevezetésére, alkalmazására.

A bekövetkezett bankrablások folyamatát, bekövetkezésük okait - hazai és nemzetközi vonatkozásban is - tudományos szinten vizsgálják a Bankszövetségek szakértői. A rablások összes elkülöníthető elemét (időpont, időtartam, a kiválasztás módja, az elkövetők létszáma, az erőszak szintje, stb.) figyelembe véve keresik azokat a biztonsági szempontból releváns elemeket, amelyek alapján a prevenció lehetséges új változatai tervezhetővé válnak.

A bankrablásokkal kapcsolatos statisztikai adatokat vizsgálva, néhány elem gyakoriságát figyelembe véve az alábbiakat lehet megállapítani:

1. Magyarországon 2007 és 2012 között az ismertté vált elkövetők ügyében folytatott vizsgálatok anyagai azt bizonyították, hogy a támadók szinte minden esetben felderítették a banki környezetet és megtervezték az elkövetést. Ezeket azonban a biztonsági szolgálatok általában nem észlelték, így megelőző intézkedéseket sem tudtak tenni. A rablótámadás megkezdésekor a banki személyzet csak vizuálisan tudta érzékelni a kialakult vészhelyzetet, riasztási szenzorok nem jelezték előre a támadást, így a lehetséges vészhelyzeti intézkedések is a rabláskori események korlátai közé szorultak.
2. A támadási helyszín kiválasztáskor a magas technikai színvonalú, látványos és integrált biztonsági elemekkel kialakított védelmi rendszerekkel bíró fiókokat a rablók elkerülték az alacsony várható nyereség és a nagy lebukási veszély miatt.
3. Az események utólagos humán hatását értékelve megfigyelhető volt, hogy a megtámadott bankfiókok alkalmazottai körében kialakult egy új jelenség, amelyet „Móri szindróma”[1] neveztek el. Ennek hatására a banki dolgozók biztonságérzete a fiókokban jelentősen csökkent, ami komoly kihatással jár az ügyfelek kiszolgálásának és a mindennapi munkavégzés vonatkozásában is.
4. A feldolgozó jelentések összegző részében az ünnepek előtt, illetve a napok bizonyos időszakaiban (nyitási és zárási időpontok) sűrűbben szerepeltek bekövetkezett támadások.

[1] A banki alkalmazottak az erőszakos cselekményektől tartva rettegnek az olyan ügyfelektől, akik valamilyen extrém magatartással kiváltják belőlük a traumás ingereket.

5. A kisszámú, spontán rablási események bekövetkezését csak a humán eredetű, rablást jellemző paraméterek (pl. zavart viselkedés, izgalmi állapot), vagy a fegyver előzetes észlelése esetén lehetett volna tudatosan megakadályozni.

A bekövetkezett eseményeket és a jelzett statisztikai adatokat elemezve arra a feltételezésre jutottam, hogy az új típusú védekezés egyik lehetséges iránya az érzékelés eszközrendszerei kiterjesztésében és az erre támaszkodó előrejelzés fejlesztésében keresendő.

A bankrablást közvetlenül megelőző, a bűncselekmény kísérleti szakaszára olyan új megközelítést tükröző, biológiai detektorokon alapuló fizikai és humán biztonsági funkciókat ellátó, aktív rendszer kifejlesztése lenne kívánatos, amely az esemény folyamatától függően, valós időben a biztonsági riasztások és intézkedések fokozatait indít(h)a(t)ná be.

Szakterületi ismereteim alapján kijelenthetem, hogy a biztonsági rendszerek tervezésekor, a pénzintézeti biztonság területén jó hatásfokkal használnak logikai és fizikai biztonsági rendszereket, de még kevéssé terjedt el a humán biztonsági és bűnmegelőzési szűrésekből fakadó technikai alkalmazások keresése. A biztonsági rendszerek nem hatékonyan integráltak, nem rendszeresítenek biometrikus szenzorokat, amelyek bizonyos védelmi döntések meghozatalát lehetővé teszik.

A humán biztonsági kutatás területén az elkövetői magatartások elemzésére léteznek nemzetközi szakirodalmi megnyilvánulások. A kutatási eredmények azt bizonyították, hogy az elkövetői magatartások olyan jellemző biológiai azonosítókat hordoznak, amelyek e célra fejlesztett biotechnikai eszközök alkalmazásával nyomon követhetők a deviáns magatartási jegyeket hordozó bioinformációk - és így akár a rablásmegelőzés szolgálatába állíthatók.

Elméletileg megalapozottnak tekinthető tehát az a cél, hogy kifejleszthetők, vagy adaptív úton alkalmazhatók olyan intelligens bioszenzorok, amelyek a rablótámadásra jellemző biológiai előjeleket (életjeleket, biológiai paraméter-változásokat) értékelik-elemzik (és a keletkezett információkat egy e célra fejlesztett - nevezzük így - Integrált Biztonsági Központnak továbbíthatják).

Összefoglalóan: a bankrablás tervezésekor és az elkövetést közvetlenül megelőző szakaszban az elkövető egy jól felismerhető magatartási mintázatot hordoz, idegrendszeri és pszichés ismertetőjegyeket közvetít. Amennyiben ezen ismertető jegyek elégséges szintje meghatározható, akkor ezek érzékelésekor a támadási szándék feltételezhető.

Továbblépve:

1. Az említett magatartási mintázat és a fegyver együttes jelenléte egyértelműen meghatározza a bankrablási szándékot.
2. A test infravörös sugárzása, illetve annak változása (dinamizmusa) magában hordozza ennek a magatartási mintázatnak a jellemzőit. Ez nagy pontossággal mérhető.

Ha az említett magatartási, cselekményfüggő biológiai ismertető jegyeket a fejlesztett, vagy alkalmazott biztonsági eszközök felismerni képesek, akkor a feldolgozott és továbbított paraméterek alapján keletkezett riasztást a pénzintézet biztonsági személyi állománya képes kezelni.

A riasztások akár több fokozatúak is lehetnek: az azonnali beavatkozástól kezdődően az ellenőrzést igénylőkig. Ezek működéséből az ügyfél és a támadó semmit nem észlelhet, nem okozhatnak egészségkárosodást és a pénzintézeti üzletmenetet (BCM) sem zavarhatják.

A pénzintézeti biztonságtechnika területén a paradigmaváltás lehetséges irányai közül az egyik út tehát az érzékelés új típusainak alkalmazása lehet.

A másik irány - megítélésem szerint - a beavatkozás, reagálás eszközeinek és módszereinek fejlesztésében rejlik - messzemenően figyelembe véve, hogy a pénzintézeti biztonság elsődleges védelmi feladata az emberélet megóvása és az erre épült az értékvédelem csak ennek szem előtt tartásával működhet.

A reagálási eszközök lehetséges fejlesztési iránya például a bankrablás esetén az ügyféltér elárasztására alkalmas, semleges kémhatású, magas levegőtartalommal rendelkező, ugyanakkor „átláthatatlan”, nagy sebességgel terjedő ködszerű anyag és az azt előállító készülék lehet.

Összefoglalóan: a ködfejlesztő berendezések (ködgenerátor, „füstágyú”) alkalmasak a megkezdett rablási folyamat megállítására és az elkövetők menekülésre kényszerítésére.

A fentiek megállapítása érdekében vizsgálni kell:

1. A köd előállító eszköz alkalmas-e megfelelő mennyiségű és sebességgel terjedő anyag előállítására (pl. a pénztár „eltüntetésére”).
2. Az elkövetőben kialakul-e a menekülés kényszere az alkalmazáskor.
3. Fizikailag kialakítható-e menekülési útvonal.

4. Az alkalmazott eszköz, anyag okoz-e bárminemű egészségkárosodást, illetve annak alkalmazása járhat-e olyan fokozott stressz-hatással, ami az ügyfél egészségét, életét veszélyeztetheti.

A témaválasztás indoklása

Hosszú évek szakmai tapasztalata köt a biztonságpolitika világához, amelyben számos területen tevékenykedtem, láttam el vezetői feladatokat, az utóbbi években oktatói tevékenységet. Munkáimban azonban egyértelműen prioritást a pénzintézetek belső biztonsági folyamatai, azok eszközspecifikációi, humánkockázati elemei és ezek optimalizálásának lehetőségei jelentették. A társadalmi és gazdasági folyamatok alapján egyértelművé vált számomra, hogy a pénzintézeti működések megbízhatósága mind a privát szinten (egyének állami működésbe vetett bizalma és vagyonbiztonsága), mind a vállalkozásokban, és végső soron az állami folyamatokban is elsődleges fontosságú befolyással bíró elem. Ezen elvek mentén kezdtem meg vizsgálataimat a pénzintézeti biztonsági szintek területén.

A biztonságvédelmi tevékenységben alapvetően makro-, és mikroszférát különítünk el, melyben a makrószférába az államilag intézményesített védelem (közrend, közbiztonság, nemzetbiztonság, stb. [1]) fogalomköre tartozik, míg a mikroszférába azokat a privát védelmi területeket és tevékenységeket soroljuk, amelyek biztosítására általában jogos önérdekből, szolgáltatásszerűen kerül sor. [2]

A személy- és vagyonvédelmi vállalkozások legdinamikusabban fejlődő szegmense a pénzintézeti szféra, amely „janusarcú" terület. Ugyanis egyfelől a védelem alapvető biztonsági követelményeit jogszabályi kötöttségű, másfelől azonban a biztonságvédelmi erőforrások jelentős részét, külső személy-, és vagyonvédelmi vállalkozások szolgáltatásszerű működése biztosítja. Kiegészítő, nehezítő elemként értékelhetjük a szolgáltatásokat igénybe vevő magánemberek körét.

Több, speciális tulajdonság jellemzi a pénzintézeti nomenklatúrát:

- a biztonsági tevékenység magas szintű állami kontroll alatt áll;
- a biztonságról való aktív gondoskodás a tulajdonosi önérdekből fakad, ugyanakkor államilag is intézményesített kötelezettség;
- pénzintézeti szolgáltatások átalakulása
    - jelentős globális korszerűsítési folyamatok,

    - indukálják a tradicionális védelmi technikák, eljárások dinamikus fejlődését is;
- a biztonsági infrastruktúrák-, és szolgáltatások jelentős költségű finanszírozása;
- „full service”, vagyis a komplex szolgáltatások iránti igény;
- egzakt mérési technikák bevezetése a szolgáltatási teljesítmények értékelésére, a biztonsági beruházásokra, üzemvitel biztonságra és az őrzési tevékenység végzésére;
- egységes szemléletű és részletesen szabályozott biztonságvédelmi mechanizmus.

Pénzintézeti biztonsággal sokan és sokféleképpen foglalkoztak és foglalkoznak, azonban nagyon kevesen irányították figyelmüket a pénzintézetek speciális szerveire, a „perifériára”, a létezőtől eltérő, innovatív módszerek alkalmazására. A legtöbb kutatás megakad a pénzintézetek alapos vizsgálatánál, működési anomáliáinál és nem lép azon túl. Jelen kutatásommal - figyelemmel a bűnügyi statisztikákra - új, eddig nem alkalmazott, aktív, prevenciós technikákat és a technikai fejlődés mechanikai, elektronikai, sőt biológiai és kémiai eredményeit, valamint a humán kutatások innovációit célzom beépíteni a biztonsági fejlesztési folyamatokba.

Fentiek érdekében dolgozatom egyrészt áttekintést nyújt a pénzintézeti biztonsági folyamatok fejlődéséről és jelenkori működéséről. Számba veszi az erőszakos bűncselekmények generálta legaktuálisabb problémákat, és választ keres arra a kérdésre, hogy miként lehetne a XXI. század kihívásainak megfelelő, leghatékonyabb elveket, módszereket alkalmazni a pénzintézeti biztonság komplex, minden területet átfogó megvalósítása érdekében.

Kutatási célok

A forráskutatás során tett megállapításaim alapján célként fogalmaztam meg, hogy olyan értekezést készítsek, amely megalapozhatja a pénzintézeti biztonsági rendszerek tervezési standardjainak olyan átalakítását, amellyel egyértelműsíthető pénzintézeti biztonsági politika paradigmaváltásának egyre sürgetőbb volta, elengedhetetlensége.

Ugyanakkor célom volt, hogy kutatásom megfelelő alapot teremtsen a terület további tudományos elemzéséhez és vizsgálatához is.

Kutatási céljaimat egyértelműen a preventív aktív beavatkozási, akadályozási módszerek bevezetésének, alkalmazásának, a beavatkozás, reagálás eszközeinek és módszerei-

nek fejlesztéséhez igazítottam, figyelemmel az elmélet és a gyakorlat korrelációs kapcsolatára.

Kiemelt, stratégiai célként határoztam meg a pénzintézeti biztonságpolitika és az aktív prevenciós technikák, illetve a biometrikus szenzorok, és ezen módszerek gyakorlati alkalmazása közötti viszonyrendszer ok-okozati összefüggéseinek globális környezetben történő vizsgálatát.

Ugyancsak célként fogalmaztam meg annak bizonyítását, hogy e kettő alkalmazása biztonsági kérdés, amely alapvető hatással van a pénzintézetek belső biztonságára is.

Speciális célként jelöltem meg, hogy a témával kapcsolatos kutatások, projektek és vizsgálatok feldolgozásával és elemzésével rávilágítsak arra, hogy a bankrablást közvetlenül megelőző, a bűncselekmény kísérleti szakaszára olyan új megközelítést tükröző, biológiai detektorokon alapuló fizikai és humán biztonsági funkciókat ellátó, aktív rendszer kifejlesztése kívánatos, amely az esemény folyamatától függően, valós időben a biztonsági riasztások és intézkedések fokozatait indítja be.

Sajátos célom volt annak bizonyítása, hogy az érzékelés eszközrendszerei kiterjesztésének és az erre támaszkodó előrejelzés fejlesztésének módszereivel (tehát a biometrikus szenzorok alkalmazásával, amelyek bizonyos védelmi döntések meghozatalát lehetővé teszik) fokozható a biztonsági szint.

Kulcscélként fogalmaztam meg, hogy a preventív, aktív beavatkozási, akadályozási módszerek bevezetésének egyértelműen biztonságnövelő hatása van a pénzintézeti működéseket tekintve.

Végül pedig személyes célom az volt, hogy elméleti ismereteimnek és gyakorlati tapasztalataim, amelyeket a választott témámmal összefüggésben szakspecifikus munkákban, projektekben szereztem átadásra kerülhessenek.

Értekezésem hipotézisei

1. **A pénzintézeti életben alkalmazható biometrikus azonosítás módszerére összeállítható egy feladatorientált specifikációlista, amely alapján a legoptimálisabb módszer kiválasztható.**

   A hipotézishez: A biomertikus azonosítás, adatfelvétel lehetőségét általában két klasszikusan nagy csoportra osztják, amelyben a biológiai és a viselkedésbeli pa-

raméterek szerepelnek. A biometriai adatok megbízhatóságát, univerzális alkalmazhatóságát két elem garantálja: egyrészt ilyen adatai mindenkinek vannak és ezen adatok illetéktelen kezekbe jutásának százalékos esélye elenyésző; másrészt ezen adatok ténylegesen személy-specifikusak, egyediek, tehát magas bankbiztonsági előírásoknak minden tekintetben megfeleltethetők.

2. **A dinamikus testhőváltozás detektálása, és elemzése passzív biztonságtechnikai eszközként már alkalmazott elem. Ennek aktív módon történő alkalmazása – pl. az ügyféltérbe lépő személy meleg levegővel való „megfúvása" és a kép elemzése - a bűncselekményi prevenciót támogatja, a befejezett elkövetések számát csökkenti.**

   A hipotézishez: A befejezett bankrablások elkövetési módszereinek elemzése alapján kijelenthető, hogy a ruházatba rejtett fegyver viselése általános elemként szerepel ebben a bűncselekményi kategóriában. Amennyiben még az elkövetések megkezdése előtt hatástalanítható az elkövetéshez használandó fegyver, magát a konkrét bűncselekményt hiúsíthatjuk meg.

3. **A pénzintézet biztonsági rendszerében található egyes technikai védelmi anomáliák, hiányosságok a ködgenerátor alkalmazásával korrigálhatók.**

   A hipotézishez: Maga a ködgenerátor a megelőző aktív beavatkozás eszköze. A magyar pénzintézetek sérelmére elkövetett rablások tapasztalatait összegezve[2] megállapíthatjuk, hogy az elkövetéseket a nagyfokú profizmus jellemzi. Ez az elszántság, nagyobb fokú felkészültség a bankbiztonság szereplőitől is nagyobb szakértelmet, eszközspecifikációt, újabb, hatékonyabb technológiákat követel. A pénzintézeti biztonsági rendszerekben fellelhető akár technikai, akár humánbiztonsági veszély a ködgenerátor alkalmazásával kiiktatható, mivel a ködgenerátor bevetésekor mindennemű fizikai aktivitás ellehetetlenül.

4. **Az élőerő esetleges inkompetenciája generálta biztonsági deficit a ködgenerátor alkalmazásával, és a hozzá kapcsolódó rezsimintézkedésekkel lefedhető.**

   A hipotézishez: Magyarországi tapasztalatok szerint számos esetben segíti elő a bankrablások „eredményes" kimenetelét a biztonsági őrök szakmai dilettantizmusa, mint pl. abban az esetben, amikor az őr percekre őrizetlenül hagyta egy

[2] Forrás: Police.hu http://crimestat.b-m.hu/

pulton a fegyverét.[3] A ködgenerátor specifikus helyzetekben, bankrablásoknál történő bevetésére való szakszerű felkészítés esetén a biztonsági őröknek védelmi, szakmai feladatuk nincs. Ugyanakkor természetesen a képzés ki kell, hogy terjedjen az esetlegesen a banktérben jelenlévő egyéb, vétlen személyekre, és az őket érintő szakszerű fellépésre.

5. **A ködgenerátor alkalmazásával mind az elrettentés, mind a késleltetés területén biztonsági nyereség érhető el.**

   A hipotézishez: Rendőrségi felmérések, vizsgálatok és a befejezett bűncselekmények tapasztalatait feldolgozó kutatások eredményei igazolják, hogy azok az objektumok, amelyek több, különböző vagyonvédelmi technikával, mechanikus védelmi eszközzel védettek (és ez transzparensszerűen kommunikációra is kerül), kisebb százalékban válnak betörés célpontjává. Ezért a nagymértékű biztonsági növekedés első eredménye a ködgenerátor alkalmazására kihelyezett figyelmeztető táblák elrettentést generáló hatásában érhető tetten, objektíven viszont a már kísérleti szakaszba jutott bűncselekmények esetében látható. Az eszköz másodpercekben mérhető működése is már ellehetetlenít bármi fizikai interakciót. Mindez a késleltetéssel lehetővé teszi a hivatalos szervek időbeni helyszínre érkezését.

6. **A ködgenerátor alkalmazása az alkalmazotti állomány, és az esetlegesen jelenlévő ügyfelek tekintetében tartalmazhat humánkockázati elemet.**

   A ködgenerátor kiválthat extrém stresszhelyzetet a vétlen személyek körében, melyet kezelni kell. Az ebben a helyzetben kiváltódott, a pszichológiai kutatások alapján anticipált félelemnek azonosított érzelem kezelhető[3] előzetes tájékoztatással, felvilágosítással.

Kutatási módszerek

A téma jellegéből, összetettségéből adódóan, a kutatási módszerek tekintetében szükségszerű az interdiszciplináris megközelítés alkalmazása. Következik ez abból, hogy a bankbiztonság témaköre több tudományterületet érint. Többek között releváns terület a

[3] Vannak veleszületett félelmek. Ezek a születést követően azonnal jelentkezhetnek, létrejöttükhöz nincs szükség előzetes tapasztalásra és az eseménnyel egy időben azonnal fellépnek. Ilyenek a hangos zajokra, fájdalomra, hirtelen zuhanásra, váratlan mozgásra jelentkező félelmek. Az emlékezet fejlődésével a félelmek elveszítik szituációfüggőségüket és a szocializáció előrehaladásával párhuzamosan megjelenik a szülői intelmek hatására kialakuló, azaz az anticipált félelem.

természettudományokon belül a biológiai tudományok, a társadalomtudományok területén a pszichológia, vagy éppen a műszaki tudományokhoz tartozó informatikai tudományok is. Mindezek figyelembevételével lényegesnek tartottam az interdiszciplinaritás elvének megfelelő megközelítést és feldolgozást.

Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplexitásban történő vizsgálatára.

Elméleti kérdésekben a hatályos jogi normák figyelembevételével közelítettem meg a kérdéseket, amelynek végén a gyakorlati megvalósíthatóság elvét tekintettem célként. Az objektív eredmény elérése érdekében alkalmaztam az absztrakció lehetőségét.

A forrásanyagok feldolgozása, saját kutatásomban történő felhasználása, integrálása, tapasztalatainak leszűrése érdekében felhasználtam az analízis, és a szintézis nyújtotta módszereket. A kutatási eredmények (részeredmények) speciális törvényszerűségeitől az indukció és a dedukció segítségével jutottam el az általánosan elfogadható következtetések megfogalmazásáig.

Az egyes biometrikus és aktív preventív technikák elemzéseinél alkalmaztam az összehasonlítást és a biológiai, pszichológiai, matematikai módszereket is.

A dokumentum-, és kutatáselemzéseket minden esetben saját kutatási témámhoz kapcsolódóan végeztem. Célom volt egy lineárisan permanens, ok-okozati összefüggéseket láttató, átfogó munka megalkotása. Elsődlegesen figyelemmel voltam a gyakorlati tapasztalatok szintézisére, elemzésére, az értékelhető (vég)következtetések megfogalmazására.

Kísérletsorozatot folytattam a vizsgált aktív megelőző eszköz, a ködgenerátor alkalmazásának sajáttapasztalatú elemzése érdekében. Az empirikus adatokból technikai, alkalmazásspecifikációs és humánbiztonsági, pszichoszomatikus jellegű következtetéseket is levon(hat)tam.

Kutatásaimat 2015. november 29-én zártam le, így az azt követő jogszabályi változásokat és tudományos anyagokat ez az értekezés nem tartalmazza.

1. A BIZTONSÁG ÁLTALÁNOS ÉRTELMEZÉSE, LÉTREHOZÁSÁNAK ALAPELVEI, MEGHATÁROZÓ FELADATAI

A biztonság fogalom [1], tartalmi része önmagában, önmagától nem létezik, és nem alakulhat ki.

A tudatos védelemi tevékenységgel megvalósított biztonság egy térkorláttal jellemezhető alapfogalom, olyan kategória, mint pl. a lét és a tudat, ezért megfogalmazni sem lehet csak általánosságban, általánosságokkal kifejezve (nevezetesen pl.: a fenyegetettség hiánya).

Valódi értelmet akkor nyerhet, ha szakjelzőivel hozzárendeljük ahhoz a területhez, amit definiálni kívánunk vele (pl. személy*biztonság*, tűz*biztonság*, vagyon*biztonság*, köz*biztonság*, stb.). [2]

Amennyiben humán közérzeti megközelítésben vizsgáljuk, akkor egy olyan nyugalmi állapotot jelent, amely a veszélyszituációkat megfelelő távolságban tudja tartani attól a személytől, vagy folyamattól, akit, vagy amit védelemben részesítünk.

1.1. A biztonság értelmezésének kiterjesztése [3]

Jelen értelmezésben a biztonság [4] tekinthető olyan alapfogalomnak, amely megteremtésekor elsődlegesen mindig egy élettér, vagyis az abban létező egyén védelmét „hajtjuk végre” a nem kívánt környezeti behatások ellen. Ez csak egy állandó védelemi tevékenységgel biztosított térben valósulhat meg, ahol a fenntartott, előírt és elvárt állapot szerinti szinten megjelenő biztonság, a hozzárendelt erőforrások folyamatos működésének hatására viszonylagosan stabilizálódhat.

A biztonság létrehozását döntően egy állandó egyensúlyra törekvés jellemzi a jelen lévő és várható kockázati szint nagysága és a védelem ereje között. Mindezt - ideális esetben - statikus és dinamikus védelmi elemek tervszerű egymásba építésével hozzuk létre.

A biztonság megléte több, szigorúan szabályozott, egymásra ágyazott cselekmény sorozat eredménye. A létrejött állapot sohasem önfenntartó, folyamatos és a környezeti hatásoktól befolyásolt, vezérelt szolgáltatásszerű üzemeltetést és erőforrást igényel. [5]

A megteremtett és megszokott alapként létrehozott biztonság megléte a benne élő személyeket a külső kockázati tényezők további növelésére, kísértésére sarkallhatja (pl.

sziklamászás biztonsági felszereléssel, bázisugrás), ami ezért újabb veszélyhelyzeteket, kockázati problémákat idéz elő, amelyekre az adandó válaszok a védelmi ráfordítások további növelését jelentik - a kockázati egyensúly fenntartása érdekében.

Egy létesítmény, rendezvény, vagy gazdasági termelési folyamat és azok környezeti biztonságának megteremtésére végzendő feladatok egy összetett, sokténye zős kockázati mátrix alapján határozhatók meg.

Az alapfeladat nyilván a résztvevő szereplők védelme köré csoportosul, de emellett az általuk végzendő szaktevékenység biztonságos és ciklikus lezajlása is a tervezés fő részét képezi.

1.1.1. A biztonság értelmezési korlátai

A biztonsági tevékenység szintjét, külső és belső kockázati elemek egyaránt befolyásolják, motiválják, ezek kockázatarányos gátlása, vagy kizárása záloga a sikeres biztonsági, védelmi munkának.

Egy katasztrófakutató példabeszédében azt találta mondani, hogy „Ha Dél-Amerikában egy pillangó meglebbenti szárnyát, [6] az akár cunamit is okozhat Japán partjainál”[1]. A bekövetkezett kockázati események rossz esetben képesek egymást olyan szinten gerjeszteni, hogy végeredményben láncreakciók kialakításával, akár katasztrófák okozására is alkalmassá válhatnak. Ebből következik, hogy minden megismert védelmi cselekményünk tekintetében ártalmasnak ítélt kockázati eseményt a keletkezése pillanatában és helyszínén kell akadályozni, vagy felszámolni - a kárkockázati veszteség csökkentése, minimalizálása érdekében. A multiplikáció ekkor, és csakis ekkor akadályozható meg kellő hatékonysággal (természetesen az is elgondolkoztató kérdés, hogy a véletlenszerű vagy sztochasztikus események mi módon ismerhetők meg és vehetők figyelembe a védekezés tervezése során).

A biztonság szemszögéből vizsgálva két elfogadott mérőszámot, illetve ezek variánsait szokták felhasználni a veszélyhelyzeti értékelésekor kockázati elemként. Az egyik az események bekövetkezésének gyakorisága, a másik pedig az okozható kár nagyságának mértéke. Ezeket viszonylag egyszerű statisztikai adatokon alapuló számítások alapján kifejezhetjük és a kockázati mátrixba illesztve számításaink során felhasználhatjuk.

[1] A mondat eredete Edward Lorenz 1963 tanulmányában gyökerezik, ahol a szerző a káoszelméleten belül a véletlenszerű folyamatok pozitív visszacsatolásáról és azok lehetséges hatásairól értekezik.

A „szárnylebbentésre” gondolva azonban azzal is számolnunk kell, hogy a kár-, vagy katasztrófaeseményt, akár egy eddig nem ismert cselekmény, vagy egy új beavatkozás által keletkezett következményhatás idézte elő. Ezért lényeges minden új eszköz, folyamat, gyártás bevezetése előtt környezettanulmányt végezni: felmérve, hogy a beavatkozás okozta változások milyen reakciókat hozhatnak létre a kiválasztott helyszínen, amelyek esetleg további láncreakciót indíthatnak el[2].

Nyilván a helyesen megválasztott kockázatmátrix alkalmazása lehetőséget biztosít a tudatosan optimalizált védelemre, de egyben felelős kockázatvállalásra is tanít: a kockázat bevállalási határ mértékének kiválasztása nagy hozzáértést, és felelősségtudatot követel.

A már kialakított, egy adott mikroterületre értelmezett védelmi rendszerek, makrórendszeri egységükben vizsgálva ronthatják, vagy javíthatják egymás hatékonyságát - függően az illesztettségük szintjétől. Praktikusan a feladatorientált védelmi koncepciók mentén érdemes a makró-, és mikrorendszereket egymásba ágyazni, illeszteni, az ideális hatásfok elérése, vagy növelése érdekében. A védelmi koncepció megfogalmazásánál pontosan meg kell határozni a védekezés célját, irányát és területi integritását. Nincs értelme és nem is lehet minden veszélyelemet figyelembe venni, de bekövetkezésük lehetőségét, hatásának nagyságrendjét teljességgel elvetni sem lehet.

A területi értelmezés korlátait is a védekezési célok pontos követése mentén szükséges megállapítani. A meghatározható és felismert kockázati elemekből kiindulva, kötelező területi érvénnyel kell zárttá tennünk a szükséges, adott területre értelmezett védelmi rendszert. Végiggondolva a lehetséges térnövelő lépéseket (személy, lakás, település, ország, Európa, Föld, bolygóköz, stb.) olyan szédítő és átfoghatatlan közeghatárok kerülnek elénk, amelyekre, és amelyekben a védekezési lehetőségek és a ráfordítható költségek fogalmai értelmezhetetlenné válnak.

[2] Pl. a ködeszközt működésbe hozó kézi vezérlő használatával megakadályozunk egy rablási helyzet továbbfejlődését. Ugyanakkor a kiszellőztetéskor a szomszédban üzemelő automatikus oltórendszer a füst hatására beindul és a védelmi területet vízpárával elárasztva tönkreteszi az ott üzemelő eszközöket (a kialakuló szekunder hatásokat tehát akadályozni kell).

1.2. A kockázatarányosság igénye [7]

A biztonsági feladatok tervezésekor a teljes körű védelem létrehozására törekszünk, bár tudjuk, hogy a gyakorlatban ennek elérése szinte lehetetlen. Ennek gyökér okai között a következőket érdemes figyelemmel venni:

- A valós kockázati elemek teljes vertikumának megismerése lehetetlen, mivel egyes bekövetkezések meglehetősen véletlenszerűek, és időnként egymással is ok-okozati összefüggésben vannak (komplex, összetett kockázatmátrix modell alkalmazásával közelíthetjük legjobban a valóságot optimálisan követő folyamatrendszert).
- A megismert kockázatok teljes biztonsági lefedése költségoldalról olyan aránytalanságot tükröz a haszon/ráfordítás függvényében, hogy az kivitelezhetetlenné válik. Ezért azokat a kockázatarányos megoldásokat tartjuk ideális lehetőségnek, amelyek a megismert kockázati elemek bekövetkezési lehetőségének bizonyos hányadát tudatosan bevállalják.
- A humán kockázati tényezők kezelése. [8] A legvariábilisabb kockázati csoportok tartoznak ide, ráadásul ezek egyedi stabilitása is több tényező mentén és akár teljesen ellentétes irányban változhat. Egy védelmi, védekezési folyamat leggyengébb láncszeme leggyakrabban maga az ember. [9] Ennek minimalizálása az automatikusan működő, személytől független, intelligens rendszerek alkalmazásával és az ezekhez szorosan kapcsolódó rezsimintézkedések működtetésével érhető el. [10]

Nyilvánvaló, hogy statikus biztonsági állapotot kialakítani szinte soha nem tudunk, mert a folyamatok, és végrehajtási környezetük dinamikus egyensúlyban vannak egymással, bármelyik minimális változása is a kockázatelemzési paraméterek láncfolyamati változását vonja maga után.

A biztonság kockázati alapú megítélése esetén alaposan végig kell gondolnunk az értelmezésünk felügyeleti hatáskörébe vont végzendő szaktevékenységeket is. Nincs értelme külön személy-, munka-, tűz-, környezet-, energia-, hálózat-, adat-, információbiztonságról beszélni. Mindezeket egységes biztonsági kockázatkezelő felületbe integrálva a megoldás hatékonysága, és egyben a gazdaságossági mutatók ugrásszerű javulást mutatnak.

Eljutva azokhoz a határfelületekhez, ahol még rejtett biztonsági tartalékok találhatóak megállapítható, hogy ezek a védelmi tevékenységet végző csoportok együttműködési lehetőségeiben, szervezeti illesztettségében, valamint a biztonságvédelmi rendszeregységek ideális összepárosításából adódó előnyökben rejlenek.

További kockázatcsökkentési lehetőséget hordoz magában a bekövetkezett káresemények elemzése indukálta előrejelzések figyelembe vétele (pl.: árvízi előrejelző rendszer létrehozása és alkalmazása). Ezen a helyen egy nem szokványos példa talán megbocsájtható nekem: a legenda szerint Hunyadi Mátyást 1458. január 24-én, Budán, a Duna jegén választották királlyá. Ezen jelentős létszámban az ország főurai, főpapjai és nemesi elitje vett részt. Mai fejjel gondolkodva a következőkre figyelhetünk, illetve tételezhetjük fel:

- A rendezvényt biztosító katonai parancsnok nevét nem jegyezték fel.
- Nincs adat róla, hogy ellenőrizték-e a Duna jegének teherbírását, a terület (felület) maximális befogadóképességét, sőt a síkosságra, elcsúszásveszélyre felhívó táblák kihelyezéséről sincs tudomásunk.
- Nem tudjuk, hogy jelöltek-e ki menekülési útvonalakat.
- Az esetleges terrorveszélyt valószínűleg nem vizsgálta senki (pedig tudjuk, hogy ez a korszak elég viharos, hatalmi harcokkal terhelt időszak volt).

Mindezek után megállapítható, hogy valószínűleg csak a szerencsén múlott, hogy az akkori Magyarország királyát, elit vezetőgárdáját nem érte baleset, támadás. Jelen korunkban ilyen felelőtlenséggel már nem állhatunk hozzá egy hasonló szintű jelentős rendezvény lebonyolításához. Egy nagy tömeget és VIP vendégeket mozgató esemény biztonságos lebonyolítása jelentős tervezési feladatot igényel, előre meghatározott forgatókönyv (scenario) alapján - a kockázatminimalizálás érdekében. Ebben természetesen a személybiztonság elsődlegességét a vagyon és folyamatbiztonsággal folytatva értünk volna el a „Duna jegének" szilárdságtani vizsgálata és „csúszékonysága" (súrlódási tényezője) tényéig.

Egy jól előkészített, technikailag megtervezett folyamat biztonságát - különösen, ha ennek ciklikus ismétlését is tervezzük - részelemeire bontva szükséges lépésről lépesre kidolgozni és felügyelni.

A tervezés kezdetén meg kell azokat az ismert belső és külső kockázati elemeket határozni, amelyek az ideális működést akadályozhatják (ebbe beleértendő az illegális hoz-

záférés, a szabotázs, a terrorveszély, a kémkedés, sőt a reputációs kockázat is). Ezek tükrében kell létrehozni azt az ideális, a védelem szempontjából kívánatos biztonsági teret, amely a személyi és a folyamatműködési kockázati elemeket minimalizálja. Mindezt időben, térben és szervezésileg illeszteni kell a környezetben már működő biztonsági rendszerekhez.

Ezek elvégzése után a folyamat megindulhat: előbb kísérleti, majd állandó üzemben. Ellenőrizni kell, hogy a működés kezdetekor a kockázatminimalizálás úgy valósul-e meg, ahogy terveztük: ha igen, akkor fenntartását a folyamatos kontrollponti ellenőrzésekkel biztosítható (ami egyben a szükséges módosításokra is lehetőséget biztosít). Ezen időszakban folyamatosan ellenőrizni kell a folyamat közvetlen környezetének változásait is, mert a folyamatbiztonság fenntartását ez is jelentősen befolyásolhatja.

1.3. Az alkalmazotti jelenlétből, viselkedésből fakadó biztonsági feladatok

Az elmúlt évtizedek történései az alkalmazotti kört erodálták, biztonságérzetük csökkent, megbízhatóságukkal kapcsolatosan gyakran megfelelőségi problémák vetődtek fel - szakmai és sajnos erkölcsi téren egyaránt. [11] Ezek a problémák kialakulásának döntő többsége közvetlenül a végrehajtási környezetben keletkezik, ott detektálható és egyben meg is akadályozható. Ezért különösen lényeges a biztonsági szemléletmód kiterjesztése, a szabályozott környezet létrehozása és az automatikusan működtetett, kikerülhetetlen kontrollok alkalmazása.

A kontroll-folyamatok bevezetése, fenntartása, és a visszacsatolásokból adódó szükség szerinti frissítése vezetői feladat és felelősség. Ennek többlépcsős ellenőrzése, hatékonyságának rendszeres értékelése a záloga a kockázati elemek megfelelő alacsony szinten tartásának és a biztonság humán oldali magas minőségű megvalósulásának. [12]

A biztonsági szolgáltatások [13] minőségének megítélése körül gyakran alakulnak ki értelmezési viták. Ennek megelőzésére a biztonsági minőségellenőrző rendszerek kidolgozása és bevezetése a legcélszerűbb megoldás, hiszen ezeknek a feltételeknek a megállapítása, jogszerű rögzítése már az alapszerződés szintjén megoldható. [14] Hosszabb távon a minőségbiztosító rendszerek uniformizálása, kiterjesztése és kötelező alkalmazása megteremtheti az egységesen értelmezett és elvárt szolgáltatási szinteket.

A biztonságtechnikai eszközök [15] alkalmasak arra, hogy az egyéb humán szolgáltatásokkal összerendelve, kikerülhetetlen ellenőrzési pontként működjenek - kikényszerítve

az előírt kontrollok végrehajtását. Ez jótékonyan segítheti a folyamatbiztonság fenntartását, mivel a folyamatok végrehajtásának gyorsítási „megoldásai” között gyakran fordul elő az előírt kontrollok rövidítésének, vagy akár a biztonsági elemek alkalmazásának kihagyása. A körültekintően és a lehető leghatékonyabban megtervezett technikai kontroll segíti a védelmi folyamatot [16] - annak működésbiztonsága fenntartása mellett.

1.3.1. Az védelem alá vont személy fizikai, magánéleti és üzleti titkainak biztonsága [17]

A célszemély biztonságának védelmét tervezve, köré - gondolatilag - egy őt körülvevő, burkoló gömböt képezünk, amely a számára ártalmas külső környezeti behatásokat a lehető legnagyobb mértékben kizárja. Ez a védelmi rendszer dinamikusan kell, hogy igazodjon a külső környezeti behatások nagyságának és típusainak változásaihoz, ezért egy folyamatosan jelenlevő, kontrollrendszer működésével vezérelt, a terhelés függvényét követő védelmi erőforrásra van szükségünk a biztonság elvárt szintű fenntartására.

Azért, hogy ezt megtehessük, elsődlegesen fel kell ismernünk azokat a létrejöhető lehetséges ártó tényezőket, melyek a célszemélyt veszélyeztetik, számára kockázati tényezőként jelentkeznek.

Némileg bonyolítja a helyzetet az, hogy a láncfolyamati kockázatok, illetve a még be nem következett, így nem ismert kockázati tényezőket nem tudjuk előre figyelembe venni. Ekkor a felismert kockázati tényezők elleni védekezés optimális eszközeinek meghatározását is el kell végeznünk, beillesztenünk a védelmi rendszerünkbe azért, hogy a „burkoló gömböt” megszerkeszthessük, erőforrásának szükséges elemeit biztosítsuk.

A fizikai védelem tervezésénél [18] ezek a műveletek plasztikusan, egyénre igazítottan nagy biztonsággal elvégezhetők. Azt azonban tudnunk kell, hogy a védekezés tervezésében a legmagasabb kockázati fokot képező veszélyelem maga a célszemély, aki a veszélyforrások generálása tekintetében általában a legaktívabb. Ez a szabály különösen érvényesül a célszemély magán és üzleti titkai védelmének tervezése esetén.

A titokvédelem elsődleges szabálya a célszemély kioktatását írja elő a saját tevékenysége és kommunikációja tartalmi részének kialakításával kapcsolatosan. Ez azt jelenti, hogy tevékenységével és magánéleti titkaival kapcsolatosan meg kell

szerkeszteni azt a kommunikációs-, és közeghatárt, amely biztosítja a védett információi sérthetetlenségét. Ez tulajdonképpen még csak általános fogalmi feladat, mert a kommunikációs határok kialakításánál messzemenően számít (és figyelembe veendő) a célszemély családi környezete, a közeg, amelyben tartózkodik, illetve az alkalmazott kommunikációs eszköz, amelyen az adatközlést végzi, végezzük.

A közeg, amelyben tartózkodva kommunikálunk, nem csak a velünk közvetlenül együttlevő személyekből állhat, hanem a hallótávolságban levő egyéb személyek is kockázati tényezőként szerepel(het)nek.

Mindezek után következik a céltudatos információvadászok és az ő információszerző technikai eszközeik elhárítási feladatainak tervezése.

Több évtizedes tapasztalataim birtokában bátran kijelenthetem, hogy az információvesztés, adatszivárgás bekövetkezésekor elvégzett vizsgálat eredményeképpen több mint 90 %-os volt az adatgazda által bekövetkezett figyelmetlenség, „jólértesültség", vagy felelőtlenségi okokra visszavezethető adatvesztési esemény.

Az üzleti vagy magánéleti „hírszerzés" legbiztosabb forrásai a vendéglők, sportpályák, baráti társaságok, stb., ahol az információ birtokos célszemély megfordul. Technikai eszközök bevetése ezekben az esetekben nem feltétlenül szükséges: a feladatot egyénre szabottan célszerű elvégezni és a külső kontrollok mentén a szivárgási forrásokat felderíteni.

1.3.2. Az ipari kémkedés objektiv veszélye, megvalósulási területei [19]

Az ipari kémkedés rendkívül kényes kérdés, határai szinte kontúrmentesek, gyakoriságára nincs valós adat, de bizonyosan állítható, hogya dinamikus és feszült gazdasági helyzetben bármilyen ellenfélről szerzett, előnyt biztosító információ gyüjtése és felhasználása csökkenti a kiugrás lehetőségét, versenyhelyzeti pozíciót és a termék eladhatósági lehetőségeit (pl. a Play Station II., vagy a Samsung-ügy).

A termelés védelmi biztonságát meghatározó, alapvető kérdések:

- a termék szabadalmi korlátai, újszerűsége;
- a forgalmi és a kereskedelmi adatok;
- ügyfélköri adatok;

- a fejlesztésben vagy a kivitelezés irányításban résztvevő szakemberek „elcsábítása” - megtartása;
- az alkalmazotti kör megbízhatósága;
- alapanyag beszerzési kérdések.

A leírtak az értékteremtést, mint alapfolyamatot veszik figyelembe és az általános, kihagyhatatlan védelemtervezési alapokat foglalják össze. Nyilván egy konkrét feladat során további specifikus szempontok is megjelenhetnek.

1.4. A létesítmények működtetésének kockázati alapfeltételei

Ahhoz hogy bármilyen értékteremtési műveletet megkezdhessünk, a végzendő folyamatok működésének ideális feltételeit [20] kell megteremteni. Ez a létesítményi, eszköz, erőforrás, energiaszolgáltatási és logisztikai elemek biztonságos működésének megteremtése mellett lehetséges csupán. [21] Ezek bármelyikének veszélyeztetése a produktum előállítására, vagy az elvárt teljesítményre vannak negatív hatással, tehát magának az értékteremtés folyamatának az útjában állnak.

A működési folyamatok biztonságának veszélyeztetése kritikusan befolyásolja az értékteremtés lehetséges nagyságát. A biztonsági feladatok tervezése, a létesítmény kialakítása az üzemeltetésés az értékesítés folyamatait körülveszi és a kialakult veszélyhelyzetek, valamint az újólag formálódó, valós biztonsági feladatok mentén dinamikusan változik.

Az optimális működést garantáló ellenőrző biztonsági auditot magánbiztonsági szolgáltatásként, polgári jogi szerződés alapján, biztonsági szakemberek végzik az alábbi módszerekkel:

- dokumentumok tanulmányozása,
- interjúk készítése,
- helyszíni szemlék,
- információkérés hatóságoktól,
- fedett módszerekkel megfigyelés,
- helyzet-beállításos gyakorlati kísérlet,
- SWOT analízis alapján kockázatelemzés-készítés.

Az audit összefoglaló jelentéssel zárul, amely tartalmaz biztonságvédelmi javaslatokat is.

A következőkben az itt említett területeken haladunk végig kissé részletesebben.

A megvalósítás első lépéseként a megfelelő helyszínt kell kiválasztanunk, ahol az értékteremtés folyamatait kívánjuk végezni, feltételezve, hogy az elméleti tervezési, technologizálási folyamatok már lezajlottak. Ezen a ponton a folyamatok kettéválnak - függően attól, hogy új létesítmény építéséről, vagy már egy meglévő objektum átalakításáról beszélünk. A kiválasztás fázisai a következők:

A fizikai megfelelőség meghatározásának kérdései:

- alkalmasság a kívánt feladatra (tagozottság és szintezettség, teherbírás a szükséges eszközpark ismeretében, befogadási szempontok, belső közlekedési lehetőségek, menekülési útvonalak kialakítása, szociális szükségletek),
- katasztrófa helyzetek gyakorisági kérdései (a kiválasztott helyszín környezeti katasztrófa helyzetének elemzése, árvíz, földrengés, tűz stb.),
- a szükséges energia igények ellátásbiztonsága (a létesítmény valós igényeinek megfelelő mennyiségű és minőségű, folyamatosan elérhető energiaforrások megléte vagy megteremtése),
- informatikai és hírhálózati csatlakozás lehetőségei (telefon, net),
- logisztikai feladatok végrehajtásának követelményei (a szállítás és a közlekedés szükséges mértékű meglétének, vagy a létrehozás biztosításának lehetőségei),
- munkaerő ellátás környezeti forráslehetőségei (megfelelő létszámú és képzettségű munkaerő biztosítása a feladatok végzésére).

Biztonsági kockázati kérdések:

- a környezet bűnügyi fertőzöttsége [22] (a közvetlen környezetben kialakult bűnügyi fertőzöttség felderítése, a külső támadások elleni védelem kialakításának lehetőségei, költségei),
- a tervezett létesítmény értékteremtési folyamatához rendelt szükséges védelmi szint meghatározása (bizalmasság, titkosság, adatvédelem, hozzáférés-korlátozás, védelmi technika szükséges szintje, őrzés, épületfelügyelet, tűz-, munka-, környezet-, foglalkozás-egészségügyi kérdések, pandémiás terv, stb.),
- BCP, DRP tervek meghatározásának szükséges szintje, rendkívüli esemény esetén szükséges váltóhelyek kiválasztása, a folyamatos üzemelés minimumszintjének meghatározása (katasztrófa bekövetkezése esetén az üzletfolytonosság szintjének meghatározása, krízis bizottság megalakítása, vészhelyzeti feladatok végrehajtási terve, az üzemelés helyreállításának terve),

- a biztonsági terv elkészítése (a fentiek teljes ismeretében készül a létesítmény részletes védelmi terve, amely feladata az ideális működési feltételek biztosítása).

A megvalósítás alapkérdései:

- a kivitelezési terv és az abban meghatározott alapanyagok tervi pontossága a tervekben meghatározott és elfogadott paraméterek megvalósításának fokozott ellenőrzése),
- minőségi-, és garanciakérdések (a felhasznált anyagok és a kivitelezési munka minőségének garantálása a kivitelező által),
- engedélyezési folyamatok (a létesítmény működéséhez szükséges hatósági engedélyek teljes körű beszerzése, illetve időszakos felülvizsgálatának intézése),
- parkolási lehetőségek (a dolgozók, látogatók, ügyfelek, valamint a szükséges logisztikai és szállítási tevékenységek parkolási lehetőségeinek előkészítése).

A létesítmény üzemszerű működtetése:

- a működés törvényi feltételeinek teljes megteremtése, [23]
- beléptetés rendjének és eszközeinek meghatározása (a biztonsági szint határozza meg a beléptetés, a belső mozgás rendjét és dokumentálását, ennek része a vendégek és a külső vállalkozók beléptetésének, benntartózkodásának rendje is),
- szállítás rendjének kialakítása (az áruforgalmat végző járművek ki-, és beléptetése, nyilvántartása, a szállítási útvonalak és segédeszközök biztosítása, a tárolóhelyek kialakítása, védelme, az anyagmozgatás-biztonsági ellenőrzés),
- termelési folyamat igényei (a termék előállításának folyamatát körülvevő biztonsági tevékenységek irányítása, végzése, többszintű ellenőrzése),
- a termelési folyamathoz tartozó munkavédelmi feladatok (munkavédelmi szabványok szerinti megfelelőség folyamatos biztosítása, betartásának ciklikus ellenőrzése, alkalmazotti oktatások szervezése),
- termékvédelem (a létrehozott termék szükség és előírás szerinti védelme, tárolás, szállítás közbeni ellenőrzése).

1.5. Az 1. fejezet összefoglalása

Ebben a fejezetben magával a biztonság fogalmi meghatározásával, elemzésével foglalkoztam.

Megállapítottam, hogy a biztonság egy rendszer külső és belső elemeitől egyaránt vezérelt, veszélyektől mentes, de dinamikus állapota, amelyben a biztonság kockázati alapú megítélését helyeztem előtérbe. Ennek a viszonylagosan veszélymentes, nyugalmi állapotnak a fenntartása érdekében statikus és dinamikus elemek kerülnek alkalmazásra.

Gyakorlati példák, illetve a „pillangó effektus" felhasználásával szemléltettem a kockázatmátrixban feltüntetett védelmi koncepciók fontosságát, pozitív hatását a biztonságot veszélyeztető eseményekre és kimenetelükre.

Kiemeltem a teljes körű védelemre való törekvés megfogalmazásában a kockázatarányosság igényét. Ebben a folyamatban egyértelműsítettem, hogy a valós kockázati elemek teljes vertikumának megismerése lehetetlen. Emiatt azonban elengedhetetlen a biztonsági szemléletmód kiterjesztése, a szabályozott környezet létrehozása és az automatikusan működtetett, kikerülhetetlen kontrollok alkalmazása. A biztonságtechnikai eszközök alkalmasak arra, hogy az egyéb humán szolgáltatásokkal összerendelve, kikerülhetetlen ellenőrzési pontként működjenek - kikényszerítve az előírt ellenőrzések végrehajtását.

Megállapítottam, hogy bankbiztonsági-biztonságtechnikai értelemben aktív és passzív eszközök alkalmazása szükséges, amelynek során a védelem alá vont személy fizikai, magánéleti és üzleti titkainak biztonsága elsődleges fontosságú.

Lényegi elemként foglalkoztam a létesítmények működtetésének kockázati alapfeltételeivel, amelynek konklúziójaként egyértelműsítettem, hogy elengedhetetlen az optimális működést garantáló ellenőrző biztonsági audit elvégzése. Ennek alappilléreiként határoztam meg a következőket:

- a fizikai megfelelőség meghatározásának kérdései;
- biztonsági kockázati kérdések;
- a megvalósítás alapkérdései;
- a létesítmény üzemszerű működtetése.

2. A PÉNZINTÉZETI BIZTONSÁG FOGALMA, EREDETE, MÚLTJA, JELENE ÉS JÖVŐJE

Az általános biztonsági feltételek [1] megteremtése meglehetősen szövevényes folyamatokat feltételez, [2] széles kitekintéssel, sok, látszólag nem összefüggő elméleti és gyakorlati kérdéssel foglalkozik - teszi mindezt a teljesség érdekében.

A pénzintézetek működése során történetileg - a lehetőségek és szükségletek sodrása mentén - kialakult egy alaposan körülszabályozott biztonsági koncepciórendszer, amelynek a megváltoztatásához mindenképpen a biztonság fejlődési szakaszait, lényeges állomásait, okait, korlátait alaposan elemezni és értelmezni szükséges.

Meg kell ismerni a jellemző támadási módszereket, ugyanakkor az érvényes szabályozási környezetet ahhoz, hogy hatékonyan, a pénzintézeti valós igényekhez és lehetőségekhez igazítottan lehessen fejlődni ezen a területen is.

2.1. A pénzintézetek technikai biztonságának történeti fejlődése [3]

Magyarországon 1841 októberében nyílt meg az első kereskedelmi bank, így országunkban a pénzintézeti biztonsági tevékenység fogalma, eredete ez időtől számítható.

Kezdetekben ez a biztonsági tevékenység a szilárdság és az áthatolhatatlanság növelésével volt egyenértékű. A bank működéséhez szükséges pénz szállítására erős, megvasalt járművek és a nagyszámú fegyveres kíséret volt az általánosan elfogadott lehetséges védekezési forma.

Ez időben az úgynevezett „kasszafúrás”, vagyis a páncélszekrények feltörésével elkövetett lopás volt a jellemző banki „elegáns” bűnelkövetési forma, ami az intelligens bűncselekmények csúcskategóriájába tartozott. Ezeket jellemzően éjszaka, zárás után, minél csendesebben, fondorlatosan kitervelt módon bejutva a bankfiók belsejébe - kényelmesen, kihasználva a jelzőrendszerek hiányát - hajtottak végre.

A méregdrága speciális páncélszekrények megfúrása, kinyitása jelentős műszaki ismereteket és különleges, e célra készített, fejlesztett eszközöket követelt meg végrehajtójától. Volt idő, amikor a nyomozók, az elkövetés módszeréből nagy biztonsággal a végrehajtó személyét is meg tudták állapítani az egyedi, a „kasszafúróra” kizárólagosan jellemző páncélszekrény nyitási módszerek ismeretében. Ezeket az elkövetőket egyfajta

szakmai tisztelet övezte tárgyi tudásukért, időnként még hivatalosan is igénybe vették speciális felkészültségüket.

A másik jellemző pénzintézet elleni elkövetési forma a jóval primitívebb, erőszakosabb bankrablás volt. Ekkor a nyitvatartási időben rontottak a rablók a bankfiókra és erőszakkal jutottak az ott található pénzhez. Ezen módszerek megakadályozására legfeljebb az élőerős őrzési formát alkalmazhatták a bankárok, amelynek eredményessége nagy reménnyel nem kecsegtetett - lévén a támadás bekövetkezéséről értesítést küldeni, vagy segítséget kérni híradó, informatikai rendszerek nélkül szó sem lehetett.

A technikai eszközök fejlődésével a védekezést különféle jelzőrendszerek alkalmazásával próbálták fokozni: jelzőcsengők, mechanikus „távdrótok", kötelek, csőtelefon, leeső jelzők mechanikus, később elektromos változatain keresztül alakultak ki napjaink behatolás-jelző eszközei, rendszerei. [4]

Az utóbbi eszközcsalád - minden lehetséges behatolási módszer figyelembe vételével és ismeretében - tagozódott nyitás, mozgás, rezgés, falbontás, robbantás, törés, stb. érzékelőkre. A keletkezett jelzéseket feldolgozó intelligens központi egységek pedig - felkészítve az elkövetési cselekmény lehetséges módozataira - az ezekre kifejlesztett intézkedési, védelmi programcsomagok alapján reagálnak.

A behatolás-jelző eszközök kialakulása után felmerült a kültéri vészjelzés igénye (a külvilág figyelmének felhívására a támadás eseményéről). Létrejöttek tehát a külső hang-, és fényjelző eszközcsoportok.

A hatékonyan és megbízhatóan működő berendezések megszülték a következő problémakört: a szabotázs elleni védelem létrehozásának feladatát. A bűnözők a védelmi eszközök blokkolásával, kiiktatásával (szabotálásával) próbálták helyreállítani az addig meglevő erőviszonyokat, azaz előnyre szert tenni. Elvágták az elektromos kábeleket (villany, távközlés), megrongálták, működésképtelenné tették a hang és fényjelző berendezéseket. Ezért kialakultak a második védelmi kört képviselő szabotázsvédelmi rendszerek, amelyek feladata a behatolás jelző eszközök hiteles működésének védelme, támadásuk esetén pedig riasztás-jelzés indítása.

A riasztó rendszerek eredményességük révén olyan sikeressé váltak, hogy nagy számban alkalmazták egyéb, hétköznapi területen is (lakások, gépjárművek, boltok). Ennek eredményeképpen a sok jól, de még többé-kevésbé sikerült és felszerelt eszköztől zengett a környezetünk... Ez aztán ahhoz vezetett, hogy elvesztette a külső riasztás a hite-

lességét. Külön problémaként jelentkezett, hogy a rendkívüli hangnyomású jel a támadókat is „stresszelte”, és ez több esetben ember elleni bűncselekmények kialakulásához vezetett.

Felvetődött ezért támadás esetén az átjelzés igénye, amikor a behatolás-, vagy a támadás-jelző rendszer közvetlenül az intézkedésre jogosult helyre küldi el valós időben a támadás tényét, helyét és módját meghatározó jelcsomagot olyan módon, hogy a támadó mindezt nem érzékeli (viszont a reagálásra kijelölt erők ezen információk birtokába jutva intézkedhetnek). Az átjelzések technikai színvonala a leeső jelzőtől napjainkig a szabotázsvédett, többbutas, IP alapú, valós idejű kép-, hangtartalommal bíró csomagjáig jutott el - a technika fejlődéséből adódó lehetőségek [5] ma úgy tűnik - még koránt sem kimerítettek.[1]

A felügyeleti szereppel megbízott hatóságok részéről megfogalmazódott igényként a napi és a rendkívüli események dokumentálási igénye a bekövetkezett cselekmények utólagos bizonyítása, elemzése, elemezhetősége érdekében. Ennek megoldására jelentek meg a különféle képrögzítő eszközök. A kezdeti robot fényképezőgépektől napjaink digitális technikájáig elérkezve gyorsan elszaladt az idő: az események meghatározott időtartamig történő hiteles rögzítésére, tárolására, visszajátszására, vagy - támadás esetén - a megfelelő végpontra történő továbbítására alkalmasak ezek az eszközök.

A pénzintézetek területén zajló belső mozgások szabályozására, ellenőrzésére, nyomon követésére a beléptető rendszerek gyakorlatilag korlátlan választéka ad lehetőséget. Ezek az eszközök alkalmasak a belépő személy azonosítására, jogosultsági szintjének megállapítására és a belépés tényének, valamint a benntartózkodás időtartamának megmásíthatatlan tárolására.

A pénzintézeti kockázatok csoportjába tartozó katasztrófaesemények jelzésére, elhárítására szolgáló eszközök, berendezések is a biztonságtechnika részei. Leglényegesebb ezek közül a tűzjelző-, tűzoltó eszközök családja. Az integrált tűzbiztonsági rendszerekben a személyvédelem és a menekülési útvonalak biztosítása, a tűz terjedési útjának zárása, valamint speciális kármegelőző oltórendszerek üzemeltetése programozható, alapvető célfeladat.

[1]A jelenleg alkalmazott un. Robotzsaru Rendszer tökéletes megvalósulása e tételnek [20/2011. (X. 7.) ORFK utasítása a támadásjelző rendszer működtetéséről, ORFK Tájékoztató (OT), 2011/14. szám, Budapest, 2011. október 13.].

Egyéb, az elemi károk, katasztrófaesemények bekövetkeztét gátló-érzékelő eszközöket is alkalmazhatunk még biztonsági rendszereinkben (pl.: szénmonoxid-, széndioxid-, metán-, nitrózusgáz-, stb. érzékelők).

Mindenképpen meg kell említeni még a terrorcselekmények megelőzésére, elhárítására alkalmazható eszközpark néhány elemét is:

- speciális gázok, méreganyagok, kábítószerek, vegyi és biológiai, radioaktív, valamint robbanó anyagokat érzékelő, valamint a
- fémdetektorokat és csomagvizsgáló eszközöket.

Minden védelmi eszköz alkalmazásának szabályozási rendszere is több szinten kialakult. A szabályzatok jog-, és eseménykövetően változnak.

2.2. A pénzintézeti biztonság lehetséges új alternatívái a hazai viszonyok alapján

Ahhoz, hogy a magyar pénzintézetek biztonságának lehetséges jövőképét megalkothassuk, mindenképpen szükséges fejlődésük útját, [6] eredményeit, valamint a jelen időszak történéseit elemezni. [7]

A bankbiztonsági jövőkép megfogalmazására makró-, és mikrokörnyezetünk jelentős befolyással bír, ugyanis a globális behatások meghatározó elemei egyre intenzívebben formálják át közvetlen életterünket is. [8] Ez nyilvánvalóan igaz a magyar pénzintézetek működési biztonságának értelmezésére is, hatására jelentős átalakulások mennek folyamatosan végbe a védekezés eszközei és módszerei tekintetében.

Megítélésem szerint ezeknek a változásoknak a szignifikáns jellemzői a következők:

- A változtatások igénye - amelyeket a működésbiztonság előírt szintjének fenntartása érdekében szükséges végrehajtani - folyamatossá váltak, állandósultak (pl. megjelentek a kódolt pénzszállító táskák, időzárakat alkalmaznak a pénztároló helyeken, bevezették a multisafe-rendszert az ügyféltérben, kialakult az internetes (számítógépen, mobil telefonon futtatott) „bankolás” bonyolult kódkapcsolati rendszere, a chip-kártyás alkalmazás, a paypass-módszer, stb.). [9]
- Az egyedi, Magyarországra különösen jellemző bűnmegelőzési megoldások - amelyek a hazai pénzintézeti bűncselekmények megismert, jellemző típusainak elhárítási módszereit tartalmazzák - már elégtelennek bizonyulnak napja-

inkban, mivel megjelentek (és elszaporodtak) a globális (európai) mintát követő pénzintézeti bűncselekmények (ATM fosztogató bandák, idegen számlákról hamis átutalást végző külföldiek, pénzváltó „zsonglőrök", stb.).[2]

- A védekezési lehetőségek és azok eredményeinek értelmezése, megoldásának nézőpontjai, forrásai eltérőek - még a feladatot meghatározó szakértői körökben is.[3]

Nyilvánvaló, hogy a magánbiztonság egyes, alapvető kérdései egységes szabályozási elvek, törvények, törvénymódosítások kialakítására várnak, amelyet - a többirányú behatások figyelembe vétele mentén - sürgősen el kell végezniük a jogalkotóknak. A magánbiztonság teljes területét illetően az átfogó, értelmező, szabályozó törvény igénye fogalmazódik meg, amelynek megalkotása szintén a jogalkotókat terheli - természetesen jelentős magánbiztonsági szakértői háttértámogatással. [10]

A nemzetközi gazdasági együttműködések és a nemzeti gazdaságok működésének vizsgálata, kockázati elemzéseik, valamint fenntartásának tudományos analízise során kialakultak a kritikus infrastruktúrák, ennek mentén pedig a minimális működés feltételeit biztosító alapegységek működési elmélete. Ennek pedig a pénzintézeti szegmens meghatározó alapeleme.

2.2.1. A pénzintézetek, mint a kritikus infrastruktúrák alapelemei [11]

A kritikus infrastruktúrák alatt „…olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működképesség, közegészségügyi és környezeti állapot fenntartásában." [12]

A kritikus infrastruktúrák működésének egyik meghatározó eleme a pénzintézeti szektor, mivel a gazdasági működés fenntartásának alapfeltétele a pénzforgalom biztosítása a kategóriákba foglalt alapegységek között. A 2080/2008 Kormányhatározat (amely a Zöld könyvben foglaltak magyar megvalósítását írja elő) a VII. kategóriába sorolja 31.

[2] Forrás: http://www.police.hu/

[3] Érdekes példa erre, hogy 2010-ben az Adatbiztonsági Napon, dr..Kerezsi Klára előadásában tért arra, hogy a térfigyelő kamerarendszerek szakmai használati értéke erősen kétségbe vonható. Ugyanezen alkalommal dr. Jóri András (akkori adatvédelmi ombudsman) a térfigyelő kamerarendszerek kialakult (nyilván eredményes) alkalmazása és a törvényi szabályozás személyiségi jogi ütközéseinek kérdéseiről beszélt.

sorszámmal a banki és hitelintézeti biztonság megvalósításának feladatait. Az intézmények védelmének biztosítását a tulajdonosok felelőségi körébe utalja. A pénzintézetek - mint alapkategória elemek - működése nélkül bármely más alapkategória elem működése megbénulhat, ezzel kihatva a többi rendszerelem alapműködésére is (helyi és globális szinten egyaránt).

Nyilvánvaló, hogy a magyar pénzintézetek mindazokkal a globális kihívásokkal, kockázatokkal és veszélyekkel, valamint ezek következményeivel is szembenéznek, amelyek a fejlett világ többi pénzintézetét érik.

Ezek felsorolásszerűen:

- Globális kihívások: demográfiai robbanás, energiahordozók kimerülése, víz, élelmezés, a természeti erőforrások problémája, környezetszennyezés, globalizáció, társadalmi egyenlőtlenségek.
- Globális kockázatok: migráció, fegyverkereskedelem, vallási ellentétek, nacionalizmus, tömegpusztító fegyverek terjedése.
- Globális fenyegetések: szervezett bűnözés, terrorizmus, kábítószer-maffia.

A fentiek részelemeikben, vagy következményeikben megjelennek a pénzintézeti biztonság védelmének célterületei között, ezért praktikusan egységes fellépési irányelveket szükséges megfogalmazni és alkalmazni.

Az Európai Unió Tanácsa mindezen globális kihívásokkal, kockázatokkal és fenyegetésekkel szemben közös fellépést tervez és szervez - egységes irányelvek és közös intézkedések bevezetésével. 2001. május 28-án a bűnmegelőzés kiemelt fontosságának jelzése érdekében tanácskozást folytattak, amelynek eredményeként az alábbi irányelveket alkották meg [13]:

- Csökkenteni kell a bűnalkalmakat, növelni kell annak valószínűségét, hogy a bűncselekmény elkövetőjét elfogják, és méltón megbüntetik.
- Redukálni kell a bűnismétlés lehetőségét.
- Csökkenteni kell az áldozattá válás lehetőségét.
- Terjeszteni kell a jogkövetés kultúráját országon belül.
- A prevenció lehetőségeit ki kell fejleszteni, technikai és intézkedési szinten be kell mindezt vezetni.

A fentiek gyakorlati megvalósítása megköveteli:

- a globális elkövetési módok folyamatos megismerését,

- a kimunkált preventív megoldások adaptív átvételét, és ezek alapján
- a pénzintézeti szabályzások szükséges módosítását - az előbbiek érvényesülése érdekében.

A biztonság tehát az előbb leírtak alapján egy állandó gerjesztéssel létrehozott és fenntartott szükséges és elvárt állapotot jelent - egy meghatározott (körülhatárolt) térre vonatkoztatva. [14]

Fő iránya mindig a személyre mutat, vagy a személy életteréhez köthető. A pénzintézetek az élettér részei a végzett tevékenység tartalma alapján mind az alkalmazottak, mind az ügyfelek [15] szempontjából.[4] Az ő biztonságuk és biztonságérzetének fenntartása meghatározó feladat. Ennek megteremtése több feltétel (technikai, élőerős őrzés, rezsimek, működési utasítások, szabályozások) együttes teljesülése esetén következhet csak be. [16]

Ezek vázlatszerűen:

- Technikai feltételek:
  - a mechanikai védelem kialakítása, a fizikai szilárdság megteremtése védelmi eszközök alkalmazásával;
  - elektronikai jelző és dokumentáló eszközök telepítése, azok szakszerű üzemeltetése;
  - banki folyamatok szabályozása, és a szabályzati elemek következetes alkalmazása (rezsimintézkedések betartása és betartatása).
- Élőerős őrzés felállítása:
  - a készpénzforgalom biztosítására,
  - a bankfiókok működési rendjének támogatására,
  - az intézet belső és külső rendjének biztosítására.

A technika és az élőerő együttes alkalmazása, tevékenységük egymáshoz illesztése, harmonizálása, valamint a szabályzati rend következetes alkalmazása határozza meg a biztonsági, védelmi tevékenység hatékonyságát és színvonalát. Ennek megvalósítása magasszintű minőségbiztosító háttérmunkát követel meg a biztonsági vállalkozástól.

Az előzőekben leírtak biztosítása érdekében a biztonsági szolgáltatásokat nyújtó vállalkozásokkal kötendő szerződéseknek tartalmaznia kell az alábbiakat (felsorolásszerűen):

[4] Egyik releváns területe ennek a social engineering (Douglas P. Twitchell: Social and Organizational Liabilities in Information, Security, Illionis State University, 2009)

- a feladatok és az elvárások szakszerű meghatározása;
- a szolgáltatói tevékenység elvárt minőségének pontos és részletes leírása;
- a végrehajtás ellenőrzési normáinak ismertetése;
- külön minőségbiztosítási mellékletet.

2.2.2. A pénzintézetek kárára elkövetett jellemző bűncselekmények és elkövetési módok[5]

A történeti fejlődés nyomon követhető e tekintetben is. Alapvetően megállapítható, hogy a banki biztonság fejlődésével (amit döntően az elkövetett bűncselekmények inicializálnak), a bűnözők is folyamatosan változtatják elkövetésük módszereit és irányait.

Amennyiben általános alapelveket kívánunk rögzíteni, akkor a klasszikus két bűnelkövetési mód nyomon követhető a kezdetektől napjainkig. A pénzintézetek és az alkalmazott védelmi eszközök fejlődése csak a módszerek változtatásait, finomításait hozta magával - maguk a bűncselekmény típusok megmaradtak napjainkig.

Ezek a csoportok és a hozzárendelt végrehajtási alfajok a következők:

- Erőszakos bűncselekmények:
  - bankrablás,
  - pénzszállítás közbeni rablás,
  - ügyfélrablás pénzfelvétel után,
  - banki és bankkörnyezeti terrorcselekmények,
  - ATM kirántásos műveletek,
  - ATM robbantásos műveletek.
- Intelligens bűncselekmények:
  - csalás,
  - banki alkalmazotti oldali cselekmények,
  - ügyfél oldali elkövetések (szándékos és vétlen),
  - informatikai rendszeren adathalászás.
- Banki eszközök ellen elkövetett bűncselekmények:
  - ATM támadások speciális (kifinomult) eszközökkel, módszerekkel,
  - Banki külső belső hálózatok elleni támadások.

[5] ENYÜBS: Egységes nyomozóhatósági és ügyészségi bűnügyi statisztika
http://crimestat.b-m.hu/Default.aspx, letöltve:2015. szeptember 10.
http://www.police.hu/

Magyarországon az elmúlt években jellemző pénzintézeti bűncselekmények a következők voltak (figyelembe véve az előző felsorolást):[6]

- Erőszakos bűncselekmények:
  - bankrablás: ez a bűncselekmény a tudatos védekezés és az együttműködés eredményeként megritkult, csak szórvány cselekmények tapasztalhatóak és inkább a Takarékszövetkezeti szektorban (2012);
  - ügyfél ellen elkövetett rablás: az ún. „Nápolyi" rablás (kifigyeléses, kerékkiszúrásos módszerekkel - köszönhetően a folyamatos ügyféltájékoztatásnak megritkult) egy-egy esemény fordul csak elő.
- ATM támadásos cselekmények: [17]
  - ATM kitépéses és robbantásos módszer: amióta beszerelésre került a robbanó festékes védelmi eszköz az ATM berendezésekbe, azóta gyakorlatilag megszűnt ez a támadási forma.
  - Ragasztás: ezt a módszert az ATM-ek belső védekező rendszerének fejlesztése felszámolta.
  - Kártyaadatok lemásolása technikai eszközökkel: az ATM fejlesztések hatására a klasszikus módszerek letűnőben vannak. Egy új eszköz felbukkanásával viszont komoly károkat okoznak (megfúrásos, kivágásos technika): komoly elektronikai-informatikai háttérismerettel és speciális olvasó eszközzel lopják el a kártyaadatokat és általában egzotikus (pl. délamerikai) országokból fosztják le a számlákat. A kontrollhívásos módszer egyre inkább kiszorítja ezeket a módszereket.
  - Kampózás: az ATM eszköz „reverse" funkcióján alapuló, nem kifinomult módszer. Igazi veszteség, hogy megrongálja az ATM- et.
  - Csalási bűncselekmények.
    - Ügyfél megszemélyesítéses módszerek: a személyazonosítás módszereinek kijátszásával, belső együttműködő partner alkalmazásával.
    - Lízing eszközök eltüntetése: a csődeljárás hiányosságainak kihasználásával.
    - Elektronikus bűncselekmények: informatikai rendszer ellen irányuló támadások (rendszerrongálások, DOS, DDOS, stb.).

[6] forrás: http://www.police.hu/

- Informatikai rendszeren keresztül megvalósított csalások (belső visszaélések, internet banking, applikációs hibák kihasználása, stb.).
- Adatszerzéssel megalapozott csalások (phising, bankkártya visszaélések, ATM manipulációk).

2.3. A pénzintézetek technikai védelme [18]

A (biztonság)technikai védelem fogalmi rendszere magába foglalja az épületek és egyéb építmények mechanikai, valamint elektronikai eszközökkel történő védelmét, továbbá az ezek alkalmazásához meghatározott módszereket és eljárásokat (rezsimeket).

A biztonságtechnikai, műszaki követelmények meghatározása és az egyes, ezekhez kapcsolódó feltételek biztosítása kizárólagosan a bankbiztonsági szolgálatok tervezési feladatát képezik.

A bankbiztonsági szolgálat felelősségi körébe tartozik (és előzetes véleményét ki kell kérni) a bankcsoporti működés céljára szánt ingatlanok vétele, az új iroda-, és fiókberuházások, illetve bővítések építészeti tervpályázatának kiírása, vagy építészeti tervezése esetén. Ezért a tervek építésügyi hatósági engedélyezésre való benyújtása, a kivitelezési tervek elfogadása is csak a bankbiztonsági szolgálat előzetes egyetértésével történhet (amit a terveken minden esetben rögzíteni kell).

Az elektronikai védelem megtervezéséről, kivitelezéséről, műszaki átvételéről és rendszeres karbantartásáról, valamint a tárgyi tevékenységhez tartozó kötelezettségvállalási jog gyakorlásáról - a jóváhagyott beruházási terv szerint - kizárólagosan szintén a bankbiztonsági szolgálat gondoskodik (a biztonságtechnikai védelmi rendszer jóváhagyott tervétől eltérni is csak a bankbiztonsági szolgálat hozzájárulásával lehet).

2.3.1. A pénzintézetek mechanikai és elektronikai védelmének tervezési szempontjai, a védelem eszközei [19]

A mechanikai védelem tervezése esetén az objektumunk védelmének koncepcionális kialakítását a többkörös védelmi szemléletmód jellemzi. Az létesítmény közvetlen környezete (pl. udvar, környező lakóépületek, közvilágítás) és a megközelítés lehetőségei (bejáratok, útvonalak, forgalom, stb.) is fontos szerepet játszanak a tervezés megkezdésekor. Az ügyfélbeléptetés, a pénzszállítási útvonal és a létesítmény védelmének megoldásai alapvetően szabják meg a későbbi működésbiztonságot.

Az objektum belső területének mechanikai védelemi feladata a héjszerkezet határvonalán kezdődik. Az épített szerkezetek, és a nyílászárók megválasztásánál a MABISZ által kibocsátott Betörés-biztonsági Szabályzat mellékletében meghatározott, kötött minőségű elemek alkalmazását, beépítését szükséges előírni és alkalmazni.[7]

Az épület héjszerkezetén belül a további mechanikai biztonsági előírások a következők:

- a belső pénzforgalmi tereket markáns, elválasztásra szolgáló épített megerősítésekkel és biztonsági ajtók zsilipszerű alkalmazásával kell a publikus terektől leválasztani;
- a pénz átadás-átvétel biztonságát átadózsilippel és kiépített szeparált pénzszállítási útvonallal kell megoldani;
- szabvány által garantált pénztároló eszközök (trezor, páncélszekrény, multisafe) és az időzárak alkalmazásával kell meggátolni az illetéktelen pénzhez jutást, illetve a sikeres rablásokat.

Az eszközök csak akkor teljesítik a tervezett elvárásokat, ha az előírt üzemeltetési és biztonsági szabályokat az alkalmazottak maradéktalanul betartják.

A mechanikai biztonsági eszközök önmagukban nem alkalmasak a támadás megakadályozására. Feladatuk egyrészt az elrettentés, valamint az áthatolás előírt időtartamú késleltetése (elrettentés, késleltetés). A fizikai védelem teljessé tételét a biztonságtechnikai rendszerek, valamint az élőerős őrzés integrációjával érjük el (detektálás, elhárítás).

A biztonsági védelmi folyamat első lépéseként el kell készíteni a létesítmény funkcionális működési tervét, meg kell határozni az ehhez szükséges dolgozói létszámot és a forgalomhoz rendelt várható pénzértékhatárokat.

Ellenőrizni szükséges, hogy a működési elvárások szintjének megfelelő mechanikai biztonsági szilárdsági mutatókat teljesítő felületek rendelkezésre állnak-e (ha nem, akkor ezt azonnal az elvárási szinthez kell igazítani).

Ezek után a MABISZ által kibocsátott Betörés-biztonsági Szabályzat ide vonatkozó előírásainak figyelembevételével kell elkészíteni a létesítmény teljeskörű Biztonságtechnikai Tervét.

---

[7] Az áthatolás gátlásának legegyszerűbb módszerei a vastagítás. A koronafúrás ellen speciális alakú és változó keménységű fémelemek beépítésével, míg az oxigénlándzsás támadások ellen áramkorlátozással, valamint erős, szerves füstöt termelő kompozit anyagok alkalmazásával növelhető a védekezés szintje.

A Biztonságtechnikai Terv teljes részletességgel kell, hogy foglalkozzon - funkciónként és helyiség-típusonként - az előírások szerinti részleges és teljes elektronikai biztonsági rendszerek [20] meghatározásával.

A **behatolás-jelző rendszerek** három fő részre tagozódnak: [21]

1. Az érzékelő eszközök a behatolási cselekmény által okozott változásokat jellemző fizikai paraméterek detektálásán alapulnak. Képesek a rezgés-, mozgás-, hőmérsékletváltozás, sugárzás, különféle gázjelenlét kimutatására, mérésére és megbízható, valós idejű kijelzésére. Általában többféle jelformáló fizikai módszer alkalmazását kombinálják egy érzékelő eszközben, amely révén a téves riasztás lehetősége jelentősen csökkenthető.
2. Az érzékelők által kibocsátott jeleket a jelzővonalak vezetik a központi egységbe. Feladatuk átvinni az érzékelők által kibocsátott jel pontos helyét, időpontját és típusát - megbízható, szabotázsvédett módon a központi egységbe.
3. A központi egység a beérkezett jelek kezelésére, értékelésére szolgáló vezérlő szoftver programja szerinti előírások végrehajtását, a teljes rendszer felügyeletét, tápellátását és szabotázsvédelmét végzi. Vezérli a hang és fényjelző berendezéseket, valamint indítja a távátjelző egységet a riasztási esemény kialakulásakor.

E rendszer szerves részeként - de önálló funkcióval - működik a támadásjelző hálózat. Feladata, hogy rablótámadás esetén azonnal csendes riasztást kezdeményezzen. A támadásjelző rendszer jeladóit rejtett módon kell elhelyezni (működtetésük észrevehetetlen legyen a támadó számára).

Következő nagy eszközcsoport a **beléptető rendszerek**é: [22]

- Az érzékelés módja szerint megkülönböztetünk mágneskártyás (kártyaolvasós), közelítéses (proximity, chip), aktív jeladós, valamint biometrikus típusú rendszereket.
- Feladatuk: a beléptetés és az épületen belüli mozgások automatikus, programozás szerinti vezérlése, belépési jogosultság-csoportok kezelése, a cselekmények folyamatos dokumentálása, a rendkívüli események azonnali jelzése. Összehangoltan működik (és ha kell, együttműködik) az épület egyéb biztonsági berendezéseivel (pl. tűzjelző rendszer). Alkalmassá tehető a tartózkodási hely megállapításra, az informatikai (telefon) vonal automatikus továbbirányítására, munkaidő nyilvántartás adatainak gyűjtésére, a rendszer hozzáféré-

si adatok és helyi egyéb jogosultságok tárolására (pl. kávéautomata használat). Szükség esetén az informatikai jogosultság megállapítása is hozzárendelhető. [23]

A következő csoport a képrögzítő, eseménydokumentáló rendszereké (**CCTV**). A velük szemben támasztott főbb követelmények és előírások a következők: [24]

- szélsőséges fény és hőmérsékleti viszonyok között is minőségi képalkotás,
- megváltoztathatatlan idő-, és tartalomdokumentálás,
- hiteles, megváltoztathatatlan tartalmú adattárolás,
- megfelelő (és a törvény által engedélyezett, előírt) időtartamú tárolás/törlés funkció,
- kizárólag a regisztrált személyek részére: eseménydokumentált hozzáférés,
- a távadat átviteli igények kielégítése az engedélyezett irányokba,
- folyamatos (24/7) üzembiztonság.

A kamerák tekintetében jelentős készletválaszték áll rendelkezésre, amelyek kiválasztását és alkalmazását döntően a feladatokból fakadó igények határozzák meg (MOP - Mission Oriented Application = Feladatorientált Alkalmazás).

A képrögzítési tevékenység a személyes adatok kezelése kategóriába tartozik, ezért a rendszer üzemeltetésére a személyes adatok kezelésére vonatkozó tőrvények érvényesek**.**

Az **átjelző rendszerek**kel [25] kapcsolatos elsődleges elvárás, hogy a behatolás-, és a tűzjelző rendszeren keletkezett jelzésekből - az előzetesen meghatározott rendezési és sorrendi elvek alapján kiválasztottakat - biztonsággal és tartalmi módosítás nélkül, azonnal továbbítsa a diszpécser-központba. Itt az intézkedési jogosultsággal rendelkező személyek az utasítások szerint járnak el.

Lényeges szempont az átjelző központ és a helyi rendszerek összeillesztése, megfelelő programozhatósága és 24 órás üzemképessége, az átviteli csatornák szabotázsvédettsége, az ügyeletesek gyors reagálása, a kontroll és értesítési rendszerek helyes működése, a reagáló egységek pontos, valós idejű informálása, stb.

Egy bankrablási szituáció helytelen kezelésének következményei beláthatatlanok. A Rendőrség a nappali támadásjelzések fogadására IP felületű felügyeleti rendszert fejlesztett ki, amely alkalmas a valós idejű jelfogadásra, felügyelt intézkedésre, folyamatos

képfogadásra, és kommunikációra. Lehetővé teszi a bankrablási helyzetek kezelésének, felszámolásának ismételt értékelését.

A **tűzjelző rendszer**ek [26] a biztonságvédelmi tevékenység katasztrófavédelmi ágát képviselik. Feladatuk a létesítményben keletkezett tűzesemények azonnali jelzése, speciális esetben (intelligens rendszer telepítése esetén), az oltás megkezdése (spinklerek, speciális oltógázok révén), a tűzterületek menekülési útvonalainak megnyitása és egyéb, az épületfelügyelettel kapcsolatos programozott intézkedések megtétele.

A tűzjelző rendszer központja az érvényes törvényi szabályozás alapján a tűzjelzést a területileg illetékes Tűzhatóságnak közvetlenül is köteles jelezni - párhuzamosan az átjelző rendszer központjával.

A bankrablás elrettentés, megelőzés egyik lényegi elemeként említhetők meg az elektronikus időzárak, amelyek megakadályozzák:

- az üzemidőn kívüli páncélszekrény-, vagy páncélajtó-nyitást,
- üzemidőn belül nagyobb összegek azonnali felvételét (a nagyobb összeget tároló rekeszek csak a beprogramozott idő intervallum után nyílnak a pénz felvételének kezdeményezése esetén),
- a riasztás bekövetkezése után bármilyen értéktároló szekrény vagy helység kinyitását tiltják.

Viszonylag új eszköze a bankrablások elleni küzdelemnek az ún. robbanó pénz vagy bevezetési nevén a „dye-pack”. Az eszköz aktív részét a pénztári pénzjegykötegek közé telepítik. Amikor a rabló elhagyja a bankfiókot, akkor lép működésbe az eszköz. A teljes bankjegykészletet, valamint a rablót is erős sárga, speciális szerves festékfüsttel eltávolíthatatlanul beszínezi. A pénz így értéktelenné válik, a menekülő elkövető elfogási esélye pedig jelentősen megnő.

2.3.2. Az élőerős őrzés előírásai, feladatai [27]

Az értékőrzés szerepét, feladatait a 283/2001 Kormányrendelet értéknagysághoz és tevékenységi körhöz kötötten határozza meg.

A bankfióki szolgálat ellátásához nem szabályozott egyértelműen a fegyver szükségessége. Világszerte fegyvertelen biztonsági őrök őrzik a banki ügyféltereket. Ennek oka, hogy az ügyfelek és alkalmazottak testi épsége került az első helyre (a biztonsági őrtől

elvehetik a fegyvert, tűzharc alakulhat ki, stb.)[8] az értékvédelemmel szemben (az utóbbiak védelmét döntően az új technikai megoldásokra és az időzárakra bízzák).

A biztonsági őr alapvető feladata az őrzés, amelyet az Őrszolgálati Utasításban, helyszínre szabottan kell elkészíteni. Ez tartalmazza:

- a beléptetés, belépés, biztonságos nyitás-zárás felügyeletének, az ügyfélkiszolgálás menetének zavartalan biztosításának, az ügyféltéri felügyeletnek a rendjét;
- a rendkívüli események megelőzésére vonatkozó szabályokat;
- a rendkívüli események bekövetkezésekor végrehajtandó speciális feladatokat;
- a válsághelyzetek kezelésének feladatait;
- a bankcsoport dolgozóinak és ügyfeleinek védelmét a bankcsoport területén;
- a bankcsoport tulajdonának, értékeinek védelmét, a pénzforgalom-, pénzszállítás felügyeletét, a kommunikáció, a kapcsolatok kezelését, a szabályok ismeretét, betartását és betartását, öltözeti és viselkedési normákat.

Kiegészítő feladatként jelenik meg:

- a biztonsági rendszerek üzemeltetése, működésének megfigyelése, és bizonyos rábízott biztonsági rendszerkezelési funkciók elvégzése;
- a rendkívüli események előírásszerű kezelése, a katasztrófahelyzetek menedzselése, a káresemények megakadályozása, rabláshelyzet kialakulása esetén a konfliktus kezelése.

Prevenciós feladatai közé tartozik:

- a deviáns magatartási formák észlelése, az ilyen tevékenységek akadályozása, jelentése (fiókfelderítés, ügyfélkifigyelés, a parkolóban illetéktelen személy tartózkodása, nem megengedhető kapcsolatok észlelése, stb.).

A fiók biztonsága érdekében az őrszolgálat szervezésekor stabilizálni kell az őrállomány személyi összetételét, a helyettesítés, valamint az ellenőrzés rendjét, ciklikusságát és az alkalmazott ellenőrzési módszereket (az őrzés minősége döntően az ellenőrzés

[8] Magyarországi tapasztalatok szerint számos esetben segíti elő a bankrablások „eredményes” kimenetelét a biztonsági őrök szakmai dilettantizmusa, mint pl. abban az esetben, amikor az őr percekre őrizetlenül hagyta egy pulton a fegyverét (http://www.uzletihirszerzes.hu/szemely-es-vagyonvedelem/2276-vltozsra-van-szksg-a-bankbiztonsg-terletn.html, 2015. szeptember 1.)

következetességén múlik).

A fizikai biztonság három alappillére a hagyományos pénzintézeti védelem meghatározója. Működésük eredményességét a körülölelő előírások, azok betartása és betartatása határozza meg. Ezek megléte, az új feladatok és szabályozásváltozások mentén történő módosításuk (tehát naprakészen tartásuk) ennek a témakörnek rendkívül fontos eleme.

A válságkezelés, rizikóelemzés témakörében, [28] valamint a bekövetkezett események analízisének eredményeiből a pénzintézeti vezetők részére tájékoztató előadásokat kell tartani, míg a pénzintézeti alkalmazottakat ciklikus biztonsági oktatásban kell részesíteni a következő témakörökben:

- a pénzintézetek elleni erőszakos bűncselekmények felismerése, megelőzése és a szükséges viselkedésformák;
- a pénzintézetek ellen irányuló „fehérgalléros" és egyéb bűncselekmények (lopás, okmányhamisítás, hamis átutalás, sikkasztás, stb.) felismerése - gyakorlati tapasztalatok alapján;
- a bankfiókok működési biztonságának feltételei, a Bankbiztonsági Szabályzatban foglalt felelősségi kérdések megismerése, a létesítmény egyedi biztonsági szabályainak megtartása;
- a krízishelyzetekre való felkészülés feladatai, BCP (Business Continuity Plan - Üzletmenet-folytonossági Terv), DRP (Disaster Recovery Plan - Katasztrófa-helyreállítási Terv), a bekövetkezett események kezelése;
- a titokvédelem témaköre, adatköre (banki, üzleti, magán), a titokvédelmi szabályok betartásának szükségessége, a titoksértések vizsgálata;
- a minősített iratok törvényi előírásoknak megfelelő kezelése;
- válaszadási kötelezettség hatósági megkeresésekre.

2.3.3. Pénzintézeti belső vizsgálati tevékenység [29]

Az alap vizsgálati folyamatban az elkövetett bűncselekmények észlelése, kivizsgálása, büntetőeljárás kezdeményezése jelenik meg.

Több bűncselekmény folyamatos feldolgozásából már az elkövetést lehetővé tevő hiányosságok, tanulságok levonhatóak, beépíthetők az elhárító és megelőzési munkába (elemzés, értékelés). A magyar (és külföldi) bankokat érintő bűncselekmények megismeréséből fakadó tanulságok feldolgozásával és integrálásával az elhárító tevékenység tudatos prevencióvá és bűnmegelőzési tevékenységgé válik.

A pénzintézeten belüli együttműködés és információáramlás megszervezése elengedhetetlen feltétele a működési biztonság [30] megteremtésének, amely mind a banki dolgozók, mind az ügyfelek biztonságérzetének erősítését szolgálja.

Csalás-, és veszteség-megelőzési vizsgálócsoportok kialakításával, célzott prevencióval jelentős eredménynek érhetők el a védelemben, belső esemény-adatbázis létrehozásával (szigorúan figyelembe véve a törvényi megfeleltetést) jól hasznosítható elemző-értékelő tevékenység végezhető.

A bűnüldözés és bűnmegelőzés hatékonysága érdekében a pénzintézet biztonsági munkatársai a hatósági vizsgálati szervekkel (rendőrség, ügyészség, NAV, titkosszolgálatok) személyes, naprakész kapcsolatokat alakítanak ki, és tartanak fenn.

A védelmi tevékenységben a kriminológia és a kriminalisztika eszközeinek és módszereinek alkalmazásával az eredményesség jelentősen fokozható.

A tudatos bűnmegelőzési tevékenység jellemzői: [31]

- országos szintű oktatásokat kell szervezni az elkövetések eszközeinek, módszereinek széleskörű megismertetése érdekében (ez segít az áldozattá válás megakadályozásában is);
- az elkövetett bűncselekmények jellemzőit adatbázisban kell rögzíteni, az eseteket elemezni, értékelni, majd statisztikai módszerekkel feldolgozni és ennek alapján kidolgozni a megelőzés új módszereit;
- a bűnismétlés gátlása érdekében a megismert támadási felületeket, hibás folyamatokat módosítani kell;
- a vizsgálati eredmények alapján kialakított prevenciós folyamatokat széles körben be kell vezetni;
- oktatási és ellenőrzési módszerekkel támogatottan terjeszteni kell a jogkövetés kultúráját.

A pénzintézetek biztonsági szolgálatainak bűnmegelőzési együttműködésében a Bankszövetség intézményrendszere a közös gondolkodás katalizátora lehet. Ez a pénzintézeti bűnmegelőzés jövője, ennek bázisán kialakulhat egy új tartalommal rendelkező tudományág is.

2.3.4. A rendkívüli eseményeket kezelő szabályzási rendszer kialakítása [32]

„Rendkívüli esemény” fogalma alatt értjük a bank funkcionális feladatainak ellátását akadályozó, vagy megbénító szándékos magatartások, illetve más események összessé-

gét, amelyek magukban hordozzák személyek életének, testi épségének veszélyeztetettségét, súlyos vagyoni kár bekövetkezésének a lehetőségét, vagy ezek tényleges bekövetkezését.

A rendkívüli események fajtái:

- bankrablás (bankrablás túszejtéssel),
- robbantással való fenyegetés (bombariadó),
- bankfiókon belüli rendzavarás,
- a bank egyéb érdekeit sértő tevékenység.

Részleteiben:

Bankrablás (bankrablás túszejtéssel) **[33]**

A bankrablás egy, vagy több személy által fegyverrel (fegyvernek látszó tárggyal), vagy felfegyverkezve elkövetett pénz-, értékszerzésre irányuló, jogellenes tevékenység.

Túszejtésről beszélünk, ha a bankrablást végrehajtó elkövető(k) a biztonságosabb menekülés érdekében a bank alkalmazottai, vagy ügyfelei közül valakit túszul ejtenek, és akadályoztatásuk esetére a túsz életének kioltásával fenyegetnek.

A bankrablásra készülő személy felismerése:

- A bankrablás végrehajtása előtt az elkövető(k) több alkalommal is helyszíni felderítést végez, hogy minél pontosabb információkkal rendelkezzen(ek) a tervezett bűncselekmény sikeres megvalósításának esélyeiről. A megelőzés érdekében ezért nem csak a biztonsági személyzet, hanem a banki alkalmazottak előzetes felkészítése is fontos (pl. az éves oktatás keretében): kísérjék figyelemmel a bankban gyanúsan, céltalanul, esetleg a banképület közelében tartózkodó személyeket. Gondosan ellenőrizzék a bank területén munkát végző külső vállalkozókat, vagy más szolgáltatási tevékenységet végzőket.
- A bankrablásra készülő személy próbálja az alkalmazottakat kifaggatni. Érdeklődése kiterjed:
  - a biztonsági őrök létszámára,
  - a biztonsági őrök felszerelésére, mozgási körletére, esetleges váltásuk időszakára,
  - a biztonsági őr megfigyeli-e az ügyfeleket, az ügyfelek felszerelését, táskáit,
  - a banki alkalmazottak és különösen a pénztárosok odafigyelnek-e az

ügyfelekre, vagy csak automatikusan végzik feladataikat,
    - van-e az épületben, vagy előtte állandó jelleggel őr,
    - a rendőrjárőr megjelenési ciklusai, érkezési-, távozási útvonala,
    - a pénzszállítás gyakorisága, időpontja, módszere (gépjármű, táska, stb.),
    - mikor van a pénzforgalmi csúcsidő,
    - mikor van a legkisebb ügyfélforgalom,
    - a bank nyitásának-zárásának mechanizmusa,
    - hol vannak elhelyezve a biztonságtechnikai eszközök.
- A rablást előkészítő konkrét viselkedés jellemzői:
    - többszöri megjelenés a bankban várakozó, ügyintézésre váró ügyfél benyomását keltve,
    - feltűnően, gyakran végez pénzbefizetést, kivételt, melynek során tanulmányozza az alkalmazottak szokásait, viselkedését, a pénzkezelési folyamatokat, eszközöket,
    - beszélgetést kezdeményez a banki dolgozókkal a személyes kontaktus kialakítása érdekében,
    - tudni akarja, hogy milyen módon történhet esetleges nagyobb összeg kifizetése, be kell-e azt jelenteni előzetesen,
    - szándékosan csomagot „felejt” az ügyféltérben, amiért később visszatér (ezzel mintegy teszteli a biztonsági szolgálat éberségét),
    - szándékosan rendzavarást idéz elő (ellenőrzi a biztonsági szolgálat esetleges intézkedését, az kér-e segítséget),
    - zárás előtti pillanatokban, amikor már nincs ügyfél rosszullét színlelése (az alkalmazottak viselkedésének felmérésére),
    - a bank-, illetve a fiókvezetővel szeretne beszélni az üzemi területen belül (felmérve ezzel a bejutás lehetőségét),
    - üzletemberként szolgáltatást ajánl fel kedvező feltételekkel (hogy megismerhesse a banképületet, pl. takarítás, szigetelés, festés-mázolás).

Az előbbiekben leírtak esetén, vagy gyanúsan viselkedő személyek vonatkozásában a bank alkalmazottainak előírt feladatai a következők:

- alaposan megfigyelni a személyt (hogy később pontos személyleírást tud-

janak adni róla),

- ismételt visszatérés esetén fokozottan figyelni mozgását, van-e társa az ügyfelek között, távozáskor kívül várja-e másik személy, stb.,
- amennyiben a megfigyelt személy viselkedése egyértelműen gyanús, feltűnés nélkül értesíteni kell a rendőrséget, és a Bankbiztonságot,
- ha a megfigyelt személy észleli az alkalmazottak reá irányuló figyelmét, és ennek hatására elhagyja a bankot, a rendőrséget és a Bankbiztonságot utólag kell értesíteni a pontos személyleírás megadásával,
- a bankrablás bekövetkezése esetén alapkövetelmény, hogy engedelmeskedni kell az elkövető utasításainak és arra kell törekedni, hogy az ügyfelek és az alkalmazottak életének, testi épségének közvetlen veszélyeztetésére ne kerüljön sor,
- a bankrablás észlelése esetén azonnal működésbe kell hozni a támadásjelző kapcsolókat. Ez minden alkalmazottnak kötelezettsége, hiszen a pénztáros és a támadó látószögében lévő dolgozók ezt nem tehetik meg. Amíg a támadó a bankhelyiségben tartózkodik csak csendes riasztást szabad végezni.
- Fegyveres fenyegetettség esetén is csak annyi pénzt kell átadni amennyi az elkövető által is látható, csak azokat a pénztárolókat kell kinyitni, amelyeket az elkövető követel (megfigyelései alapján tudja, hogy a jelenlévőknél van a kulcs). Az elkövető által is érzékelhető szándékos időhúzás kockázatát nem szabad vállalni. Az ún. „csali pénzt” az elsők között kell átadni a rablónak.
- Amennyiben az elkövető valamelyik alkalmazottat túszul ejti, tiltakozás nélkül engedelmeskedni kell a támadó utasításainak még akkor is, ha az látható erőfölénye ellenére képesnek érzi magát az ellenállásra.
- Amennyiben az ügyfelet ejtik túszul, akkor az alkalmazottaknak maximális együttműködési készséget kell tanúsítani az értékek átadását illetően. A támadó látószögén kívül eső munkatársak sem kezdeményezhetik az elkövető harcképtelenné tételét, nem kockáztathatják a túsz életét (az ügyfelek között segítője is lehet a támadónak). Legfontosabb az elkövető megfigyelése, a minél pontosabb személyleírás megadása érdekében:
  - az elkövető testmagassága, ruházata, álarc, szeme színe, látható jellegzetessége (pl. orr, fejforma),

- az elkövető járása, kiejtése (mit mondott?),
- milyen fegyver vagy más eszköz volt nála, milyen csomagolásban vitte el a pénzt,
- távozáskor az ügyfelek közül elment-e valaki vele együtt,
- az elkövető távozását követően az ügyfelek hogyan viselkedtek.

Az elkövető távozása után:

- azonnal be kell zárni a kijáratot,
- a jelzések ellenére telefonon is azonnal jelenteni kell a rendőrségnek az eseményt és működésbe hozni a kültéri hangos riasztást,
- az ügyfeleket - saját biztonságuk érdekében - vissza kell tartani a rendőrség kiérkezéséig,
- szükség esetén gondoskodni kell a sérült, vagy rosszullét miatt segítséget igénylő személyek ellátásáról (orvos, mentő kihívása),
- gondoskodni kell a helyszín biztosításáról (lezárni a területet, hogy a nyomok sértetlenek maradjanak),
- azonosító kártya kitöltése külön-külön, személyenként.

Robbantással való fenyegetés (bombariadó) **[34]**

A robbantással való fenyegetés (bombariadó) lehetséges céljai, potenciális hatásai a következők lehetnek:

- elterelni a figyelmet egy másik bűncselekményről,
- szabotázs,
- károkozás, pusztítás, terror,
- kiürítés közbeni sérülések előidézése.

A bombafenyegetés elkövetési módjai:

- telefonon,
- postai úton (levél, csomag),
- ajándékozás alkalmával,
- elrejtés, otthagyás révén.

Az előzőek közül telefonon történő bombafenyegetés esetén minden bombajelentést, vagy fenyegetést ki kell vizsgálni, valósnak kell venni mindaddig, amíg a vizsgálat be nem bizonyította, hogy a fenyegetés hamis volt. A telefonkezelők magatartására vonatkozó ajánlások bombafenyegetés esetén:

- őrizze meg nyugalmát,

- a lehetőségekhez mérten rögzítse a fenyegetést,
- szerezzen meg két lényeges adatot: a bomba helyét és a robbanás idejét,
- bátorítsa a hívót beszélgetésre,
- a Bombafenyegetési Nyomtatványt töltse ki.

Az intézkedő vezető feladata a rendőrség értesítése a 112-es telefonszámon. Az intézmény teljes, vagy részleges kiürítését csak az igazgató, a rendőri tűzszerész, vagy a tűzoltósági egység parancsnoka rendelheti el (válságstáb).

Kiürítésre kell rendelkezni, ha

- a rendelkezésre álló információk alapján egyértelműen megállapítható, hogy konkrét életveszély, vagy közeli robbanás bekövetkezése áll fenn,
- a bejelentés ellenőrizhető, konkrét adatokat tartalmazó, létező feltételekhez kötődik, a bűncselekmény tárgyi eszközei fellelhetők, elkövetői azonosítható személyek.

Kiürítésre lehet intézkedni, ha a fenyegetéssel kapcsolatban szerzett ismeretek mérlegelése valós veszélyt és a veszélyhelyzet létrejöttét támasztja alá, mely tragédia, súlyos sérülés bekövetkezését jelentheti.

A bombariadó levezetésének biztonsági intézkedései:

- alternatív biztonsági eljárások,
- azonnali teljes kiürítés,
- azonnali, részleges kiürítés,
- munkahelyek átkutatása a személyzet által,
- biztonsági személyzet kutatása,
- rendőrségi specialisták bevetése.

Kiürítési módszerek és utasítások:

- nyugodt és fegyelmezett módon minden személynek a fő-, vagy tűzkijáraton keresztül kell eltávoznia;
- utasítani kell a személyzetet, hogy vigye magával a személyes holmiját;
- a személyeknek előre meghatározott helyen kell gyülekezni;
- kiürítés után a biztonsági szolgálatnak ki kell kapcsolni minden elektromos fogyasztót;
- minden ablakot és ajtót ki kell nyittatni;
- a kiürített épület őrzését biztosítani kell (senki ne tudjon visszamenni).

Eljárás csomagbombák esetén:

A következő szempontokra célszerű odafigyelni:

- a küldemény címzése, mérete,
- olajos folt, vagy átlyukadás a borítékon,
- marcipán illat, vagy más, az általánostól eltérő szag,
- a boríték ragasztószalaggal történő leragasztása, illetve körülkötése,
- a címzett és a feladó általánostól eltérő megjelölése (a címzett gondos megjelölése nyomtatott betűkkel, a feladó cím nélkül, vagy olvashatatlanul),
- a borítékon megjegyzés, illetve megjelölés: „Csak sajátkezű felbontásra!”.

A levélben elhelyezett „ajándéktárgy” érzékelésének módjai:

- tapintással (hengeres tárgy, amely gyutacshoz hasonlít),
- rázással (fémtárgy gyenge hangja, amely üres hengerben van elhelyezve).

Amennyiben valamely levélnél, vagy csomagnál az előbb felsorolt kritériumok észlelhetők, a Bankbiztonságot illetve a rendőrséget kell értesíteni

Különféle cikkek fejezhetnek ki megbecsülést, de egyben a veszélyeztetett személyekre veszélyt is. Ezeket a tárgyakat ugyanis különféle robbanóeszközökkel fel lehet szerelni anélkül, hogy annak jellegét megváltoztatnák. A védett személyekre ezek a legveszélyesebbek, mivel a tárgyakat - általában - személyesen nekik adják át (pl. alkoholos üvegek használata álcázás céljából: 0,7 l, 1,5 l, 3 l-es boros, likőrös, gyári záras palackok folyékony robbanóanyaggal töltve, zenélő üdvözlőlapok, cigaretta, jegyzetfüzet, jegyzettömb stb.).

Végül pedig az elrejtéses, otthagyásos bombafenyegetés jellemzői és módjai:

- Jól képzett elkövető, gondos előkészítés után hajtja végre a cselekményt (előzetesen beépítheti a robbanóanyagot, illetve ún. átitatási módszert alkalmaz - takarítás, festés).
- Kis szakértelem, idő vagy lehetőség híján ún. becsúsztatásos módszer.

Megelőzése a veszélyeztetett objektum biztonsági őrzésével és rendszeres időnként történő átvizsgálásával biztosítható. [35]

2.3.5. A pénzintézetek informatikai biztonságának néhány aspektusa [36]

A pénzintézetek sikeres üzletmenete, jó hírneve alapvetően függ attól, hogy szolgáltatásaikat megbízhatóan, folyamatosan, zavartalanul és - nem utolsó sorban - biztonságos módon legyenek képesek nyújtani. Ennek a stabil állapotnak a fenntartása a pénzintézetek alapvető üzleti érdeke, kritikus sikertényezője, ezért a szakterület biztonsági kérdéseinek különös jelentőséget tulajdonítanak, azt kiemelten kezelik.

A pénzintézetek szolgáltatásainak döntő többsége már nagyon régen igényel valamilyen szintű számítógépes támogatást. Ezen informatikai rendszerek biztonsági követelményeiről rendelkezik a számítógépközpontok tűzvédelmére vonatkozó MSZ 02102 műszaki irányelv. Előkészületben van egy PSZÁF ajánlás az elektronikus banki szolgáltatások biztonsági követelményeiről, amely alapvetően nemzetközi szabványokon, ajánlásokon alapul.

Bár az elmúlt néhány évben - elsősorban nyugat-európai - információbiztonságot érintő szabvány, ellenőrzési és biztonságirányítási módszertan ajánlásként történő megfogalmazásával (pl. BS 7799, ISO 13335, COBIT) magyar szabvánnyá adaptálásával (MSZ ISO 17799, MSZ ISO 25001) sokat javult a helyzet, mégis még mindig elmondható, hogy a magyar jogszabályi környezet a gyakorló szakemberek számára rendkívül kevés támpontot nyújt az informatikai rendszerek információvédelmi feladatait illetően.

A fentiek mellett van néhány speciális körülmény, amelyet a pénzintézetek informatikai rendszerei biztonságának tervezésekor, fejlesztésekor és üzemeltetésekor feltétlenül figyelembe kell venni.

Ma a pénzintézetek funkcióinak fenntartása, szolgáltatásaik függése saját informatikai rendszereiktől olyan mértékű, hogy ezen informatikai rendszerek jelentős része nélkül nem lennének képesek alapvető szolgáltatásaikat nyújtani. Az elektronikus elszámoló, átutalási, pénzügyi tranzakciókat támogató üzenetkezelő valamint bankkártya-rendszerek (pl. GIRO, SWIFT, VISA, EC/MC, VIBER, stb.) mellett a banki szolgáltatások közül egyre többnek jelenik meg telekommunikációs hálózatokon keresztül informatikai eszközökkel igénybe vehető változata. Ezen funkciók jelentős része csak nagyon rövid ideig, vagy egyáltalán nem pótolható más eszközökkel, illetve e rendszerek kiesése az érintett banki szolgáltatást vagy belső folyamatot ellehetetleníti. A banki szolgáltatások egyre nagyobb és folyamatosan bővülő köre 24/24 órás típusú, tehát folyamatos rendelkezésre állási igényt támaszt - rendkívül rövid kiesési idő toleranciával.

Az e-business, e-commerce, e-banking, e-bróker, e-paymant, stb. csoportokba sorolható szolgáltatások (beleértve a mobil telefonokhoz köthető szolgáltatásokat is) a banki informatikai rendszerek nyíltságát és ezzel földrajzi helytől független támadhatóságának lehetőségét és veszélyét tovább fokozza. [37]

A pénzintézetek működése során keletkezett, feldolgozott adatok szinte kivétel nélkül jogszabályok által titokvédelmi szempontból is védeni rendelt adatok. Valamennyi védendő titokfajta, így a bank-, pénztár-, értékpapír-, üzleti titok, vagy személyes adatnak minősülő információ is előfordul a pénzintézetek adatkezelése kapcsán. Mivel a pénzintézetek a fenti információk döntő többségét informatikai eszközökön tárolja, kezeli, ezeknek a rendszereknek a bizalmassága, hitelessége, sértetlenségének védelme különösen fontos feladat.

A pénzintézetek szolgáltatásainak csalárd felhasználása a bank, illetve ügyfeleinek megkárosításával a fehérgalléros bűnözés egyik jelentős területe. E támadások közvetett, illetve akár közvetlen eszköze is lehet az informatikai rendszer. Megszervezéséhez, illetve kivitelezéséhez - a várható haszon nagyságának megfelelően adott esetben - igen jelentős anyagi és technikai erőforrásokat, illetve szakértelmet alkalmazhatnak a támadók. Ezek kivédése, illetve megelőzése kapcsán mindig professzionális felkészültségű [38] támadókat kell feltételezni.[9]

Az informatikai rendszerek által tárolt adatok, a rendszer működésére vonatkozó információk valamilyen szinten szükségszerűen hozzáférhetők a banki alkalmazottak számára, így a belső közreműködéssel megvalósított, vagy tisztán belső támadások kockázata sem elhanyagolható.

A következőkben áttekintek néhány olyan területet, amely különösen nagy jelentőséggel bírnak a pénzintézetek informatikai rendszerei biztonságát illetően.

Az informatikai rendszerek rendelkezésre állása **[39]**

Annak az állapotnak a fenntartása, hogy egy bank informatikai rendszere a szükséges időszakokban korlátozások nélkül rendelkezésre áll, számos feltétel együttes biztosítását jelenti.

[9] Ugyanakkor nagy biztonsági deficitet eredményez, és ebből kifolyólag az egyik legsérülékenyebb területet a humánoldal, illetőleg a social engineering támadások jelentik.
(Dr. Kovács László - Dr. Krasznay Csaba: Digitális Mohács - kibertámadási forgatókönyv Magyarország ellen, http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csabadigitalis_mohacs_.pdf, letöltés: 2013. december 10.)

Ezen feltételek első csoportja az informatikai rendszer egyes elemeinek, ezen belül is kiemelten központi géptermeinek, kommunikációs központjainak megfelelő fizikai védelme. Itt fontos szerepe van a helyiségek telepítési környezetének kiválasztása. [40]

Különös figyelmet kell fordítani e géptermek fizikai behatolás-védelmére és beléptetés ellenőrzésére. Géptermeket, az informatikai rendszer kritikus elemeit befogadó helyiségeket mindig regisztrálást is végző, valamely fizikai eszköz (pl. proximity, smart kártya) birtoklását és használatát megkövetelő beléptető rendszer óvja. Szigorúan védendő helyiségek esetében a biometrikus azonosítás, illetve a bizottsági típusú - legalább két személy együttes jelenlétét – megkövetelő megoldásokat is mérlegelni kell. A térfelügyelet fontos eleme ezen informatikai területeken a zártláncú videó megfigyelő rendszerek alkalmazása.

A pénzintézeti géptermek fontosságuknak megfelelően kiemelt tűzvédelmi megoldásokat igényelnek. Célszerű a nagy értékű és kritikus informatikai eszközök belső terét aspirációs elven működő tűzjelző rendszerrel, sőt helyi, automatikus, rendszerint gázalapú automatikus tűzoltórendszerrel is védeni. Az automatikus tűzoltórendszerek telepítése ezen géptermek tekintetében mindenképpen kockázatarányos megoldásnak tekintendő. Az automatikus oltórendszerek telepítésekor különös figyelmet kell fordítani ezeknek a rendszereknek a vezérlésére, amelyet össze kell hangolni a klimatizálást és szünetmentes áramellátást (UPS - Uninterruptible Power Supply) biztosító épületgépészeti rendszerekkel és a beléptető rendszer zárvezérléseivel.

A légkondicionált, pormentes környezet ma már természetes követelmény a pénzintézeteknél alacsonyabb rendelkezésre állási elvárást támasztó számítógéptermek esetében is. A légkondicionálás természetesen nem csak a stabil hőmérséklettartást jelenti, hanem a levegő páratartalmának megfelelő szintjét is, amely fontos szerepet kap a számítógépek antisztatikus védelmében.

A pénzintézetek által napjainkban létesített számítógéptermek döntő többségnek biztonságát sugárzott és vezetett zavarvédelmi megoldásokkal is fokozzák. Ezek a műszaki-technikai megoldások azt hivatottak biztosítani, hogy az ilyen módon védett terekben elhelyezett központi számítógépeket ne érhessék az elektromos hálózat, az adathálózat oldaláról, illetve elektromágneses sugárzás révén olyan hatások (hálózati zavarokból, villámcsapás első, és másodlagos hatásaiból, rádiófrekvenciás jelforrásokból származó

túlfeszültség, vagy túláram), amely működésüket zavarná, a berendezéseket károsíthatná.

A számítógéptermek befogadó környezetének függvényében szükség lehet - a központi számítógépek megbízható működésének biztosítása érdekében - speciális rezgéscsillapító megoldások alkalmazására is.

A legalapvetőbb fizikai védelmi megoldás a központi géptermek számítógépeinek folyamatos és megbízható áramellátása. E területen a független kettős betáplálás mellett a pénzintézetek szünetmentes tápegységekkel biztosítják az üzleti szempontból kritikus informatikai rendszereik működését - egy esetleges áramkimaradás esetére. A pénzintézeti rendszerek döntő többségénél a folyamatos üzem fenntartását kell biztosítani, tehát a szünetmentes tápegységek áthidalási időit akár több órás áramkimaradásra kell méretezni. Tovább nehezíti a helyzetet, hogy ezeknek a rendszereknek az áramkimaradáskor táplálni kell az adathálózati aktív hálózati elemeket ugyanúgy, mint a nagyteljesítményű klímaberendezéseket és a biztonsági rendszer elemeit is. Emellett gondoskodni kell a szünetmentes áramellátást biztosító rendszer tartalék háttérrendszeréről is.

Hibatűrő hardware eszközök és megoldások alkalmazása **[41]**

Tekintettel arra, hogy a pénzintézeti informatikai rendszerek kritikus helyreállítási ideje (CRT – Critical Recovery Time) rendszerint nagyon rövid, ezért olyan megoldásokat kell választani, ahol a rendszerkiesés valószínűsége rendkívül alacsony legyen.

A pénzintézetek informatikai rendszereik megbízhatóságának növelése érdekében nagy teljesítményű, korszerű, nagy megbízhatóságú, hibatűrő informatikai és biztonsági rendszerelemekből építkeznek, melyeket szigorú fejlesztési és üzemeltetési rend mellett alkalmaznak.

Hibatűrő processzorarchitektúrák és memóriamodulok választása mellett, ugyanilyen tulajdonságú redundáns háttértármegoldásokat választanak. [42] Ilyen például a különböző tükrözött és más logikai elvek alapján redundáns disk-alrendszerek (pl. RAID diszktömbök) alkalmazása, ahol a redundáns eszközök fizikailag akár több km távolságban is lehetnek. A nagysebességű adatátviteli kapcsolatok lehetővé teszik intelligens háttértárrendszerek fizikailag nagytávolságú logikai összeszervezését (SAN - Storage Area Network) és központi felügyeletét.

Központi gépek fürtözése (cluster architektúra) széles körben elterjedt megoldás. A ma korszerűnek és megbízhatónak tekinthető operációs rendszerek - ha némiképp eltérő módon is -, de mindegyike kínál ilyen típusú megoldást.

Gyakori biztonsági megoldás, amikor komplett IT rendszerek, számítógépközpontok és a kiszolgáló infrastruktúrák valamilyen szintű duplikálásával oldják meg a pénzintézetek (cold-warm-hot site) a megfelelő rendelkezésre állási paraméterek biztosítását.

A fenti megoldások mellett feltétlenül meg kell említeni azokat a rendszer-felügyeleti eszközöket, megvalósításokat, amelyek proaktív módon az esetleges kritikus rendszerhibák előrejelzésére alkalmasak.

***Az üzletmenet-folytonosság biztosítása* [43]**

A magas rendelkezésre állási követelmények biztosítása magas színvonalon kialakított, szervezett üzemeltetés-biztonsági, tervezési, működtetési eljárásrendet és szabályozási környezetet feltételez (és egyúttal követel meg). Ennek a követelménynek való megfelelés a BCP, illetve DRP elkészítésével kezdődik, majd ezeknek a terveknek a tesztelésével, karbantartásával folytatódik, illetve válik folyamatos feladattá.

Megbízható azonosítás, hitelesítés, bizalmasság

A megbízható azonosítás, illetve ehhez kapcsolódóan a hitelesség kérdése kulcsfontosságú egy hagyományos banki tranzakció elvégzésekor (pl. pénztári kifizetés - természetes személy azonosítása) ugyanúgy, mint valamely elektronikus banki művelet végrehajtásakor (amikor az azonosítás kizárólag elektronikus úton történhet). A megbízható azonosításnak, hitelesítésnek, illetve bizalmasság megőrzésének kiemelt szerepe van a bankkártya-műveletek, elektronikus számlavezetési, átutalási rendszerek, az „e” és „mobil” műveletek (e-business, e-commerce, e-banking, e-bróker, e-payment) működtetése és alkalmazása esetén - függetlenül a megvalósítás módjától (pl. kapcsolt vonal, browser-es technológia, WAP, stb.).

Az elektronikusan kommunikáló felek (pl. ügyfél és bank egy elektronikus számlaművelet esetén) kölcsönös és megbízható azonosítása mellett ugyanilyen fontos, hogy kommunikációjuk bizalmassága kapcsolatuk (adatátvitel) során ne sérülhessen és mindkét fél biztos lehessen abban, hogy a másik valóban azt az üzenetet, rendelkezést adta, amelyet partnere küldött, egyszerűbben fogalmazva: a kommunikáció során az adatok nem változhatnak meg úgy, hogy arról a kapcsolatot tartó felek ne értesüljenek.

A megbízható azonosítás, hitelesítés, illetve bizalmasság biztosítása nem valósítható meg csak konzisztens, egymásra épülő, szakszerűen menedzselt kriptográfiai környezetben.

Magyarországon az elektronikus aláírásról szóló törvény elfogadásával megteremtődött annak a jogi lehetősége is, hogy egyre több pénzügyi és jogi tranzakció kerülhessen elektronikus módon lebonyolításra. Erre alapozva a pénzintézetek belátható időn belül megteremtik saját PKI (Privat Key Infrastructure) rendszerüket, amely rendkívül tág teret nyit a biztonságos elektronikus pénzintézeti tevékenységeknek.

A pénzintézeti informatikai rendszerek határvédelme **[44]**

A mai pénzintézetek szolgáltatásaikat kiterjedt informatikai hálózatok segítségével nyújtják. Ezen hálózatok alapvetően két részre oszthatók. Az első rész az adott pénzintézet belső védett hálózata, amely felett az adott pénzintézet informatikai apparátusa - normális esetben - teljes kontrollt gyakorol. A hálózat másik része azon külső - ún. nem védett - hálózati rendszerek, hálózati elemek, eszközök, amelyekkel a belső hálózat - megfelelő szabályrendszernek megfelelően - kapcsolatot tart. A külső hálózat működésére, biztonsági tulajdonságaira a pénzintézetnek gyakorlatilag alig van hatása. Ilyen nem védett hálózati kapcsolat például egy bérelt adatátviteli vonal, vagy maga az Internet.

A két - védett és nem védett - hálózat találkozási pontjait, határát védik az ún. határvédelmi eszközök tekintettel arra, hogy a nem védett hálózat felől számtalan támadás fenyegeti a belső védett hálózatot. Ezek lehetnek vírustámadások, egyes banki szolgáltatások, vagy informatikai rendszerszolgáltatás (pl. WEB server) megbénítására vagy manipulálására irányuló kísérletek, csalárd banki tranzakció-kezdeményezések, stb.

A határvédelmi eszközök közé sorolhatjuk a tűzfalrendszereket, az idegen behatolást detektáló eszközöket, a vírusvédelmi megoldásokat, a levelező rendszereket védő tartalom, levélszemét (SPAM) és kémprogram szűrőket, az ezekhez a rendszerekhez kapcsolódó naplófájl-elemző eszközöket. A pénzintézetek ezeket - tekintettel szoros logikai kapcsolataikra - kombináltan alkalmazzák belső hálózatuk (és így szolgáltatásaik) védelme érdekében.

Az informatikai rendszer biztonsági menedzsmentje **[45]**

A pénzintézetek informatikai rendszereik biztonsági menedzsmentjének központosítására egységes, áttekinthető, számítástechnikai eszközökkel történő támogatására, illetve e

rendszer lehető legnagyobb mértékű automatizálására és az emberi tényező lehetőség szerinti kiiktatására törekszenek.

Lényeges, hogy egy pénzintézeti informatikai rendszer felhasználói adminisztrációs oldala legyen képes a felhasználói hozzáférési jogosultságokat illetően gyors, egyértelmű és áttekinthető információk szolgáltatására és szükség esetén tegye lehetővé a kritikussá vált hozzáférési lehetőség teljes rendszerre vonatkozó megszüntetését.

A pénzintézetek informatikai rendszereit és belső, védett hálózatát illetően sohasem kizárhatóak a belső, alkalmazotti hűtlenségre visszavezethető rosszindulatú cselekmények. Ez utóbbiak kezelésének fontos eszköze és területe az informatikai rendszer megfelelő hozzáférés-kontrollja és a jogosultság adminisztrációja, amelynek a banki üzleti folyamatok összefüggésein alapuló jogosultsági mátrixon kell alapulnia.

2.4. A 2. fejezet összefoglalása

Történeti áttekintését adtam a magyarországi pénzintézeti, és konkrétan a pénzintézeti biztonság fogalmának.

Kifejtettem a technikai eszköz-innovációs folyamat kontraindukált elemeként tapasztalható hatásláncot, amelyben a mechanikus eszközök fejlődésével, a behatolás-jelző rendszerek specializációja eredményezte a következő problémakört: a szabotázs elleni védelem létrehozásának feladatát. Ugyanilyen hatást produkált a profi biztonsági rendszerek civil környezetben történő tömeges alkalmazása. Ebben a vonatkozásban például a behatolás-jelzés terén a nagyszámú helyi riasztók alkalmazása érdektelenséget, sokszor dühöt és ellenállást váltott ki a környezetből, amely éppen ellenkező előjelű a kívánt hatást tekintve. Ennek eredményeképp, illetve az elkövetők elfogásának nagyobb valószínűsége érdekében került alkalmazásra a védett objektumokban a néma riasztás, az élőerő azonnali indításával egybekötve.

Az eszközspecializációval korrelációban fejlődött a felügyeleti tevékenység, a rögzítési technika szükségessége, és váltak szét az egyes szakterületek technikai lehetőségei - minden esetben az igényekhez igazodva.

A fejezetben egyértelműen bizonyítottam, hogy a terület folyamatos változáson, specifikáción megy keresztül, amelyben minden védelmi eszköz alkalmazásának szabályozási rendszere is több szinten kialakult. Ezen szabályzatok jog-, és eseménykövetően változnak.

Elemeztem a magyarországi pénzintézetek működési biztonságának szignifikáns jellemzőit, felvázoltam a folyamatos átalakulás elemeit a védekezés módszerei és eszközei tekintetében. Kiemeltem a magyarországi sajátosságok közül a speciálisan, bűncselekmény-specifikus prevenciós megoldások alkalmazásának gyakorlatát, amely az új, erőszakos jellegű deliktumok megjelenésével biztonságtechnikailag egyértelműen kiegészítésre szorul. Kiemeltem e tekintetben a kódolt pénzszállító eszközök, multisafe-rendszer, internet-bankolás, ügyféltér biztonsági elemeinek szerepét.

Megállapítottam, hogy a jelen bankbiztonsági szabályzók nem egységesek, ez pedig a biztonsági tevékenység színvonalának nem kedvez. A magánbiztonság egyes alapvető kérdései egységes szabályozási elvek, törvények, törvénymódosítások kialakítására várnak.

A bankokra, pénzintézetekre kritikus infrastruktúraként kell tekinteni, amely értelemben a globális kihívások, veszélyek érintettjei, és amelyekre való felkészülés, illetve a biztonságtechnikai válasz(ok) adása kötelező.

Elemeztem a pénzintézetek kárára elkövetett jellemző bűncselekményeket és elkövetési módokat. Mindezek alapján meghatároztam a fő biztonságpolitikai célterületeket, amelyek: a pénzintézetek technikai védelme, benne az eszköz-innovációs elemek és emellett az élőerős őrzés előírásai, feladatai.

A működési biztonság megteremtésének alapelemeként határoztam meg a pénzintézeti belső vizsgálati tevékenységet is. Kiemeltem ezek közül a rendkívüli eseményeket kezelő szabályzási rendszer kialakításának fontosságát.

Ugyancsak lényeges területként tekintettem a pénzintézetek informatikai biztonságának megteremtésére, mivel a pénzintézetek sikeres üzletmenete, jó hírneve alapvetően függ attól, hogy szolgáltatásaikat megbízhatóan, folyamatosan, zavartalanul, vagyis a legbiztonságosabb módon legyenek képesek nyújtani.

3. A PÉNZINTÉZETI BIZTONSÁGI PARADIGMAVÁLTÁS LEHETSÉGES IRÁNYAI[1]

A múlt és a jelen pénzintézeti biztonságának fejlődési sebességét döntően a bűncselekmény-elkövetések elemzéséből levont következtetések vezérlik. [1] Érzékelhető, hogy az alkalmazott eszközpark technikailag még fejleszthető, finomítható, de igazi áttörést csak a paradigmaváltás okozhat.

A lehetséges új irányok megfogalmazásához, a felmerülő kérdések megválaszolásához feltétlenül érdemes széleskörű és tudományos igényű analízist végezni. A vizsgálatok egy részének az elkövetői magatartási minták értékelésével kell foglalkoznia, a másik irány az aktív beavatkozás eszközeinek és módszereinek keresése felé mutat.

A kutatás eredményei a védekezés új korszakát jelenthetik, ami nem más, mint a pénzintézeti biztonság paradigmaváltása.

A rablás elkövetőivel szemben alkalmazható új, humán természetű megoldások a következők (lehetnek):[2]

- a nyilvánosság szélesebb körű bevonása a felderítésbe (több esetben a lakosság bevonása lényegesen segítette a felderítések eredményességét);
- a törvények erős szigorítása az elkövetőkkel szemben (az ún. „Három csapás" törvény), ezzel párhuzamosana büntetés-végrehajtás szigorítása az elkövetőkkel szemben (fegyházbüntetés alkalmazása);
- a fentiek részletes kommunikálása a médiákban - valós eseteken keresztül (az elkövetett cselekmény, az érte járó büntetés, a bűnhődés és a megbánás kapjon széles médianyilvánosságot - elrettentésként);

[1] A kérdéssel intenzíven és folyamatosan foglalkoznak az érintett szakmai fórumok is, ahol a biztonságtechnika innovációinak figyelembevételével állandó a szakértői irányváltozás (MABISZ Biztonságtechnikai útmutató a betöréses lopás-rablásbiztosítási kockázatok kezelésére, 2007., ajánlás. A 6. fejezet: Behatolás-jelző rendszerek tervezése - Pénzintézetek (hatályon kívül) 2016. február 29-ig hatályos a http://www.mabisz.hu/images/stories/docs/biztonsagtechnika/mabisz-kockazatvallalasi-ertekhatarok.pdf, letöltve: 2015. november 17.

[2] A rablással, mint kiemelt bűncselekményi kategóriával a rendőrség bűnügyi szakterülete folyamatosan foglalkozik. Az aktuális időszakban elkövetett deliktumok speciális szempontú elemzésével, értékelésével folyamatos a törekvés a tapasztalatok későbbi felderítést segítő megfogalmazására. (Módszertani útmutató a Robotzsaru központi rendszerben: Egyes vagyon elleni bűncselekmények felderítése - ügytől a személyig modell, valamint az ún. személytől az ügyig modell.)

- kiváló minőségű, nagyszámú felderítő és dokumentáló eszköz szakszerű alkalmazása az elkövetés helyszínén (technikai fejlesztés, ami kihat az elrettentésre is);
- időzárak alkalmazása valamennyi lehetséges helyen (csak „kis összeg" elvitelét teszi lehetővé - ugyanakkora büntetési tétel mellett: vagyis „nem éri meg");
- tájékoztató tábla a bejáratnál, amely a folyamatos képrögzítésről, és az időzárak alkalmazásáról is tájékoztatja a belépőket (a kockázat aránytalanságát demonstrálja, elrettentés);
- az intézkedési rend demonstrálása (a belső fegyelem, szakértelem jelzése).

A paradigmaváltás irányába mutat a jelenleg rendelkezésre álló, új fejlesztésű technikai eszközpark széleskörű bevonása a banki biztonsági alkalmazásába. [2] Ebben a vonatkozásban - megítélésem szerint - a következő új feladatok megjelenésére lehet számítani már a közeli jövőben:

- az érzékelés határainak kiterjesztése (távolság, megvilágítás, biometriai elemek, stb.); [3]
- az érzékenység, kimutatási sebesség növelése;
- újabb mérhető paraméterek megjelenése (fizikai, kémiai, biológiai);
- intelligens értékelő, elemző szoftverek fejlesztése (élettelen és élő környezeti paraméterek változásainak elemző feldolgozása);
- a biometrikus detektálás legújabb eredményeinek alkalmazása (arcrészlet-, alak-, mozgás alapján történő azonosítás, testhőtérkép-változás analízis, stb.); [4]
- a felderítés, elhárítás, beavatkozás eszközeinek fejlesztése és bevezetése (THz-es tartományban működő felderítő eszközök, infraérzékelők, folyadékkristályos biztonsági üvegek, robbanó patron, felcsapódó áthallás és átlövésálló elem, ködgenerátor, stb. alkalmazása).

Mindezeken túlmenően az élőerős védelem vonatkozásában az őrszolgálat szervezése is átalakításra vár, mivel jelenlegi formájában nem kellően hatékony a bankrablások elhárításában. Ez elsősorban annak köszönhető, hogy jogszabályi előírások és egyéb szabályozók ismeretében a felállításuk, szabályzat szerinti magatartásuk kifigyelhető, kiszámítható és ennek következtében támadáskor kiiktatható. Az őrök elhelyezése, mozgatása, és alkalmazása tekintetében több alternatíva is felvetődött (az őrök bevonása a banki belső területre, több objektum egyszerre történő őrzése, gépjárműves, rendszertelenül

mozgó csapat, stb.), de ezeknek a módszereknek a valós értéke - egyelőre - még nem látható (nem keletkezett szignifikánsan számításba vehető adatmennyiség).

3.1. A paradigmaváltás kezdetének [5] lehetősége 2010-től[3]

Az európai regresszió hatására - a gazdasági folyamatok átstrukturálódása mellett - felgyorsultak a nem kívánt bűncselekményi folyamatok is. A bűnözési intelligencia, a bűncselekmények elkövetések erőszakszintje és a végrehajtások gyakoriságának száma látványosan emelkedett[4]. A védekezés jelenlegi technikai színvonala - a fejlettsége ellenére - nem alkalmas ezek teljes mértékű visszaszorítására. Szükséges tehát a védelmi koncepció terén is paradigmaváltást végrehajtani.

A jelenlegi elképzelések döntően a hozzáférés-korlátozás és a dokumentálás modern eszközrendszerének széleskörű, integrált alkalmazására alapoz, amelynek kialakítási bázisa a törvényesség és a nagyfokú személybiztonság. A gondolati váltás e tekintetben a bűncselekmény folyamatába történő beavatkozás nagy biztonságú eszközeinek kifejlesztési igényében és azok alkalmazásba vitelében mutatkozik meg.

3.1.1. A biztonságtechnikában alkalmazott eszközök paradigmaváltása

A jelenleg rendelkezésre álló, ismert fizikai beavatkozó eszközök (amelyeket már alkalmaztak banki környezetben) a következők:

- robbanó festékpatronos eszközök (pl. csapdapénz, robbanó táska, ATM alkalmazások), amelyek az elvett pénzt és az elkövetőt megfestve a rablás „eredményét" teszik tönkre, illetve az elkövető személyének felderítését könnyítik meg. A festék anyaga szerves alapú, nem közömbösíthető, nem kimosható vegyület;
- felcsapódó záróroló, amely kivitelezésében erős szerkezetű, átlőhetetlen anyagú és a kommunikációt a két oldal között teljes mértékben gátolja. Alkalmazásához a szükséges térgeometriai feltételeket biztosítani szükséges, ami egyben az eljárás alkalmazási korlátait is megszabja (alkalmazása eddig leginkább francia és olasz környezetben történt meg).

A biztonságtechnika eszközrendszerében meg kell jelenni a bűncselekmény folyamatába történő beavatkozást elősegítő, elvégző eszközöknek. Ennek előfeltétele olyan nagy

[3] Ehhez szorosan hozzátartozik a rendvédelmi szervek és a pénzintézetek szemléletváltása is, a közös fellépés preferálása. [6698-16/2011. Az Országos Rendőr-főkapitányság és a Magyar Bankszövetség között kötött együttműködési megállapodás, ORFK Tájékoztató (OT) 2011/4. szám (2011. május 6.)]

[4] Nemzetközi Bankszövetség: Rablások felmérése 2007 és 2012 között, melléklet

megbízhatóságú érzékelő, értékelő készülékek bevezetése, amelyek, az elkövetési szándék előjeleiről csalhatatlan módon, nagy gyorsasággal jelzést képesek leadni.

Az elkövetési szándék jelei (lehetnek):

- az elkövetési előkészület a végrehajtásra (viselkedési forma, illetve annak változása),
- az elkövetésre alkalmas eszköz (pl. fegyver, vagy annak látszó tárgy) rejtett hordozása,
- az elkövetés előkészületére jellemző (vagy ráutaló) biológiai paraméterek megjelenése, megváltozása (testhőmérséklet, szívritmus, vérnyomás).

Az elkövetési szándékra jellemző magatartásforma kimutatására - a digitális videotechnika alkalmazásával - intelligens szoftvereket fejlesztettek és fejlesztenek magyar és külföldi szoftver szakemberek jelen pillanatban is [6] - a banki biztonsági szakemberek bevonásával. Ezek alkalmasak különféle viselkedésminták elkülönítésére és így, a deviáns viselkedés jellemzőit is többnyire képesek kiválasztani. Az eredmények azokon a területeken ígéretesek, ahol a jellemző viselkedésforma jól körülhatárolható módon leírható [7] (pl. repülőtér, de ilyen lehet a bank, vagy a postahivatal is).[5]

Az elkövetésre alkalmas eszköz rejtett hordozásának kimutatási korlátai az érzékelés eszközeinek méretében, megbízhatóságában, vagy az érzékelés sebességében keresendők. Fegyver és/vagy bomba felbukkanása esetén az érzékelendő paraméter lehet a fegyver anyaga, alakja, vagy a robbanószer vegyi összetétele. A fegyverre jellemző alakérzékelés „hagyományos módon” átvilágítással történik (pl.: röntgen, impulzus röntgen, rádióhullámú eszközök, infravörös sugárzók), amely egy adóvevő pár (sugárzó és az elnyelést, visszaverődést felfogó ernyő) működtetésével történik. Méretében, elhelyezésének bonyolultságában, mérési időigényében és a lehetséges egészségi ártalom okozása miatti aggodalom támaszt kétségeket a hétköznapi életben történő esetleges alkalmazásukkor.

Új érzékelési lehetőséget nyújthat az emberi test maga, mint infravörös-sugárforrás (hőkibocsátó anyag). Megvizsgálandó feladat, hogy az elkövetésre alkalmas eszköz (fegyver) rejtett jelenléte kimutatható-e minden esetben ezzel a módszerrel. Ismert,

[5] Rendőri szempontból is folyamatos a terület kiemelt kezelése. A központi bűnmegelőzési egység vezetője módszertani útmutatóban meghatározta az áldozattá válás szempontjából kiemelt kockázatú csoportokat (közöttük kiemelten a pénzintézetek dolgozói) és az áldozattá válásuk megelőzése érdekében végrehajtandó feladatokat. [Módszertani Útmutató A rendőrség bűnmegelőzési tevékenységéről szóló 20/2010 (OT. 10.) ORFK utasítás 36. pontjához]

hogy a gyógyászat területén a módszer kiválóan alkalmazható - kórházi, laboratóriumi körülmények között[6]. A módszer előnye, hogy passzív működési elve okán ez egészségre ártalmas kockázati elemeket nem tartalmaz, a mérési eredmények megjelenése kvázi azonnali (így gyors beavatkozási lehetőséget nyújthat egy banki környezetben: pl. zsilipajtó lezárása).

Ködgenerátorok („füstágyúk")

Új beavatkozási lehetőséget jelenthet a ködgenerátor (egyes helyeken „füstágyú"-nak) nevezett eszköz. Ez indítása után nagy sebességgel és sűrűséggel ködszerű anyagot juttat ki környezetébe - gyakorlatilag láthatatlanná téve a behatoló, rablást megkísérlő számára a célterületet. Magyarországi telepítési helyszínei (ahol üzemszerűen alkalmazásra került): MOL és AGIP üzemanyagtöltő-állomások, ékszerboltok és kisebb üzletek, amelyek az eszköz sikeres üzeméről tanúskodnak (számos feltöltés nézhető meg az Interneten is).

A gyakorlati alkalmazás sikerességét kiválóan mutatja az alábbiakban olvasható példa is.[7]

A dégi, éjszakánként zárva tartó MOL benzinkúton 2007-ben és 2008-ban 8 alkalommal történt betörés, amelynek során zárva tartási időszakban keletkezett kb. 8 mFt lopási és kb. 3 mFt rongálási kár. A helyszín lakott településtől távol van, kis forgalmú területen helyezkedik el, ezért biztonsági szempontból az egyik legkiszolgáltatottabb töltőállomás Magyarországon.

A lopási események néhány perc alatt lezajlottak, a riasztásra a helyszínre érkező járőr már senkit nem talált. Intézkedésként előbb vagyonvédelmi technikai fejlesztések történtek (CCTV, riasztórendszer, mechanikai védelem), majd a zárva tartási időszakra élőerős védelem is biztosításra került.

Azzal a céllal, hogy a rapid betörési akció megakadályozható legyen, a jelzett intézkedésekkel párhuzamosan olyan új vagyonvédelmi technika felkutatása indult meg, amely biztonsági, költséghatékonysági, szabályozási, üzemeltetési, munkabiztonsági, környezetvédelmi és foglalkozás-egészségügyi szempontból is alkalmazható lehet. Ekkor merült fel megoldási lehetőségként a ködgenerátor alkalmazása, ezért annak tesztje mellett döntött a szakértői csapat (amelynek tagja voltam).

---

[6] A Budapesti Műszaki és Gazdaságtudományi Egyetem fejlesztette ki a Szomatoinfra eszközt.
[7] Tartalmi kivonat a MOL biztonsági vezetőjének - számomra megküldött - értékelő leveléből.

Az egy hónapos tesztre az említett üzemanyagtöltő-állomáson került sor, amelynek a végén értékelésre is sor került.

Az első indítási kísérlet egy próbariasztás volt: a ködgenerátor a betörésjelzésre indult.

A jelenlévők megállapították, hogy a rendszer alkalmas a vagyonelleni bűncselekményt lassítani, bizonyos esetekben a tettest a helyszínen tartani a kivonuló szolgálat megérkezéséig (függ a kiérkezés gyorsaságától, az elkövető térbeli tájékozódási képességétől - kvázi „vakon", a vizuális és szonikus kommunikációképesség helyreállási idejétől, stb.). Az eszköz alkalmazásával az elkövető szándéka meghiúsítható, valószínűleg csak rongálási kár keletkezik (a termelt köd 25 s elteltével kezdte el kiszorítani az elkövetőt a védett helyiségrészből).

A berendezés elektromos fogyasztása 1,2 kW működés közben és 60 W készenléti állapotban. Hidegindítás esetén 20-25 perc szükséges a felfűtéséhez. Az eszköz tartálya egy feltöltéssel 6 alkalomra elegendő folyadékot tartalmaz. A vagyonvédelmi rendszerek karbantartásával összhangban évente egyszer karbantartani kell - próbaindítással.

A ködgenerátor („füstágyú") banki alkalmazására még nincs példa, de az említetten túlmenően, más helyszíneken megtapasztalt működése alapján bankrablás esetén az ügyféltér elárasztására mindenképpen alkalmas lehet. Nyilvánvaló ugyanakkor, hogy az alkalmazás fizikai, pszichikai és egészségügyi feltételeit alaposan ki kell vizsgálni - PhD értekezésem egyik kulcselemét jelenti ennek végrehajtása és az eredmények közzé tétele.

A sikeres tesztüzem után a ködgenerátor integrálásra került a helyi riasztó és CCTV kamera rendszerekhez, a jelek bekötésre kerültek a MOL Társasági Biztonság által üzemeltetett Biztonsági Központjába, valamint a távfelügyeleti szolgáltatóhoz.

Alternatív (nem halálos) fegyverek **[8]**

A XXI. század komoly kérdése a demokrácia és az emberi jogok védelme. Minden demokráciában az emberek legelemibb jogaként az élethez és a szabadsághoz való jogot tartják a legfontosabbnak. E gondolat mentén már régebben megkezdték azon eszközök fejlesztését, amelyek hivatottak az élet kioltására alkalmas eszközök kiváltására.

Ez a fejlesztés leginkább a közeli összecsapások lövő eszközeire, kézi fegyvereire hat. Többféle út figyelhető meg ebben a témában: a speciális gázok helyi alkalmazásától a hang és fényhatáson keresztül a sokkhatást kifejtő eszközökig.

Ezek az eszközök élettani hatásmechanizmusuk alapján alkalmasak a támadószándék megtörésére és a menekülés megakadályozására.

A viszonylag magas feszültségszintet alkalmazóeszközök [9] (amelyek áramerőssége alacsony) az alábbi hatások kifejtésére alkalmasak:

- erős fájdalomérzet,
- kontrollmentes izom-összehúzódás,
- egyensúlyvesztés,
- tájékozódó-képesség elvesztése,
- izombénulás,
- agyműködészavar,
- cselekvésképtelenség,
- tudatzavar.

A felsorolt jelenségek kifejezetten átmeneti jellegűek, az alkalmazást követő néhány percig tart csak a hatásuk, egészségkárosodást nem okoznak (ha a kezelési és kiképzési előírásokat az alkalmazó maradéktalanul betartják).

Ezeket az eszközöket testközeli használatra fejlesztették ki és alkalmazták (pl. kézi sokkoló pajzsba, gumibotba, kézilámpába, stb. beszerelt változatai). Napjaink készülékei elektródákat lőnek ki (általában lőporral) a támadó megállítására. Magyarországon az alkalmazás törvényi lehetőségei még nem adottak. [10]

Az egyik leggyakoribb példányból (TASER M26, illetve X26) százezres darabszám van forgalomban a világ több pontján. A harmadik és negyedik generációs készülékeket koncentráltan a tevékenységgátlásra fejlesztették ki, amely a fokozott életvédelem mellett a mozgásszervek irányában az agy vezérlő funkcióját bénítja.

Az M típusú eszközök elsősorban a rendfenntartó erők eszközeiként voltak rendszerben a 2000-es évek elején. Az alkalmazásukból nyert tapasztalatok alapján készítették el az X26 változatot. A teljesítményszükségletet negyedére csökkentették (kb. 7 W), tömege mintegy 60 %-kal lett kevesebb. Fejlesztették a lövés távolságnál döntő szerepet játszó tölteteket. A készülék kontaktmódon is alkalmazható.

Új fejlesztés az AFID (Anti-Felon Identification - Bűncselekmény Elleni Azonosítás) megoldást alkalmazó eszköz: a lövéssel azonos időben a töltény sorszámával feliratozott kis papirkák is kilövődnek. Ezzel a lövés és a lövő személy kiléte eltitkolhatatlanná válik. A beépített videórögzítő használati alkalmat dokumentál.

Az ötödik generációs XREP vezeték nélkül, nagyobb távolságon (20 m) képes megállítani a célszemélyt, hatása 20 s-ig tart. Rendszeresített, 12 mm kaliberű puskából lőhető ki a töltet.

A TASER-ekkel a biztonságtechnikai palettán olyan védelmi beavatkozó eszközök jelentek meg, amelyek közvetlen vagy közvetett módon alkalmas a támadó személy támadási szándékának megtörésére, menekülésének megakadályozására. Kétségkívül a közeli jövő legalkalmasabb védelmi eszköze, amely leválthatja a biztonságvédelemben alkalmazott éles lőfegyvereket.

2009. szeptember 1-én hatályba lépett 32/2009. (VIII.19) IRM rendelet melléklete a Rendőrségnél rendszeresíthető kényszerítő eszközök közé sorolja az elektromos sokkolókat. Ez a módosítás így már a 1997. évi CLIX. törvény alapján a Fegyveres biztonsági őr (FBŐ) állományra is kiterjed (valószínű, hogy ez a folyamat a vagyonőrökre vonatkozó törvény módosítását is magával fogja hozni).

A TASER-ek bevezetése, alkalmazása, teljes gondolkodásmód-változást okozna a banki biztonsági őri feladatrendszer, a személy-, valamint az életvédelem területén.

3.1.2. A banki ügyfél-azonosítás anomáliái, bűnügyi aspektusai és a védekezés paradigmaváltásának lehetőségei

A banki számítástechnikai rendszerek belső hálózatainak nagyfokú biztonsági szintje gyakorlatilag lehetetlenné teszi az illetéktelen hozzáférést (és ezen keresztül pl. a számlafosztogatást).

Az ügyfélszámlák támadhatósága csak a bemeneti pontokon az azonosító adatok meghamisítása [11] (vagy eltulajdonítása) révén valósítható meg.[8] Ennek egy lehetséges elkövetési formája, ha a számlakezelésre jogosult ügyfél szerepét egy olyan valaki veszi át, aki megfelelően hamisított igazoló okmányok birtokában, az ügyfél életviteli ismeretéből, szokásaiból és annak aláírás-mintájából felkészülten, az ügyintézőt félrevezetve jut a számla kezelési jogához. A sikeres akció eredménye az egyszeri gyors lefosztástól a netbanki számlakezelő rendszer fölötti kezelési jog átvételéig terjed.

[8] Ezen gyenge pontok kiiktatása érdekében a bankok saját módszertant dolgoztak ki (pl.: Hirdetmény az OTP Bank Nyrt. ügyfél-azonosítási rendjéről) https://www.otpbank.hu/static/portal/sw/file/Ugyfelazonositas_H_hun_20130809.pdf, letöltve: 2015. október 17.

Pontokba szedhetők az ilyen jellegű bűncselekmények közös lépései, nevezetesen:[9]

- banki belső együttműködő partner beszervezése,
- a megfelelő ügyfél kiválasztásának előszűrése,
- a számlatartalom, számlaforgalom megismerése,
- az ügyfélszokások elsajátítása,
- a hiteles adatokon alapuló fényképcserés igazolványok elkészítése,
- az akcióidőpont megszervezése.

Részleteiben:

Az ügyfélkiválasztás döntően a belső tippadótól indul, aki általában az illetéktelen betekintés módszerével jut a megfelelőnek tartott ügyfél adataihoz, számlaszokásainak ismeretéhez.

Az ügyfél megszemélyesítését szinte mindig a honos fiók kikerülésével valósítják meg az elkövetők. Az ügyfél-azonosítás jelenlegi szabályait alkalmazva a csalót valamelyik igazolványa (és lakcímkártyája) bemutatására, valamint a hitelesen regisztrált, általa alkalmazott aláírás minta szerinti aláírásra kérik fel. Mivel az elkövető nem a honos fiókban jelentkezik, ezért a személyes ismeret veszélye nem fenyegeti, így a fényképcsere (személycsere) csak nehezen derülhet ki. Ha kellően begyakorolta az aláírást, akkor valószínűleg azon sem bukik el. A cég és az ügyfélszokás ismeretének bennfentes jelzése, szintén bizalomfokozó tényező, elősegíti a csalás sikerességét.[10]

A személyazonosítás jelenleg ismert, elfogadott és alkalmazott módszereit már az intelligens bűnözés ki tudja játszani, nagy pontosságú másoló-, hamisító eszközökkel, valamint kifinomult, célirányos adatgyűjtéssel. A személyazonosítási kontrolleszközök halmozott alkalmazása sem hozta meg a kockázat és ár/érték arányos elvárt eredményét (a személyi igazolványellenőrzése, aláírás-minta kérése, személyes kódok ismerete, stb.).

---

[9] Jelentős területét adja ezen bűncselekményeknek az un. sociale ngineering: „Social engineering is the practice of using deception or persuasion to fraudulently obtain goods or information and the term is often used in relation to computer systems or the information they contain."Azaz: A social engineering a csalásnak vagy rábeszélésnek a gyakorlati alkalmazása információ-, vagy ingóságok szerzése érdekében. A kifejezést gyakran használják számítógépes rendszer, vagy annak információ tartalmával kapcsolatban is.

[10] Humán alapú támadástechnikák: Identitáslopás, Álruhába bújás, Céges alkalmazott, Partner cég alkalmazottja, Új munkaerő, Magas pozíciójú ember, Fontos ember, IT szakember, Tombstone theft, Third party authorization, Hamis bizalomkeltés, Reverse social engineering, Valamit valamiért, Jelszavak kitalálása, Alapértelmezett jelszavak, Személyre utaló jelszavak, Rutin munkát végzők segítségkérése, Bejutás az épületbe, Tail gating, Késés, Hamis ID használata, Piggy backing, Shoulder surfing, Dumpster diving, IT alapú támadástechnikák: Előzetes információszerzés, Web lapokról szerzett információk, Google hacking, Közösségi portálok figyelése, Blogok figyelése, Videó megosztó portálok figyelése, Phishing (Adathalászat), Kártékony programok, Frissítés/javítás felajánlása, Csatolmányok, Key logger, Baiting, Trójai programok, Hálózatok figyelése, WiFi, Egyéb IT alapú támadások, Telefonbeszélgetés, Látszólag belső cím, Távoli e-mail.

A szigorításokon alapuló módszerek - mint például az, hogy a személyes, vagy személyhez fűződő adatok változtatásának végrehajtását csak honos fiókban, saját ügyintézőnél lehessen végezni - korlátozzák az ügyfelek által elvárt rugalmas, dinamikus számlakezelési lehetőségeket, ezért nem sikeresek.

Az aláírás ellenőrzés egyelőre nem automatizálható ipari méretekben, csak egyedi esetekben végezhető el - specifikusan felkészített ügyintézők alkalmazásával.

Járható, bár nem olcsó megoldás az igazolványok eredetiségét ellenőrző eszközök beszerzése és alkalmazása fióki szinten. Ezzel kiszűrhetőek az illegálisan gyártott, kiváló minőségű, megtévesztésre alkalmas hamisítványok (ilyen pl. a határellenőrzésnél alkalmazott okmányvizsgáló berendezés).

A számlatulajdonos megtéveszthetetlen azonosítására megoldást jelenthet az erre a célra alkalmassá tett biometrikus eszközök széleskörű bevezetése. Ezek az eszközök a személytelen, távellenőrzésre is alkalmazhatóak lehetnek. A biometrikus azonosítás alapja az egyedi személyes jellemzők mérésén, összehasonlításán alapuló módszerek, eszközök alkalmazása.

A biometrikus azonosító rendszer [12] olyan technikai megoldást kell, hogy alkalmazzon, amely méri és rögzíti (speciális eljárással visszafordíthatatlan módon) egy személy egyedi fizikai, vagy testi jellemzőit. Ezek a személyjellemzésre alkalmas adatok ellenőrzésre és/vagy azonosításra, összehasonlító algoritmus felhasználásával folyamatosan alkalmazhatók[11].

3.1.3. Az élőerős őrzés lehetséges változásai[12]

A bankrablás megakadályozásának jelenleg meghatározó szereplője a biztonsági őr. [13] Tevékenységét és működésének eredményességét vizsgálva összegzésképpen megállapítható: a klasszikus biztonsági őri szerep többnyire nem elégíti ki az elvárt szolgáltatási igényeket. Kiszámítható (ezért több esetben egyszerűen hatástalanítható) tevé-

[11] Ujjnyomatunk - hozzájárulásunkkal - az új típusú (piros) útlevélben letárolásra kerül (más adatokkal és az arcképünkkel együtt). Ezt a határátlépésnél korrelációba hozva az aktuálisan beolvasott ujjnyomatunkkal egyértelmű kapcsolat állapítható meg az úti okmány és annak bemutatója között (1:1 típusú módszer = ellenőrzés). Vízum kérése esetén a biometrikus mintánk egy központi adattárolóba kerül (ahol az összes vízumot kérelmező személy mintája megtalálható). Általában a Bevándorlási Hivatal által, határátlépéskor felvett ujjnyomat(ok) aztán ezzel a teljes adatbázissal kerül(nek) összevetésre (1:N = azonosítás).

[12] Nagy befolyással vannak ezekre a folyamatokra a tevékenységet kísérő minőségi elvárások: Megalakult a Magánbiztonsági szolgáltatások nemzeti szabványosító műszaki bizottsága (http://szakmaikamara.hu/index.php?&pg=hirek&do=read&newsID=415, letöltve: 2015. november 17.)

kenység és fellépés: ezzel a fegyveres támadás többnyire sikeresen végrehajthatóvá válik. Az élőerős őrzés tekintetében is paradigmaváltásra van tehát szükség.[13]

A további megoldásra váró élőerős őrzési probléma a fegyvertípus-váltás. Jelenleg alkalmazott fegyvereink (a törvényben engedélyezett, sorozat lövésre nem alkalmas kézifegyverek, pl. Glock, Parabellum) kategóriájukban megegyeznek a rendőrség által is alkalmazott kézi fegyverekkel: az élet kioltására alkalmasak és nem megfelelő használatuk vétlen személyeknek is súlyos egészségkárosodást, vagy akár halált okozhat (vétlen találat, gondatlan kezelés, stb.).

3.2. A 3. fejezet összefoglalása

A fejezetben ismertettem azt a társadalmi folyamatok generálta bűncselekményi, bűnözői átstrukturálódást, amelyben az elkövetési módok, az elkövetés eszköze és a támadott érték is átalakult. Megállapítottam, hogy a pénzintézeti biztonság megteremtéséhez szükséges a védelmi koncepció terén is paradigmaváltást végrehajtani.

A jelenleg rendelkezésre álló, ismert fizikai beavatkozó eszközök mellett a biztonságtechnika eszközrendszerében meg kell jelenni a bűncselekmény folyamatába történő beavatkozást elősegítő, elvégző eszközöknek. Ezeknek a preventív szerepet kell betölteniük, tehát a tulajdonképpen a még kísérleti szakban lévő deliktumokat kell detektálni és jelzésük alapján az élőerőnek a jogsértő cselekményt megakadályozni. Mindehhez pedig az elkövetési szándékra jellemző magatartásforma kimutatására van szükség. A digitális videotechnika intelligens szoftveres támogatottsággal történő alkalmazása a pénzintézetekben nagyon hatékony lehet. A sajátos speciális körülmények miatt jól detektálható viselkedésparaméterek a szándékos, erőszakos elkövetések esetében alkalmas prevenciós eszközzé tehetik a szoftveres magatartásmegfigyelő-szűrési technikát. Ennek alkalmazásához azonban még számos kísérlet, fejlesztési folyamat és eszköz-innovációs elem szükséges.

Szintén új és biztonsági szempontból eredményes eszközként elemeztem az emberi testet, mint infravörös-sugárforrás (hőkibocsátó anyag). Vizsgálandó kérdés e körben az, hogy az elkövetésre alkalmas eszköz (fegyver) rejtett jelenléte kimutatható-e minden esetben ezzel a módszerrel. Az első alkalmazási mód passzív eszközként alkalmazta a

[13] Jelenleg több koncepció fut teszt üzemmódban a mobilizálástól az élőerő teljes kiiktatásáig - keresve az ideális új megoldást (pl.: SECURIMASTER, ERSTE Bank, SBER Bank, stb.).

technikát, azonban nagyobb eredményesség produkálható, hogyha aktívvá tesszük (tehát pl. a bankfiók ügyfélterébe lépő személyt célzottan megfújatjuk egy gyenge légsugárral). Annak pontos és megbízható detektálásához azonban, hogy a célszemély visel-e fegyvert még számos vizsgálat, kísérlet lefolyatatása szükséges.

Saját kutatást, kísérletsorozatot folyatattam le az innovatív, aktív biztonságtechnikai eszköz, a „ködgenerátor" esetlegesen banki környezetben történő alkalmazási metodikájára. Ez az eszköz indítása után nagy sebességgel és sűrűséggel ködszerű anyagot juttat ki környezetébe - gyakorlatilag láthatatlanná téve a behatoló, rablást megkísérlő számára a célterületet. A bűnügyi érdeket és elkövetési magatartást figyelembe véve került meghatározásra a kísérlet helyszíne. Az alkalmazási szimuláció kiértékelésének eredményeképp megállapítottam, hogy az eszköz alkalmazásával az elkövető szándéka meghiúsítható, valószínűleg csak rongálási kár keletkezik. Ugyanakkor arra a következtetésre jutottam, hogy a helyszínen tartózkodó vétlen személyek vonatkozásában további vizsgálatok szükségesek, az esetlegesen őket ért poszttraumás stressz-szindróma, illetőleg az egyéb negatív pszichés hatások elkerülése érdekében.

4. PARADIGMAVÁLTÁS A PÉNZINTÉZETI SZEMÉLYAZONOSÍTÁSBAN

Az emberi test, testrészletek alaki és funkcionális tekintetben rengeteg közös és egyedi jeggyel rendelkezik, rendelkeznek, amely(ek) mérhetővé tétele általában nem technikai probléma. A mérőeszközök detektorfelületeinek érzékenysége, a mérési távolság, a meghatározás sebessége - hogy csak néhányat emeljek ki azok közül a fejlesztési területek közül, ahol nagy valószínűséggel még fogunk találkozni újabb és újabb, egyre fejlettebb megoldásokkal. A „klasszikusnak" mondható biometrikus azonosítás [1] (ujjnyomat, arc, írisz, stb. alapján) mellett a viselkedéselemzésből fakadó tevékenységazonosság, vagy a deviáns megnyilvánulás is lehetőséget ad az egyénre jellemző paramétereket szolgáltató mérési, összehasonlítási módszerek alkalmazására.

Egy biometrikus azonosítási módszer akkor alkalmazható hatékonyan [2] a (pénzintézeti) személyazonosításban, ha a nyert adathalmazt biztosító alaptulajdonság:

- egyedi (csak arra a személyre jellemző),
- állandó (pl. a korral nem változik),
- mérhető (adattá konvertálható),
- gyors (néhány másodperc alatt eredményt szolgáltat),
- elfogadott(higiénikus felvételi-ellenőrzési eljárás),
- megbízható (nem sérülékeny, csekély számú támadási ponttal rendelkezik).

Biztonsági szempontból kiválasztott és elfogadható, azonosításra alkalmas paramétereknek tekinthetjük a következőket:

- Az emberi test egyedi, csak arra az egy személyre jellemző jegyei (amelyek a mérhető jellemzőkkel rendelkeznek):
  - fizikai érintkezés alapján: ujj-, tenyér-, talplenyomatok, fül, stb. és a bőrzsír,
  - a testről lehulló biológiai anyagmaradványok (elszáradt bőrdarab, haj), amelyek DNS vizsgálatra alkalmasak,
  - amelyek a test funkcionális működése következtében jutnak a személyünk környezetébe és az egyéb személyazonosításra alkalmas testvegyületek (kilélegzett pára, vizelet, széklet, verejték), amelyek a DNS vizsgálatra alkalmasak,
  - esemény-reakciótermékek (kipárolgással jelennek meg).

- Személyiséget meghatározó alaki formajegyek melyek képrögzítés, képelemzés, hangrögzítés után elemezhetőek:
    - az arc vonásai, kéz-, és ujjérhálózat geometriája, az írisz hálózata, a beszédhang frekvencia jellemzői,
    - egyedi testjellemző mozgásjegyek,
    - deviáns testtartás, alaki egészségi okokból eredő mozgási szokások, stb.,
    - egyedi szokásjegyek: kéz láb tartása, lábrázás, fej kapkodása, stb.
- Sérülésből eredő nyomok (felhámfoszlány, vér),
- Közös, minden emberre vonatkozó, közel azonos cselekményfüggő paraméterek:
    - a pulzus és a légzés feszült állapotot jellemző szaporasága,
    - az adrenalin szint emelkedése,
    - az emberi test infravörös sugárzása.

Mindezek után - talán túlzás nélkül - lehet azt mondani, hogy az érzékelés ismert eszközei, az érzékenységi korlátok, a mérési sebesség, stb. a legfőbb akadályai a fantáziánk által sugallt további lehetséges paramétereknek. [3]

A biometria alkalmas egy személy megadott biológiai paramétereinek mérésére, [4] azok rögzítésére és - összehasonlításon alapuló algoritmusok segítségével - ellenőrzésre, azonosítására, hitelesítésére. Személyazonosításra magát a személyt, és nem egyéb, azonosítás céljából hozzárendelt eszközt (pl. különböző igazolványok) használ fel.

Az egyértelmű azonosításhoz a következő, személyenként eltérő, egyedi élettani vagy viselkedési jellemzőket használják:

- aláírás,
- arckép,
- ujjlenyomat, ujjnyomat, ujjnyom,
- talplenyomat,
- hangtónus,
- DNS genotípus,
- fehérvérsejt antigén,
- kézgeometria,
- kézerezet, ujjerezet (érhálózat),
- arc (2D, 3D),
- kéz, csukló,
- szem retinájának vagy íriszének mintázata, stb.

A mérési folyamat mechanizmusa a következő:

- A szenzor, detektor rögzíti a szükséges biometriai mintát az adott személytől.
- A teljes mintából a program kiemeli a jellegzetes (azonosításra alkalmas) jegyeket.
- Az algoritmus ezt az adatbázisban található mintaelemekkel összeveti és kiértékeli.
- Ez alapján azonosítási választ generál (egyezik - nem egyezik, „Go - No go" típusú azonosítás).

A különféle biometrikus rendszerek biztonságának mérésére a sok mutató közül a két leglényegesebb a [5]:

- téves elfogadási hányad - FAR ((False Acceptance Rate: jogosultként ismer fel nem jogosult személyt),
- téves visszautasítási hányad - FRR (False Rejection Rate: nem jogosultként ismer fel jogosult személyt).

Közülük nyilvánvalóan a FAR index a fajsúlyosabb, hiszen ez azt jelenti, hogy ekkor olyan személy kap jogosultságot, aki azzal egyébként nem rendelkezik. Néhány biometrikus rendszer FAR mutatója (tájékoztató jellegű, eszköz-specifikus adatok):

- hangazonosítás, hanganalízis: 200…1.000 : 1;
- arcfelismerés (2D, 3D): 2.000…10.000 : 1;
- kézgeometria-analízis: 10.000…100.000 : 1;
- érhálózat-azonosítás: 100.000…1.000.000 : 1;
- ujjnyomat-azonosítás: 100.000…1.000.000 : 1;
- írisz-, retinavizsgálat: 10.000.000 : 1.

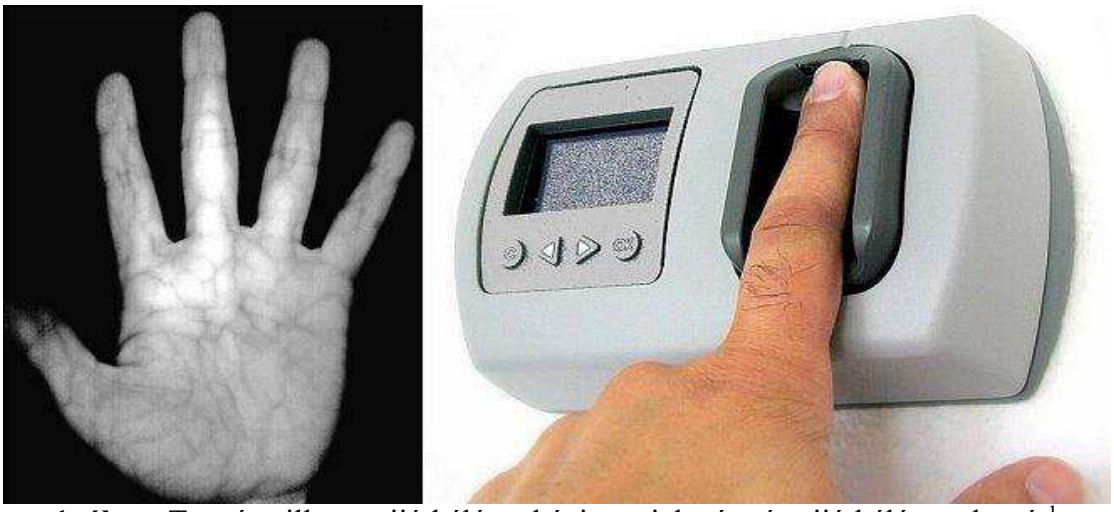
4.1. A legelterjedtebb biometrikus azonosítási módszerek [6]

A jelenleg leginkább alkalmazott biometrikus azonosítási módszerek:

- ***Kézgeometria-azonosítás.*** Működésének lényege, hogy a kéz felületéről és formájáról vesz mintát: figyelembe veszi az ujjak hosszúságát és szélességét, a kézfej szélességét, illetve a tenyér és az ujjak méretarányát. A hatékony felismerést négy pozícionáló tüske segítségével érik el, amely azonos állásba helyezi a különböző felhasználói tenyereket a beolvasáshoz. Léteznek pozícionáló tüske nélküli változatok is, amelyeknél további paramétereket jelentenek - többek között - az ujjba, illetőleg tenyérbe írt körök sugarai. A módszer széles alkalmazási terü-

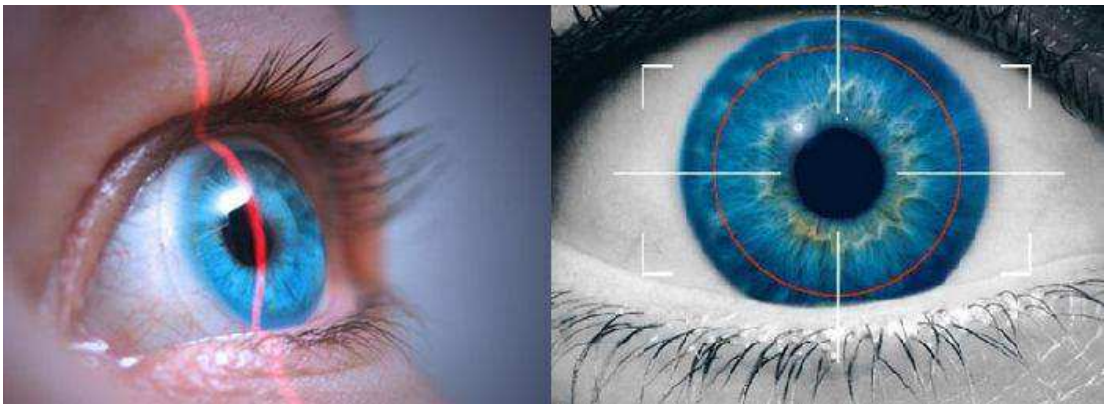
lettel rendelkezik, pl. munkaidő nyilvántartási feladatokra, illetve az egészségügyben a betegek azonosítására használják.

- ***Ujj-, és tenyérerezet-azonosítás.*** Az ujj-, és tenyérerezet azonosítás egy viszonylag új módszer a biometrikus azonosítás terén. A működés alapja, hogy az ujjat vagy tenyeret infravörös fénnyel megvilágítják, és a vérben levő hemoglobin elnyeli a fotonokat. Belső biometriai adatokat mér, tehát nehezen hamisítható (kevésbé sérülékeny) módszer (**1. ábra**).



1. ábra: Tenyér-, illetve ujjérhálózat képi megjelenése és ujjérhálózat olvasó.[1]

- ***Írisz-azonosítás.*** A szem szivárványhártyának mintázatán (**2. ábra**) alapuló biometrikus azonosítás egyike a legjobb azonosítási módoknak, köszönhetően az akár 400 azonosítható jellemzőnek. Az írisz életünk során nem változik,már az embrionális korszakban kialakul. Annak az esélye, hogy két írisz megegyezzen, szinte kizárt, ennek a valószínűsége $1:10^{70}$ nagyságrendbe esik. A leolvasás során aktív, illetve passzív felvételkészítésről beszélhetünk (együtt kell működni az eszközzel utasításokat végrehajtva - vagy sem).



2. ábra: Írisz-azonosítás.[2]

[1] Forrás: http://cache.gizmodo.com/assets/images/gizmodo/2008/07/palm-vein-scan.jpg; http://img.directindustry.com/images_di/photo-g/biometric-sensor-finger-vein-reader-396431.jpg

[2] Forrás: http://www.airport-int.com/upload/image_files/articles/images/companies/1688/biometrics-sec01-l.jpg; http://fingerprint-security.net/wp-content/uploads/2011/05/Iris-Scan.jpg

- ***Retina-azonosítás.*** A retina alapú azonosítás során infravörös fénnyel világítják meg a szemfenéken található retinát, így az ujj-, és tenyérerezet azonosítóhoz hasonlóan működve, az infrasugarak eltérő mértékben nyelődnek el az érhálózatban annak környezetéhez képest - kirajzolva egy viszonylag könnyen feldolgozható rajzolatot. A módszer egyik legnagyobb hátrányát jelenti, hogy a mintavételezési eljárás során az olvasóval közvetlen kapcsolatot kell kialakítania a szemnek, ami által nő a fertőzésveszély (nagy a felhasználói ellenállás az alkalmazással kapcsolatban). A technológiát ma már csak rendkívül ritkán alkalmazzák, akkor is különösen nagy biztonságot igénylő objektumokban.
- ***DNS-azonosítás.*** A DNS esetében drága berendezések kellenek a pontos azonosításhoz, ehhez képest igen könnyen másolható akár az utcán (porszívó-tartalom) talált anyagból (hajszál, szőrszál). Gyakorlatilag alkalmazhatatlan, elméletileg a legbiztonságosabb.
- ***Ujjnyomat-azonosítás.*** Az ujjnyomat azonosítási technika [7] kulcsa, hogy az ujj barázdáltsága mindenkinek egyedi mintázatú. Ez 18 hetes korunkban alakul ki és a későbbiekben sem változik (jelentősen), követi a kéz méretbeli változását. Az égés, vágás, kopás vagy marás során keletkező sérülések 10-40 napon belül képesek regenerálódni. Az ujjunkra tekintve láthatunk kis barázdákat, vonalakat, amelyeket fodorszálnak, illetve fodorvonalnak nevezünk. A fodorszálak az ujjnyomat globális (boltozat, hurok, örvény) és lokális jellemzőit (végződés, sziget, pont, elágazás, híd, stb.) határozzák meg. Az ujjnyomat azonosítók (**3. ábra**) az utóbbiakat használják működésük során.

3. ábra: Ujjnyomat-olvasó eszközök.[3]

[3] Forrás: http://fingerprint-security.net/wp-content/uploads/2011/07/fingerprint-scan.jpg; http://www.procontrol.hu/GyartasFejlesztes/Termekeink/ProxerBio2/proxerbio_300.jpg

- ***Arc alapú azonosítás.*** Az arc alapú azonosításnak két módszere van: a minta alapú, valamint a geometriai. A minta alapú azonosítás során egy már korábban letárolt mintával hasonlítják össze az arc globális tulajdonságait. Az összehasonlítás az arc részleteinek (szem, ajkak,orr) korrelációjával történik. A geometriai elvű arcazonosítás során az arc körvonalainak és különbözőrészleteinek egymáshoz viszonyított helyzetét méri és hasonlítja össze az adatbázisban tárolt adatokkal. Az azonosítás során mért paraméterek a következőek:
  - a jobb és a bal szem két szélsőpontja,
  - a jobb és a bal orrcimpa két szélsőpontja,
  - a száj középpontja (stabilabb, mint a két szélsőpont),
  - az áll jobb és bal pozíciójának vízszintes pozíciója,
  - az áll közepének függőleges pozíciója,
  - a jobb (bal) szemöldök függőleges pozíciója,
  - a jobb (bal) fülcimpa vízszintes pozíciója.

  Ha nem egy, hanem több képalkotó eszközt tartalmaz az azonosító, nem csak 2D, hanem 3D képet is képesek vagyunk készíteni.

  Az arcfelismerésben jelenleg nem elterjedt eljárás az arc thermogramjával történő azonosítás. A thermogram - az érhálózat egyedisége alapján - ugyancsak alkalmas az azonosításra. Ez a szükséges képrögzítő eszköz, a hőkamera költségei miatt azonban nem terjedt el napjainkban. A digitalizált felvételen a mintát azonosító algoritmus ellenőrzi a relatív hőmérséklet különbségeket.

4.1.1. A biometrikus eszközök alkalmazásának kockázata, vizsgálati szempontjai [8]

Egy biometrikus azonosítást igénylő biztonságtechnikai probléma megoldása során lényeges, hogy az adott rendszert ért váratlan esemény(ek)ből keletkező kár várható értéke a lehető legkisebb legyen. Ha egy nagyobb biztonsági kockázatú folyamat zavartalan lefolyását kell biztosítanunk valamilyen biometrikus eszközzel, célszerű kockázatelemzést is készíteni, hiszen ki kell választanunk azt az eszközt, amely az adott kockázatokat a lehető legnagyobb mértékben költséghatékonyan csökkenti le.

A kockázatelemzésnek 9] feltétlenül tartalmazni kell a felhasználói környezet leírását, amelyből értékelhető információkat kapunk arról, hogy milyen létszámú és természetű

személyek jogosultságait akarjuk meghatározni, valamint milyen értékű tulajdont akarunk védeni.

Nyilvánvaló, hogy egy nagy eszmei, anyagi értékkel bíró tulajdont nem védhetünk egy könnyen kijátszható eszközzel. Az viszont gyakran a szakemberek figyelmét elkerüli, hogy az eszközök különböző fizikai környezetben különböző módon működnek, amelyek téves jogosultságkiadásokat-visszatartásokat vonhatnak maguk után.

A gyártók publikációikban, datasheet-jeiken feltüntetnek adatokat az eszközök stabil működéséhez szükséges fizikai környezetről, viszont ezek nem feltétlenül fedik le a teljes spektrumot.

A sérülékenységi paraméterek meghatározása, az ehhez kapcsolódó mérések elvégzése a referenciául szolgáló paraméterek mellett valós képet ad az eszközök egy adott környezetben történő működéséhez.

A különböző klímatényezők (páratartalom, hőmérséklet), valamint a fényviszonyok és az elektromágneses viszonyok mellett figyelembe kell venni a felhasználói viselkedésekből, hajlandóságokból adódó kockázatokat. Meg kell vizsgálni egy létesítés megkezdése előtt azt is, hogy a felhasználók milyen hajlandóságot mutatnak [10] a biometrikus azonosító eszköz használatával kapcsolatban. A használatra vonatkozó hajlandóság nagyban növeli a biztonság szintjét.

Nagy kockázatot jelent a nem megfelelő adatvédelmi protokollok, jelzésátvitelek választása. Az eszközök kijátszása, ezáltal hamis jogosultságok megszerzése nem csak fizikai, hanem szoftveres módon is történhet. A biometrikus azonosító eszközök működéséből adódóan fenn áll annak a veszélye is, hogy jogosulatlanok hallgatnak le bizonyos kommunikációs csatornákat - így szerezve érzékeny információkat.

Közvetlen támadások érhetik egy eszköz által rögzített minták adatbázisát is, amellyel szintén jogosultságokat szerezhetnek arra nem illetékes személyek. Az adat-, és információ védelemmel párhuzamosan fejlődnek a támadó jellegű eljárások, amelyek fontossá tették az információ védelem naprakészségét is.

A pénzintézetekben alkalmazható biometrikus azonosítók vizsgálati szempontjai a következők:

- Általánosság, univerzalitás: a felhasználói csoport minden egyes tagja rendelkezik-e a mért jellemzővel.

- Egyediség: előfordulhat-e az az eset (milyen gyakran), hogy több felhasználó is ugyanazzal a jellemzővel rendelkezik.
- Maradóság: változik-e idővel az adott paraméter.
- Eltulajdoníthatóság: mennyire másolható, eltulajdonítható az adott biológiai, biometriai jellemző (külső vagy belső paramétereket mérünk-e).
- Teljesítmény: a biometrikus adat beolvasása után milyen gyorsan képes a módszer a válaszadásra.
- Elfogadottság: a felhasználó részéről mennyire elfogadható módszer (szükséges-e közvetlen kontakt az eszközzel az adatfelvételhez).
- Megtéveszthetőség: mennyire megtéveszthető az adott biometrikus módszer (idegen, hamis minták bevitele egy adott rendszerbe).

A fejezet első részében felsorolt módszerekre alkalmazva a vizsgálati szempontrendszert jutunk a **4. táblázat**hoz (a következő oldalon).

módszer / szempont	univerzalitás [%]	egyediség[b]	maradóság	eltulajdonníthatóság[c]	teljesítmény[d]	elfogadottság[e]	megtéveszthetőség[f]	megjegyzés (hibaforrás)
kézgeometria	~ 100[a]	nagymértékben egyedi	kis mértékben változhat (tömegváltozás, sérülések)	egyszerűen másolható	s	a módszerhez létezik érintés nélküli eszköz	szükséges az élőminta felismerést az eszközbe integrálni	nem teljesen egyedi, kis mértékben változhat, másolható
érhálózat	~ 100	teljesen egyedi	nem változik felnőtt korban	nem másolható	s	érintés nélküli	nem téveszthető meg	esetleg az eszközben
írisz	~ 100	teljesen egyedi	csecsemőkorban már stabil	egyszerűen másolható	10…30 s	érintés nélküli	szükséges az élőminta felismerést az eszközbe integrálni	szükséges az élőminta felismerés
retina	~ 100	teljesen egyedi	betegséggel módosulhat	nem másolható	10…30 s	érintkezés a mérőeszközzel	nem téveszthető meg	fertőzésveszély, felhasználói ellenállás
DNS	100	teljesen egyedi	stabil	másolható	h	érintés nélküli	nem téveszthető meg	lassú
ujjnyomat	~ 95	teljesen egyedi	sérüléssel változhat	egyszerűen másolható	s	érintéses	szükséges az élőminta felismerést az eszközbe integrálni	20-ból egy embernek nincsen ujjnyomata
arc	100	egyedi	az évek során változik	egyszerűen másolható	s	érintés nélküli	szükséges az élőminta felismerést az eszközbe integrálni	változhat, másolható, elfedhető

Jelmagyarázat:

[a]: a ~ 100 % azt jelenti, hogy csak azok nem rendelkeznek az adott jellemzővel, akinek fizikailag hiányzik az adott szerve.

[b]: korreláció a FAR indexszel: *egyedi*: 2.000…10.000:1; *nagymértékben egyedi*: 10.000…100.000:1; *teljesen egyedi*: 100.000…10.000.000:1.

[c]: a külső biometrikus jellemzők az egyszerűen másolhatók. Általában védelmi megoldást jelent az élőminta-felismerés eszközbe integrálása.

[d]: 1:N típusú azonosítás esetén az felhasználói bázis méretétől függően jelentős eltérések lehetnek. Beléptető rendszereknél az áteresztési idő a feltűntetett időnek akár a többszörösével lehet számolni.

[e]: az érintés nélküli technikák elfogadottabbnak számítanak (nincsen fertőzésveszély).

[f]: a módszer megtéveszthető-e hamis mintával.

4. táblázat: A pénzintézetekben alkalmazható biometrikus azonosítási módszerek vizsgálata feladatorientált szempontrendszer alapján.

A **4. táblázat** elemeit lássuk el színkitöltéssel olyan módon, hogy jelöljük zölddel a teljesen mértékben alkalmas, sárgával az elfogadható míg, naranccsal a kismértékben elfogadható jellemzőket (**5. táblázat**).

módszer / szempont	univerzalitás [%]	egyediség	maradóság	eltulajdoníthatóság	teljesítmény	elfogadottság	megtéveszthetőség	megjegyzés (hibaforrás)
kézgeometria	~ 100	nagymértékben egyedi	kismértékben változhat (tömegváltozás, sérülések)	egyszerűen másolható	s	a módszerhez létezik érintés nélküli eszköz	szükséges az élőminta felismerést az eszközbe integrálni	nem teljesen egyedi, kis mértékben változhat, másolható
érhálózat	~ 100	teljesen egyedi	nem változik felnőtt korban	nem másolható	s	érintés nélküli	nem téveszthető meg	esetleg az eszközben
írisz	~ 100	teljesen egyedi	csecsemőkorban már stabil	egyszerűen másolható	10…30 s	érintés nélküli	szükséges az élőminta felismerést az eszközbe integrálni	szükséges az élőminta felismerés
retina	~ 100	teljesen egyedi	betegséggel módosulhat	nem másolható	10…30 s	érintkezés a mérőeszközzel	nem téveszthető meg	fertőzésveszély, felhasználói ellenállás
DNS	100	teljesen egyedi	stabil	másolható	h	érintés nélküli	nem téveszthető meg	lassú
ujjnyomat	~ 95	teljesen egyedi	sérüléssel változhat	egyszerűen másolható	s	érintéses	szükséges az élőminta felismerést az eszközbe integrálni	20-ból egy embernek nincsen ujjnyomata
arc	100	egyedi	az évek során változik	egyszerűen másolható	s	érintés nélküli	szükséges az élőminta felismerést az eszközbe integrálni	változhat, másolható, elfedhető

5. táblázat: A 4. táblázat elemeinek színkódolása.

Az **5. táblázat** adatait tanulmányozva az alapján, hogy a narancssárgával jelölt mezők gyakorlatilag valamilyen elfogadhatatlan jellemzőt hordoznak a szempontjaink vonatkozásában (biometrikus módszerek alkalmazhatósága a pénzintézeti körülmények között) megállapítható, hogy a feladatnak leginkább az érhálózat (tenyér és/vagy ujj) azonosítási módszer felel meg.

4.2. A humán infraemissziós képalkotás

Kutatási területem szempontjából legérdekesebb biometriai vizsgálati terület az emberi test infravörös sugárzásával foglalkozó kutatási irány.[4]

A tárgyak, anyagok, szövetek, tehát az elő emberi bőr is energiát bocsát ki elektromágneses sugárzás formájában - mindez az infravörös kamera segítségével mérhető. A sugárzás intenzitása és hullámhossza a testfelület hőmérsékletétől és emissziós képességétől függ. Az emberi élőbőrnek ideális, az abszolút fekete testhez közelítő a sugárzóképessége (ezért lényeges a fekete test hőmérsékleti sugárzásának fizikai törvényszerűségeit ismerni).

A történelem folyamán a hőmérsékletmérés és a hősugárzás megismerése fokozatosan fejlődött, csakúgy, mint a testhőmérséklet szerepének orvosi jelentősege:a hőmérséklet és az infravörös sugárzás mérésére, érzékelésére különböző típusú,tulajdonságú, technikai felépítésű mérőeszközt fejlesztettek ki. A modern detektorok az ún. mikrobolométeres technológiát alkalmazzak, az érzékelők mátrixszerűen (sorokban, oszlopokban) helyezkednek el.

Az infravörös sugárzáson alapuló hőmérsékletmérésnél több tényezőnek a hatását is figyelembe kell venni, pl. emissziós tényező, relatív páratartalom, levegőhőmérséklet, tárgy-kamera távolság, környezeti objektumok hőmérséklete.

Az infravörös képalkotó eljárás elsősorban nem anatómiai-morfológiai képletek bemutatására alkalmas, hanem a testben zajló funkcionális folyamatok, mint például az izomösszehúzódás, emésztés, idegi aktivitás, vagy a szervekben, szervrendszerekben lezajló biokémiai folyamatok által létrehozott hőmennyiségek eloszlását, azok gócpontjait, illetve a hőtranszport-folyamatok komplex képét mutatja meg.

[4] E témakörrel a Budapesti Műszaki és Gazdaságtudományi Egyetem Egészségügyi mérnökképzési szakán Dr. Szacsky Mihály professzor és tanítványa, Hegedűs László foglalkozott behatóan.

A szervezet anyagcsere-folyamatai mindig hőtermeléssel járnak (kb. 34 °C feletti környezeti hőmérséklet esetén hőfelvétel is van). Minthogy a keletkező hő mennyisége az anyagcsere-folyamatok intenzitásával aranyos, a hőleadás pedig a külső környezet hőmérsékletétől is függ, a szervezet hőegyensúlyát a hőtermelés és hőleadás állandó változtatásával, a hőszabályozásnak kell biztosítania.

Nyugalomban a hő elsősorban az agyvelőben, a szívben, májban, a gyomor-bélrendszerben és a vesében keletkezik, míg mozgások során az izomzat hőtermelése a legjelentősebb tényező. A keletkezett hő kb. 85 %-ban a bőrön és 15 %-ban a tüdőn keresztül távozik. A hőtermelés és a hőleadás helyei között a vérkeringés teremt kapcsolatot, a szállító közeg a vér. A szervekből érkező vénás vér hőmérséklete magasabb, mint az odaáramló artériásé, a bőrből és a tüdőből jövő pedig valamivel alacsonyabb az artériás hőmérsékleténél.

A ma gyártott infravörös kamerák már kis térfogatúak és tömegűek, nagy teljesítményű akkumulátorról működtethetők, igen mobilak. Bekapcsolást követően szinte azonnal használhatok. Egyes modellek kalibráltak, ezáltal nagyon pontos hőmérsékleti adatok mérésére is alkalmasak. Több tudományos és fejlesztési ágban szinte nélkülözhetetlen eszközzé váltak.

A 80-as években az amerikai Védelmi Minisztérium titkos, nagyléptékű megbízást adott a Honeywell és a Texas Instruments (TI) vállalatoknak a hűtés nélküli infravörös érzékelő technológia kifejlesztésére. A hadsereg olyan eszközt akart, amelynek nagyon rövid a bekapcsolási ideje. Mindkét program igen sikeres volt: a TI a tűzérzékelő (pyroelectric sensor), a Honeywell pedig a mikrobolométer[5] kifejlesztése területén ért el sikereket.

1992-ben az amerikai kormányengedélyezte az infravörös technika-kereskedelmet, de azóta is ellenőrzése alatt tartja a technológiát. [11]

Ma már általánosan elterjedtek a modern felvezető bolométerek, amelyekben a platinát félvezető csíkokra cserélik ki (ezeknek sokkal nagyobb a hőmérsékleti együtthatójuk, ami az eszközt érzékenyebbé teszi).

[5] Sugárzó hő mérésére szolgáló érzékeny műszer. Eredeti formájában két részből áll, mindkettő elfeketített (kb. 1 μm vastag) platina csíkokat tartalmaz, amelyeket egy szigetelő keretben helyeztek el egymás után cikk-cakkban sorba kötve. A két részt egy Wheatstone-híd két szomszédos karjára kötik, az egyik részt sugárzásnak teszik ki, a másikat leárnyékoljak. A sugárzásnak kitett rész ellenállásának megváltozása (amelyet az áthidaló árammérő segítségével lehet mérni) lehetővé teszi az elemre eső sugárzó hő kiszámítását.

A biztonságtechnikai szakemberek sem találkoznak gyakran hőkamerákkal [12] a munkavégzésük során, mert a felhasználhatóságuk, és nem utolsó sorban a költségigényük általában az ipari, illetve katonai környezethez köti azokat.

Az emberi szem az elektromágneses spektrum csak nagyon kis szeletét képes látni. Nem érzékeljük sem az UV, sem az infra tartományokat - ezekhez a csúcstechnikát kell igénybe venni. A biztonsági szakma egyre újabb és újabb területeit fedezi fel a hőképek felhasználásának.

Elődeink már évezredek óta alkalmazták (és ebben mi sem vagyunk kivételek), hogy hideg időben a tűz körül (illetve napjaik modern embere a beépített kandalló mellett) ülve a tenyérrel próbálták felfogni a tűzből áradó meleget (azaz tenyérrel meg tudjuk találni azt a pontot, ahol a hőáramlás számunkra a legkedvezőbb).

Ezt a fizikai jelenséget felhasználva napjainkban a tudomány már egészen elképesztő eredményekkel képes szolgálni a kiemelkedő biztonsági kockázatú létesítmények biztonsági rendszerei kiépítésben.

A kezdeti fejlesztések oka ebben az esetben is az „egyszerűen” meghatározható katonai igények voltak: látni kell sötétben, bármiféle megvilágítás nélkül, és látni a füstös, rosszlátási viszonyokat biztosító csatatereken is.

A „bolométer elv” maga már sok-sok éve ismert [13]: tárgyak, élőlények elektromágneses sugárzásának mérése azok hősugárzásának felhasználásával. A teória kidolgozásban Samuel Pierpont Langley (1878) járt az élen, majd százéves szünet következett, míg az elektronika olyan szintre volt képes fejlődni, ahol a szenzorok által biztosított elektromos jelek gyors feldolgozására már megvolt a reális esély.

Mielőtt részletesen beszélnék a hőkamerák működésének vonatkozásában fontos tartomány a 1 µm-es hullámhosszúságnál kezdődik és 1 mm hullámhossznál fejeződik be. A biztonságtechnikai alkalmazások esetében a leggyakoribb a 8--14 µm-es LWIR (Long Wave Infrared)[6] tartományban működő kamerák felhasználása.

A biztonságtechnikai kamerákban használt „mikrobolométer” elnevezésű hőérzékelő [14] valójában egy speciálisan a hőkamerák számára kialakított bolométer. A hűtetlen hőképalkotó kameráknál az alapanyag a leggyakrabban a VO (vanádiumoxid) háló, vagy amorf szilikon. Az igényes biztonságtechnikai alkalmazások esetében a VO elekt-

[6] Long Wave Infrared - hosszú hullámú infravörös sugárzás

ronikai szempontból igen kedvező, mivel a legtöbbet használt hullámhosszúságú tartományban a vanádiumoxid jól mérhetően változtatja az elektromos ellenállását. Ez az érték 100 kΩ nagyságrendű, ami igen jól használható különböző mérőáramkörök készítésénél.

Hőkamerák esetében nem egyszerű az egyes eszközök összehasonlítása. A CCTV rendszerekkel foglalkozó kollégák pontosan tudják, hogy a látható tartományú kamerák összehasonlító vizsgálatánál szükséges egységes vizsgálati módszer miatt minden paramétert, műszaki jellemzőt pontosan meg kell határozni a mérések előtt. Természetesen ebben ez esetben sem lehet eljárni másként, azonban van egy alapvetően meghatározó paraméter, amely az eszközbe beépített mikrobolométertől függ: ez az NETD[7]. Ez a műszaki jellemző meghatározza a felhasználni kívánt kamera „érzékenységét", megmutatja milyen hőmérséklet különbséget lesz képes a kameránk érzékelni. Ezt a paramétert egy adott "F Stop" szám megadása mellett szokás meghatározni (pl.: 50 mK = 0,05 ºC - F1.2).

Napjainkban a legtöbbet eladott mikrobolométer hálót (képalkotó elemek rendszere) tartalmazó kamerák felbontása 640x480, 320x240, vagy 160x120.

A legjobb felbontású háló (1024x768) 2008-óta van jelen a piacon, de természetesen még az 1 MP feletti felbontású érzékelő is megtalálható a gyártásban (azok kizárólag a katonai alkalmazások számára elérhetőek).

A képtömörítési technológia folyamatos fejlődésének, a növekvő átviteli csatornák sávszélességének és az egységnyi megabyte-on történő tárolás árának csökkenése is okozhatja, hogy folyamatosan nő a megapixeles képet adó kamerák alkalmazása.[8] Ez érthető fejlődés a látható fény spektrumban történő képalkotáskor, azonban ebben a technológiai környezetben akár a legkisebb felbontású érzékelőt tartalmazó kamera is kiváló eredményt érhet el egy adott alkalmazásban és adott képelemző program támogatásával. Soha nem szabad figyelmen kívül hagyni azt a tényt, hogy egy hőkamerás rendszer képét nem nézik az operátorok (t. illik nem azért készül). A fő funkció a videó analitikai szoftverek kiszolgálása, jelzésadás, ha az ellenőrzött képtartományban az előre beállított szabályoknak megfelelő változás van.

[7] NETD - Noise Equivalent Temperature Difference - Zajszinttől (hőzaj) megkülönböztethető hőmérséklet különbség
[8] Stepping into new trends: Video surveillance in 2015 (http://www.asmag.com/showpost/18290.aspx)

A mikrobolométerek felhasználása nagyban függ az elérendő céloktól, így azok különböző fajtái a funkciómeghatározott, célberendezésekben más és más kialakításban kerül beépítésre. A bolométer-fajták speciális környezetben történő alkalmazását elsősorban az ún. hűtött detektorok felhasználása jellemzi (a kialakított mikrobolométert, a lényegesen jobb NETD érték elérése érdekében hűtéssel látják el). A hűtés hatására több olyan műszaki jellemző változik, amelyek a vizsgált alkalmazás esetén előnyökkel kecsegtet.

Az előnyök:

- alkalmas multi spektrumú sugárzásnál,
- nagysebességű változások esetében is jól használható,
- az érzékenysége nagyságrenddel jobb.

A nem hűtött detektorok elterjedését a mikroáramkörök, alkatrészek fejlődése is támogatta. A tömeges gyártásunkhoz jelentős érdekek fűződtek, mivel a nagyarányú elterjedésük a hétköznapi életben történő felhasználásukat (például a tűzoltóság mentési munkái, a polgári repülés rossz látási viszonyok között, stb.), is lehetővé tették. [15]

Előnyök:

- kis mérete miatt probléma nélkül gyártható biztonságtechnikában használatos kamerákhoz,
- valós idejű videó jelet biztosít,
- alacsony az energiafogyasztás a hűtött detektorhoz képest,
- olcsó, így a civil felhasználásban elterjedhet.

Talán azt is mondhatnánk, szerencsés szakember az, aki hőkamerákkal kapcsolatos gyakorlati feladatokkal, akár tervezés, kivitelezés, üzemeltetés szintjén találkozik. Ennek egyszerű oka a hőkamerák ára. A felhasználhatósága szinte minden területen [16] elképzelhető lenne, de a jelenlegi árak miatt az elterjedtség nem lehet általános (azért előfordul hazánkban is).

Néhány kivételtől eltekintve a kameraképeket képelemző programok [17] dolgozzák fel és adnak jelzéseket az operátorok részére, indítanak vezérléseket a videó analitikai programban beállított szabályoknak megfelelően. [18] Maga a képelemzést végző számítógépes program célszerűen a hőkamerás képek elemzésre készül, a szabályok a funkcionális feladatokat támogatják.

Néhány a biztonságtechnikában előforduló elemzési feladat, amely érinti a szabadalom témáját a következő:

- mozgásérzékelés,
- útvonal detektálás és követés,
- jelenlét detektálás (megjelenik valami a megjelölt területen),
- tömegdetektálás megjelölt területen.

Jogos kérdés, hogy a hőkamerák milyen módon használhatóak. A kutatási terület a Detektálás - Felismerés - Azonosítás szerephármast érinti, ennek is leginkább az első és második tagját, a detektálást és a felismerést. A számszerűsíthető értékelés érdekében célszerű figyelembe venni a Johnson kritériumot.[9] John B. Johnson katonai célú kutatásai alapján a detektálás, felismerés, azonosítás kiegészült egy negyedik orientációs kategóriával is. Ennek harcászati fontossága nem elhanyagolható, azonban biztonságtechnikai relevanciája minimális.

A detektálás (Detection) az, amelynek során az adott kamera már érzékeli a környezetétől eltérő sugárzást. A felismerés (Recognition) esetén azt a távolságot jelenti, amelynél az adott kamera képén már felismerjük, hogy miről is van szó (élőlény, tárgy).

Azonosítás (Identification) esetén az a távolság, amelynél az adott kameraképet vizsgálva már azonosítani tudjuk, hogy a képen feltehetően egy katona, terrorista, cilvil, fegyveres személy, stb. látható. A felsoroltak angol nyelvű megfelelőinek kezdőbetűiből alakul ki a kamera DRI paramétere, melyek a különböző kamera katalóguslapokon megtalálhatók.

A kezdetben használt képerősítő csöves eszközöknél a távolság meghatározásához a Johnson kritériumban szereplő felbontási értékek használhatóak voltak. E szerint a detektáláshoz 1,5 lp/mm[10], a Felismeréshez 3,8 lp/mm, míg a detektálásához 8 lp/mm szükséges célszemély esetén. Ezeket az értékeket nagyban befolyásolhatja a képernyőn jelentkező szcintillációs ingadozás.[11] Ezen túlmenően a DRI értékekre hatással van a látás szöge (ami befolyásolja a célszemély/céltárgy oldalarányait[12]), valamint a képalkotó rendszer kontraszt átviteli függvénye (CTF), vagy a méréseknél inkább használt mo-

[9] Image Intensifier Symposium, (1958. október 6-7.), pp. 249-272
[10] vonalpár / mm
[11] Coltman, J. W.: Scintillation limitations to resolving power in imaging devices JOSA 44(3) : 234–237, 1954
[12] Baker, H. andNicholson, R.: Raster scan parameters and target identification. In Proceedings of the 19th Annual National Aerospace Electronics Conference , 1967, pp 285–290

dulációs átviteli függvénye (MTF)[13] Bár köztudott volt, ennek ellenére 1973-ig[14] nem készült modell arra vonatkozóan, hogy a képalkotó eszköz zajtermelése, milyen módon befolyásolja a DRI értékeket.

Lloyd és Sendall által bevezetett minimális hőmérséklet felbontás (MRT[15]) koncepció[16] felhasználásával a Night Vision Lab próbált modellt felállítani a FLIR[17] eszközök DRI értékeinek meghatározására.

Az igazi áttörés 1974-ben következett be Lawson és Johnson további kutatásainak köszönhetően.[18]A publikációjukban megjelenő formulák némi kiegészítéssel (környezeti változók, kritériumok és beállítások figyelembe vétele mellett[19]) a mai TTP[20] modellnél is alkalmazhatók.[21]

Annak érdekében, hogy egy rendszer tervezésénél elkerülhessük a TTP modellben alkalmazott formulákat, néhány gyártó táblázatok segítségével szemlélteti a DRI-hez tartozó értékeket(**(6. táblázat)**.

6. táblázat: Néhány hőkamera DRI paramétere.[22]

A táblázaton jól látható, hogy például a Xenics belga gyártó egyik legnagyobb teljesítményű hőkamerája, típusnevén az MK-F-75-RA-re vonatkozó DRI adatok személyre vonatkozóan a következők:

- Detection:1.800 m;
- Recognition: 450 m;
- Identification: 120 m.

[13] Sagi, D.: The combination of spatial frequency and orientation is effortlessly perceived. Perception & Psychophysics, 43, 1988, pp. 601-603
[14] Rosell, A. and Willson, R. H.: Basics of detection, recognition and identification in electro-optical formed imagery. In Solving Problems in Security Surveillance and Law Enforcement with Optical Instrumentation,, 1973, pp. 107–122, International Society for Optics and Photonics
[15] Minimum Resolvable Temperature
[16] Lloyd, M. and Sendall, R. L.: Improved specifications for infrared imaging systems, 1970, Proc. IRIS Imaging, pp. 109–129
[17] Forward-Looking Infrared
[18] Johnson, J. and Lawson, W.: Performance modeling methods and problems. In Proceedings of the IRIS I maging Systems Group, 1974
[19] Schmieder, D. E. and Weathersby, M. R.: Detection performance in clutter with variable resolution. Aerospace and Electronic Systems, IEEE Transactions on, AES-19(4):622–630, 2003
[20] Targeting Task Performance
[21] Vollmerhausen, R. H. and Jacobs, E.: The Targeting Task Performance (TTP) Metric A New Model for Predicting Target Acquisition Performance, 2004
[22] A belga XENICS gyártó Meerkat elnevezésű hőkameráinak adatai.

A hőkamerák tekintetében a másik igen fontos tényező a kamerajellemző, amely már nem csak a képfelvevő elemről, hanem az optikával összeépített kameráról ad információt. Ez a jellemző nem más, mint az a távolság, amely esetén a kamerából felhasználható képet kapunk.

Elmondható, hogy a hőkamerák használata a biztonságtechnikában nagyon kívánatos, a biztonsági kockázatokat egy jól megválasztott, tervezett és kivitelezett rendszer esetén szignifikáns módon lennének képesek csökkenteni. Tekintettel arra, hogy az elektronika fejlődése rohamléptekkel folytatódik, [19] az áramkörök árai hasonló módon csökkennek, így várható, hogy az infra-tartományban működő, ma még drága kamerák hamarosan megérkeznek a mindennapi élet szintjére.

4.3. Pénzintézeti alkalmazási lehetőségek

A kibocsátói üzletágban felmerült károk és veszteségek Magyarországon a bankok által kibocsátott kártyák országon belüli és külföldi használatához kapcsolódó visszaéléseket tartalmazzák (ez a kategória magában foglalja a kártyát kibocsátó bank saját hálózatában, a saját kártyáival lebonyolított műveletek során keletkezett károkat és veszteségeket is).

A következő adatok (2006) feldolgozásakor Európán belül a bankkártyák egy jelentős része még csak mágnes csíkkal rendelkezett és a berendezések szintén jelentős része is csak az ilyen típusú kártyákat tudta olvasni.

- a kibocsátói üzletágban felmerült kár értéke 246 mFt,
- a kibocsátói üzletágban felmerült kár mértékének emelkedése 2005-höz képest 13 %,
- a kár összegének a kibocsátói forgalomhoz viszonyított aránya 0,004 % (nincs változás a megelőző évhez képest),
- a visszaélések darabszámát tekintve 100.000 a kártya jogos birtokosa által végrehajtott műveletre 2,5 jogosulatlan esett,
- a hamisított kártyákkal elkövetett kár értéke 126 mFt,
- ellopott vagy elvesztett kártyákkal okozott kár értéke 88 mFt,
- az elfogadói üzletágban felmerült kár értéke 190 mFt,
- Az elfogadói üzletágban felmerült kár mértékének emelkedése 2005-höz képest 20 %.

A legnagyobb kárt a másolt vagy lopott bankkártyákkal, vagy hamis személyazonossággal, ellopott jelszavakkal okozták (okozzák).

A következőkben egyrészt a biometrikus azonosítás, másrészt az infravörös hőkép pénzintézetekben történő biztonságtechnikai alkalmazási lehetőségeit vizsgálom meg.

4.3.1. A bometrikus azonosítás a pénzintézeti gyakorlatban

A biometrikus azonosítás már nem a jövő gondolata. Elegendő olyan mindennapi dolgokra gondolni, mint az új típusú útlevelek[23], egyes laptopok, mobiltelefonok és láthatjuk, hogy széles körben egyre gyarapszik a biometrián alapuló azonosító rendszerek felhasználási köre.

A rohamos elterjedés mögött mind a kereslet, mind a kínálat komoly szerepet játszik. A keresleti oldalon erős az igény a biztonságra. Az egyes államok szeretnék tudni, kik lépik át határaikat, a cégek pedig, hogy kik is lépnek be épületeikbe. A kínálat oldalán pedig megjelentek azok a rendkívül kompakt és olcsó készülékek, amelyek könnyedén beépíthetőek bármilyen eszközbe.

A beléptetésen kívüli alkalmazásra álljon itt néhány példa:

- Fizetés az üzemanyagtöltő-állomásokon. Chicago-ban az ujjnyomat-érzékelős készülékek az autósok bankszámlájához kapcsolódnak, így a fizetés onnan történik.
- Pénzautomaták. Bankok ATM rendszerei, pénzfelvétel céljára (Japán, ujjnyomat **- 7. ábra -**, illetve kártya összekapcsolása a tulajdonossal tenyérérhálózat-azonosítás révén).
- Disney World-ben (Florida) a beengedő kapuknál minden látogatótól ujjnyomatot vesznek és társítják a belépőkártyájukhoz. A parkban nincsen készpénzhálózat, a fizetés ujjnyomattal történik (ami a bankszámlához kapcsolódik). [21]
- Rabok nyilvántartása. Az Egyesült Államokban 1996 óta alkalmaznak egyes büntetés-végrehajtó intézményekben írisz felismerésen alapuló rendszert.

Talán a legjobb példa a biometrián alapuló azonosítási rendszerek széles körű alkalmazására, az Egyesült Államok bevándorlási hivatalának rendszere. Ez a belépő személyek ujjnyomatát hasonlítja össze az adatbázisában szereplő több mint 2,5 millió azonosító-

[23] Magyarország 2006. augusztus 29-től kezdte meg a digitális arcképet és az útlevél adatoldalán megtalálható személyes információkat, 2009. június 28-tól pedig a digitális ujjnyomat adatokat is hordozó chippel ellátott biometrikus útlevelek kiadását.

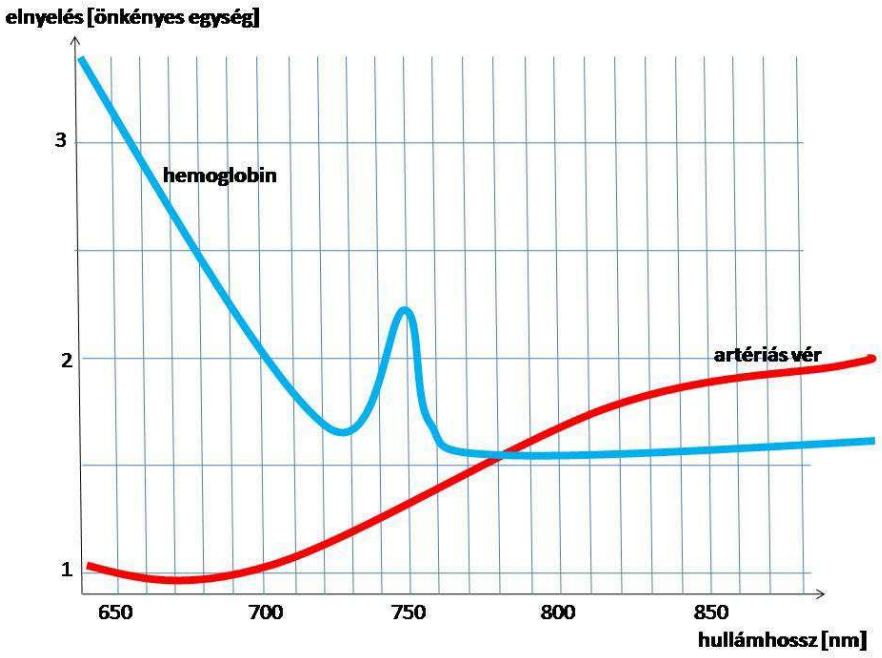
jával. 2004-es bevezetése óta több mint 75 millió látogató ment keresztül a rendszeren, és körülbelül ezer alkalommal tagadták meg a belépést.

7. ábra: Ujjnyomat-érzékelős ATM.[24]

4.3.2. Az érhálózat-azonosítás alkalmazhatósága a bankszektorban

A tenyér-, és ujjerezet-azonosítás alapja a bőr felszíne alatt levő érhálózat kimutatása. A tenyeret a közeli infratartományú fénnyel kell megvilágítanunk, ami kb. 700…1.000 nm között van. Vannak olyan hullámhossztartományok, amelyeken belül a kötött formában levő oxigénben dús hemoglobin (artériás vér), és vannak olyanok, ahol a dezoxidált hemoglobin (vénás vér) nyeli el jobban az emittált fényt (**8. ábra**). Meg kell azonban jegyezni, hogy a vénás vér oxigén tartalma is legalább 70 %, míg az artériásé valamivel kevesebb, mint 100 %.

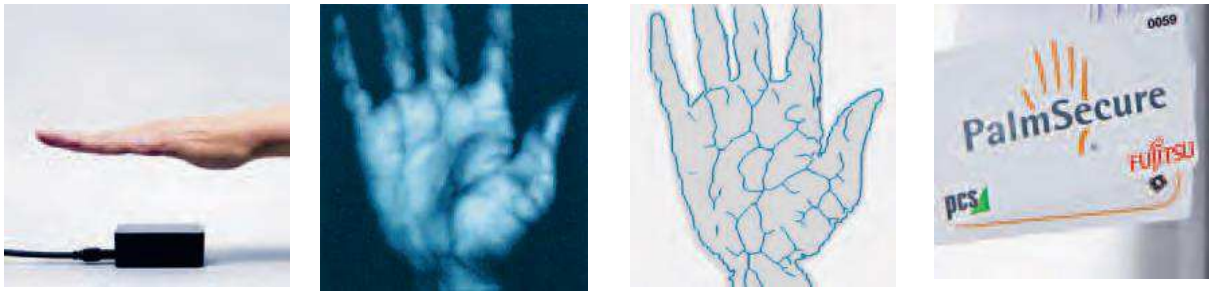
[24] Forrás: http://www.itcbd.com/wp-content/uploads/2010/09/Biometric-Solution.jpg



8. ábra: A vérben levő hemoglobin abszorpciója az infratartományban [22].

Az erezet-azonosítás folyamatát röviden a következőképpen lehet összefoglalni: infravörös fénnyel (általában 750 nm) világítjuk meg a kezet (tenyeret), illetve az ujjat (**a**). A kézben (ujjban) levő erekben áramló vér hemoglobinja az infra tartományban elnyel. Az infra fényre érzékeny kamera képén (~ 5 MB) ezek a területek sötétebben látszanak (**b**).

A képelemző szoftver ebből vonalas grafikát generál (**c**), ami aztán lementésre kerül pl. kártyára (800 byte; d). Ez az azonosítás alapja, hiszen az aktuális mintát összevetve a letárolttal az eszköz szoftvere hoz döntést a minta elfogadásáról, illetve elutasításáról. A letárolt minta generálási folyamatát mutatja be a **9. ábrasorozat**.



a b c d

e

9. ábrasorozat: A tenyérerezet-azonosítás folyamata (e: tenyérerezet 850 nm).

A Fujitsu gyakorlatilag versenytárs nélküli piaci szereplő az érhálózat azonosításban. A cég viszont elég szűkszavú az eszközei által alkalmazott eljárásokról, valamint a képalkotást követő algoritmusokról. Az eljárás fizikai kontaktus nélkül zajlik (néhány modellnél az ujjakat feltámasztó távtartó figyelhető meg[25]), a közeli IR (NIR) tartományban történő, automatikusan beállított erősségű megvilágítás során az abszorpciós/reflexiós folyamat eredményeként egy CCD szenzor végzi a képrögzítést.

Ezt a képet egy algoritmus vonalas grafikává alakítja, majd ez kerül letárolásra. Az éppen azonosított minta a vonalas grafika előállítása után az adatbázisban letárolt mintákkal kerül összehasonlításra egy korrekciós algoritmus segítségével (a tenyér, ujj általában eltérő pozícionálása miatt lényegében mindig más képet kapunk, sablonszerűen tökéletesen egyezőt sohasem (ROI - Region of Insert - meghatározás a szakirodalomban).

Sérülékenységi vizsgálatok* [23] *és az érhálózat-azonosítás

A gyártók által kiadott műszaki adatlapokon feltüntetettek a környezettől függően a gyakorlatban eltérhetnek a leírtaktól. Ez több okra vezethető vissza. A leglényegesebb üzemeltetési paraméterek (hőmérséklet, levegő-páratartalom és ezek stabilitása ott, ahol

[25] Pl. az INTUS PS modell

az eszköz felállításra került) alapvetőek a működés szempontjából. Gyakran a felhasználók fizikai paraméterei (sérült vagy piszkos ujj, kancsalság, stb.) nem megfelelőek a sikeres biometriai azonosításhoz. Néha az is megtörténik, ha a készülék a működési paramétereinek maximumához közel üzemel, hogy az azonosítási eredmények feltűnő mértékben leromlanak.

A biometrikus azonosítás fejlődése szükségessé tette tehát a biometrikus azonosító eszközök sérülékenységi vizsgálatát, amire gyakran használják az „etikus hack[26]" kifejezést.

A sérülékenység vizsgálat nem más, mint olyan folyamatok összessége, amely az adott eszköz gyengeségeire, hiányosságaira mutat rá, a folyamat jellegétől függően egyben megoldást is kínál az adott problémára.

A sérülékenység vizsgálatnak az egyik fő célja a MOA (Mission Oriented Application), vagyis az adott eszköz feladatorientált alkalmazásának meghatározása, tehát azt milyen feladatra lehetséges igénybe venni.

A sérülékenység vizsgálatokat leginkább az információvédelemben alkalmaznak a lehetséges támadási felületek felderítésére, majd ezek megszüntetésére. Természetesen mindezek a biometrikus azonosításban is aktuálisak, [24] mivel támadási felületnek számítanak az olvasó terminált és az azt vezérlő számítógépet összekötő kommunikációs csatornák, valamint a tárolt mintázatokat tartalmazó adatbázisok is.

A biometriai jellemzőket nem csupán a kisebb adatméret miatt kódolják az algoritmusok által, hanem védelmi céllal is, hiszen ha egy mintázat valós képét tárolná a szoftver, akkor a sikeres támadás után azonnal másolható lenne az adatbázisban szereplők biometriai jellegzetességei.

További biztonsági rést jelentenek a különböző kommunikációs csatornák, mivel ezek működésükből adódóan lehallgathatóak. [25]

A sérülékenységi vizsgálatok irányulhatnak egy eszköz fizikai környezettel szembeni sérülékenységére is. A fizikai környezet nem más, mint a klíma-(környezet hőmérséklet és páratartalom), fény-, hang-, és rezgésviszonyok, különböző elektromágneses behatások, valamint közvetlen fizikai ráhatások (ütés, vagy különböző szennyeződések).

[26] Az „etikus hack" az eszközök fejlesztésére (a gyenge pontok feltárására és az azok kijavítására), nem pedig azok rosszindulatú kijátszására irányul.

A másik fontos minősítő jellemző az ún. ACOM (Anti-Cloning Operation Methods), ami lényegében azt vizsgálja, hogy egy adott eszközmiként reagál egy hamisított minta felhasználása esetén.

A gyártók arra törekszenek, hogy megnyugtassák a felhasználót: a lehető legbiztonságosabb eszköz tulajdonosává vált (vagy válik). Rendkívül kellemetlen lehet, ha kiderül: egy nagy beszerzési költségű eszköz működése igen kicsi anyagi ráfordítás révén is megzavarható, befolyásolható. A sérülékenység vizsgálatok publikációi azon célt szolgálják, hogy egy műszakilag képzett potenciális felhasználó is fel tudja mérni, hogy egy adott biometrikus eszköz sérülékenységi kockázatait a felhasználási hely képes elviselni-e vagy sem.

A legjobb védekezési lehetőségek közzé tartozik a megfelelő élőminta felismerő rendszerekkel való bővítés, vagy éppen olyan azonosítási technológia alkalmazása, amely magába foglalja az élőminta felismerését is. Az érhálózat azonosító technika esetében erre az emberi test által kibocsátott 3.000…14.000 nm hullámhossz tartományú IR sugárzást érzékelő szenzor alkalmas. Az élőminta felismerést végző, kiegészítő hardverek működési elvük alapján az alábbiak lehetnek:

- Összehasonlító analízist végző eszközök. Az aktuális mintákból generált adatsort algoritmusok hasonlítják össze a letárolt abszorpciós, reflexiós értékekkel.
- Elektromos ellenállást mérő eszközök. Az élő mintába gyenge áramot vezetnek, majd ennek révén a minta ellenállását mérik. Mivel ez nagyban függ az emberi bőr nedvességtartalmától, az ellenállásértékek széles határok között mozoghatnak (nem biztonságos megoldás).
- Relatív permittivitást vizsgáló eszközök. Az eszköz az elektromos térbe helyezett emberi bőr vákuumhoz viszonyított relatív permittivitását vizsgálja, majd összehasonlítja a letárolt értékekkel. A relatív permittivitást nagyban befolyásolja a bőr nedvességtartalma mellett a hőmérséklet is (nem biztonságos eljárás).
- Hőmérsékletérzékelő eszközök. Annak következtében, hogy az emberi test önmagát melegen tartja, az élő minta felületén, normál körülmények között 26-30 °C hőmérséklet mérhető.
- Pulzoximetriai eszközök. A pulzoximetria az oxingénben dús hemoglobin áramlás mérését jelenti. Egy vörös és egy NIR fényforrással világítják meg a mintát. Az elnyelés mértéke attól függ, hogy a vérben levő hemoglobin kötött formában tartalmaz-e oxigént, vagy már a szövethez eljutva leadta azt és dezoxidált he-

moglobinként távozik a szövetektől. A készülék ezt a körforgást érzékeli az elnyelődés/visszaverődési arány váltakozásából, majd ebből megállapítja a szaturáció függvényét.

A budapesti Groupama Aréna biometrikus beléptető rendszere (1:1 típusú összevetés: kártyára veszik a mintát, beléptetésnél ez kerül összevetésre az aktuálisan leolvasottal[27]) egy Fujitsu alapú érhálózat-azonosító, amelyen magyar hardver-szoftver szakemberek - figyelembe véve az alapkészülék üzemeltetési évei során felmerült hiányosságokat (mintahamisíthatóság, működési anomáliák, stb., amelyekre az Óbudai Egyetem Alkalmazott Biometria Intézetének munkatársai több alkalommal is rámutattak [26]) - jelentős fejlesztéseket végeztek.

A készülék leírása szerint az érhálózat azonosítása:

- 5 millió képpont alapján történik,
- ideje: ≤ 1 s,

Az eszköz:

- kültéren is alkalmazható,
- belőle az üzemeltetésből fakadóan adatgyűjtés nem lehetséges,
- nem készít képet(azonnal titkosított adatcsomagba képezi le az érhálózatot, majd azt kártyára írja, tehát nincsen letárolás),
- nem alkalmas az azonosítandó személy egészségügyi állapotára való következtetés levonására.

A bankszektorban történő alkalmazhatóságot tekintve:

- a belső informatikai rendszerek védhetővé válnak az illetéktelen hozzáférés ellen,
- kiváltásra kerülnek a jelszavak, a belső ügyintézés, átutalási rendszer védhetővé válik illetéktelen hozzáférés ellen („a kéz mindig kéznél van”),
- a Netbankár esetében az ügyfelek másodlagos azonosítóként az érhálózat-azonosítón keresztül igazolják magukat, ami lehetőséget teremt arra, hogy kizárólag csak az arra jogosultak használhassák a rendszert,
- ATM automaták kiegészítése másodlagos azonosításként „mach on card” rendszeren keresztül (azaz a chipkártya tartalmazza az érhálózat adatcsomagját, ami

[27] Ez tulajdonképpen nem azonosítás, hanem ellenőrzés: a kártya tulajdonosa megegyezik annak felmutatójával. Ezzel kiküszöbölésre kerültek az adatvédelmi aggályok is.

a bankomat használata során leadott mintával kerül összehasonlításra: ellenőrzés, hasonlóan a Groupama Arénabeli alkalmazással).

4.3.3. Bankbiztonsági szempontokat figyelembe vevő infravörös sugárzási mérések[28]

A 2014 telén végrehajtott vizsgálatok céljai a következők voltak:

- megállapítani, hogy a ruházatban lévő ember infravörös sugárzása érzékelhető (mérhető)-e laboratóriumi körülmények között;
- mekkora a mérés időtartama;
- érzékelhető-e a véráram okozta dinamikus sugárzásváltozás,
- érzékelhető-e a ruházat alá rejtett (fémből készült) fegyver.

Az alapfeltételezés az volt, hogy az emberi test, mint önálló sugárforrásként képes „működni". Ennek felhasználhatósági értéke lényeges lehet a paradigmaváltás eszközeinek keresésében, hiszen egyrészt kimutathatja a testen rejtett módon viselt idegen tárgyat (fegyvert), másrészt a test jellemző, az átlagostól eltérő(izgalmi) állapotáról is információt szolgáltathat - kellően érzékeny detektor (kamera)esetén.

További feltételezés volt, hogy miután a test a hőmérséklet egyenletes elosztását és fenntartását a véráram útján biztosítja, ezért a véráramot vezérlő frekvenciát, azaz pulzusszámot is lehetséges érzékelni. Amennyiben ez távérzékeléssel is kimutatható, akkor a szapora pulzust, mint támadási előjelzés tekintetbe vehető.

A test dinamikus hőmérsékletváltozását egy rejtett tárgy (fegyver) csak késleltetéssel tudja követni, ennek következtében az kimutathatóvá válhat.

A mérőeszköz jellemzői a következők voltak:

- Bosch VOT-320V013H típusú hőkamera, 320x240 pixel felbontás, 13 mm lencse, 30 Hz-es frissítés,
- 320x240 VOx hőkemarás szenzor,
- integrált képtartalom-elemzés - hőkamerás alkalmazásra optimalizálva.

A mérés során a következőket állapítottam meg:

- A test infravörös sugárzása egyértelműen érzékelhető laboratóriumi körülmények között.

[28] A vizsgálatban részt vett Tóth Levente biztonságtechnikai szakértő is.

- Az érzékelés sebessége megfelelő (késleltetés nélküli).
- A ruházat által okozott késleltetés színeltérésben (hőmérsékletkülönbség és változás) mutatkozik.
- A véráram okozta dinamikus változás („lüktetés”) nem kimutatható.
- A fegyver kőrvonala stacioner állapotban látható.

Összességében megállapítható volt, hogy a felhasznált, legérzékenyebb infravörös kamerák sem alkalmasak (egyelőre) - még laboratóriumi körülmények között sem - a feltételezéseimben megfogalmazott kimutatásokra. Ennek oka elsősorban a ruházat árnyékoló hatásában keresendő. Amennyiben ezt a jövőben sikerül kiiktatni, illetőleg a hőkamerák is további fejlődési szakaszon mennek keresztül, akkor az elképzeléseim megvalósíthatósága - nyilvánvalóan - jelentősen fog növekedni.

A 4. fejezet összefoglalása

A fejezetben megállapítottam, hogy egy biometrikus azonosítási módszer kizárólag akkor alkalmazható hatékonyan a pénzintézeti személyazonosításban, ha a nyert adathalmazt biztosító alaptulajdonság egyedi, állandó, mérhető, gyors, elfogadott és teljes mértékben megbízható adattal szolgál.

Bizonyítottam, hogy a morfológiai, fiziológiai jegyek mellett a személyiséget meghatározó alaki formajegyek képrögzítés, képelemzés, hangrögzítés után elemezhetőek. A folyamat rögzítését és összehasonlításon alapuló algoritmusok segítségével történő ellenőrzésének folyamatát a következőkben határoztam meg:

1. szenzoros detektálás
2. kódolás
3. algoritmus alapú adatértékelés
4. „Go - No go” típusú válasz-generálás

Külön vizsgáltam a biometrikus rendszerek biztonságának mérési problematikáját. Kiemeltem a FAR és az FRR index hangsúlyos szerepét a rendszerek biztonságtechnikájában. Megállapítottam, hogy e szempontok szerint, a biometrikus rendszerek tekintetében az írisz- és a retina-alapú azonosítás jelenti a legmegbízhatóbb technikai megoldást.

Ezt követően egyedi szempontok alapján külön tárgyaltam a legelterjedtebb biometrikus azonosítási módszerek alkalmazási gyakorlatát. Meghatározott vizsgálati szempontjaim alapján kimutattam a biometrikus eszközök alkalmazási kockázatait. A kockázatelemzés

során kiemeltem a felhasználói környezet elsődleges szerepét és a használatra vonatkozó hajlandóság biztonsági szintet befolyásoló hatását.

Feladatorientált szempontrendszert állítottam össze a pénzintézetekben alkalmazható biometrikus azonosítási módszerek vizsgálatára. A pénzintézeti körülmények figyelembe vételével megállapítottam, hogy a feladatnak leginkább az érhálózat (tenyér és/vagy ujj) azonosítási módszer felel meg.

Kiemelten foglalkoztam a humán infraemissziós képalkotás alkalmazhatóságával a pénzintézeti környezetben. Jogtörténeti és technikatörténeti elemzést követően megállapítottam, hogy a hőkamerák használata a biztonságtechnikában nagyon kívánatos, a biztonsági kockázatokat - egy jól megválasztott, tervezett és kivitelezett rendszer esetén – ezek a módszerek szignifikáns módon képesek csökkenteni.

A bankszektor regnáló biometrikus alapú biztonsági rendszerei közül az ujjnyomat, érhálózat alapú azonosítás gyakorlati tapasztalatait vetettem vizsgálat alá. Megállapítottam, hogy a bankbiztonsági szempontokat figyelembe vevő sérülékenységi vizsgálatok összeegyeztethetők az általános, lehetséges információvédelmi támadási felületekkel. Ennek értelmében lehetséges támadási felületnek számítanak az olvasó terminál és az azt vezérlő számítógépet összekötő kommunikációs csatornák, valamint a tárolt mintázatokat tartalmazó adatbázisok is. További biztonsági rést jelentenek a különböző kommunikációs csatornák. Ezek védelme tehát kiemelt biztonsági feladat.

Egyedi, specifikált vizsgálatot végeztem a bankbiztonsági szempontokat figyelembe vevő infravörös sugárzási mérések terén. Ennek során megállapítottam, hogy a felhasznált, legérzékenyebb infravörös kamerák sem alkalmasak (egyelőre) - még laboratóriumi körülmények között sem - a feltételezéseimben megfogalmazott kimutatásokra. Ennek oka elsősorban a ruházat árnyékoló hatásában keresendő. Amennyiben ezt a jövőben sikerül kiiktatni, illetőleg a hőkamerák is további fejlődési szakaszon mennek keresztül, akkor az elképzeléseim megvalósíthatósága reális közelségbe kerülhet.

5. PARADIGMAVÁLTÁS A PÉNZINTÉZETEK AKTÍV VÉDELMÉBEN[1]

Hazánkat a pénzintézetek sérelmére elkövetett rablások tekintetében az EBF (European Bank Federation) a legbiztonságosabb országok közé sorolja. Mindennek ellenére nem túlzás kijelentenünk, hogy kereskedelmi bankjaink, takarékszövetkezeteink csaknem állandó célpontjaivá váltak az életet, testi épséget veszélyeztető fegyveres támadásoknak, támadási kísérleteknek.

Az aktív beavatkozás eszközei között említhető a felcsapódó redőnyök alkalmazása, az ajtók, pénztároló eszközöknek a támadásjelzés következtében történő automatikus lezárása, a ködgenerátor (füstágyú) célirányos telepítése. A fejezet ezen utóbbi használata során generálódó reakciókat rendszerezi és elemzi az áldozat, az elkövetői és a passzív résztvevő oldaláról is.

2008-ban összesen 22 támadást követtek el magyarországi pénzintézetek ellen. Az EBF ebben az évben kiadott statisztikái alapján a rablási kockázati mutató Magyarországon 1/379 (minden 379 fiók közül egyet ért támadás az adott év alatt). A legmagasabb a rablási kockázat Olaszországban (1/9), míg 1/14 Csehországban és Görögországban és 1/29 Dániában. Norvégiában, Finnországban, Luxemburgban, Liechtensteinben kisebb a rablási kockázat, mint nálunk, míg vannak olyan országok is, amelyek nem szolgáltatnak elemzésre alkalmas adatokat. [1]

2009 június közepéig a magyarországi pénzintézeti támadások száma elérte a 70-et,[2] [2] 2010-ben pedig már 76-ra emelkedett. A 2011-2013 évek statisztikái valamivel kedvezőbb képet mutatnak, de nem szabad megfeledkeznünk arról, hogy akár egyetlen egy fegyveres rablás is végződhet tragikusan.

[1] A fejezetben ismertetett szimulációnál és az eredmények feldolgozásánál Nagy József (PhD, pszichológus, nyá. r. alezredes) volt segítségemre.
[2] Ebben az évben került sor a rendőrségi Robotzsaru információs rendszerbe integrált, banki támadásjelző rendszer országos hatáskörű élesítésére is. Ezt szabályozza a 20/2011. (X. 07.) ORFK utasítás a támadásjelző rendszer működtetéséről.

Országos tendencia a vagyon elleni bűncselekmények számának folyamatos növekedése.[3] [3] 2014-ben a Nemzeti Dohányboltok sérelmére elkövetett rablások száma ugrásszerűen emelkedett meg. Ez egyértelműen azt jelzi, hogy nem a bűnelkövetések hajlandósága csökkent, hanem csupán áthelyeződött a gyors pénzszerzés lehetőségének tárgya a pénzintézetekről a dohányboltokra. [4] Az, hogy mikor következik be a visszarendeződés, és bekövetkezik-e egyáltalán, az függ a pénzintézetek által alkalmazott biztonságtechnikai gyakorlattól.

A bankbiztonság növelése általánosan megfogalmazott elvárás,[4] [5] mind a bankok, pénzintézetek, mind pedig a biztonságot szavatoló cégek irányába. Újabb és újabb biztonságtechnikai eszközök, berendezések és megoldások látnak napvilágot úgy külföldön, mint pedig hazánkban.

A szemléletváltás a bankbiztonság területén kiterjed mind az eszközökre, mind a mentalitásra. [6] A hagyományos biztonsági kérdéseknél alapvetően a dokumentálás, a jelzés és a behatolás megakadályozása kapták a főszerepet. Az új szemlélet megítélésem szerint elsősorban azt tükrözi, hogy aktívan kell részt venni az események alakításában.

5.1. A ködgenerátor (füstágyú) alkalmazásának lehetősége

A ködgenerátor (füstágyú) olyan eszköz, amely rövid idő alatt nagymennyiségű, átláthatatlan (ködszerű), a levegővel megegyező sűrűségű (tehát levegőben egyenletes eloszlású) anyagot lövell ki a telepítés helyszínén. Az elkövető behatolását követően a riasztóval ellátott berendezés azonnal aktiválja a készülék védelmi rendszerét, a ködgenerátor (füstágyú) működésbe lép. 10 másodperc elteltével a védendő területet átláthatatlan köd lepi el, ami bárki számára lehetetlenné teszi a tájékozódást, ezzel gyakorlatilag megakadályozva a rablás sikeres végrehajtását.

A ködgenerátor (füstágyú) alkalmazásával pénzintézetekben nem, viszont pl. ékszerboltok, raktárok, trezorok esetében jóval gyakrabban találkozhatunk. Annak eldöntése, hogy az eszköz alkalmazása hatékony és egyben biztonságos is a pénzintézetek tekintetében általánosan alapos vizsgálatokat igényel.

---

[3] ENYÜBS: Egységes nyomozóhatósági és ügyészségi bűnügyi statisztika

[4] Elek József, az International Bodyguard Association (IBA) magyarországi képviseletének igazgatója az Üzletihírszerzés.hu-nak nyilatkozva mondta el az alábbiakat: „Az évek óta tartó ígéreteket - miszerint egységes bankbiztonsági előírás szükséges - végre valóra kellene váltani. A magyar gyakorlat ugyanis még mindig az, hogy az adott pénzintézetek hoznak meg olyan, a biztonságot szabályozó döntéseket, amelyek a védelemért felelős szakemberek feladata lenne."

A berendezés technikai leírása ismerteti, hogy az alkalmazás milyen feltételek mellett garantálja a „hatáskörzetében” tartózkodók fizikai biztonságát. A fizikai biztonság garanciája mellett azonban rendkívül fontos tényező annak vizsgálata, hogy a berendezés milyen pszichés hatást vált ki azokban, akiket működése során érint.

A vizsgálatokat 2009-ben egy alapkutatás keretében kezdtem, majd 2013-ban aktualizálva 2014-ben jutottam el publikálható következtetések levonásáig.

5.1.1. A hatásvizsgálat célja és célcsoportjai

A hatásvizsgálatok során alapvető célkitűzés volt annak megállapítása, hogy a ködgenerátor (füstágyú) alkalmazásával milyen hatások érik azokat, akik vele kapcsolatba kerülnek és ez milyen pszichikai, fizikai, biológiai változásokhoz vezet. [7]

Különösen és részletesen vizsgáltam, elemeztem, hogy az ügyféltérben tartózkodó vétlen személyek (banki alkalmazottak, vagyonőrök, fegyveres biztonsági őrök, ügyfelek és kísérőik), valamit az elkövetők vonatkozásában:

- Milyen mértékű az általuk átélt pszichés stressz? Az nagyobb mértékű-e a ködgenerátor (füstágyú) révén, mint a fegyveres bankrablás okozta stresszreakció?
- A ködgenerátor (füstágyú) által kiváltott pszichés stressz mértéke eléri-e azt a határt, amikor már kóros pszicho-fiziológiai következmények alakulhatnak ki?

A ködgenerátor (füstágyú) alkalmazásának sajátossága, hogy váratlanul több olyan érzékszervi modalitás működését is korlátozza, sőt 6-8 s elteltével részben, vagy teljes egészében blokkolja is (látás, hallás, térérzékelés), ami a jelenlevőket ideiglenesen fizikailag cselekvésképtelenné teheti.

A váratlan esemény bekövetkezése és annak intenzitása extrém stressz-élményt válthat ki. [8] Ennek hatására a kognitív funkciók, helyzetfelismerés, gondolkodás, döntéshozatal, cselekvési kontroll képessége csökken, vagy teljesen megszűnik, a viselkedés ösztönvezéreltté válhat.

Ebben az állapotban - mint ahogy általában veszély esetén-, a támadó cselekvését leginkább a megküzdés vagy a menekülés jellemzi. Az is előfordulhat, hogy az élettani határ közelében mozgó szívfrekvencia miatt teljesen „lefagy” ideiglenesen működésképtelenné válik, feladja eredeti szándékát.

A banki alkalmazottak és a vagyonőrök intézkedés-lélektani, biztonságtechnikai tréningen történő felkészítésével az eszköz alkalmazásának negatív hatásai teljes mértékben kiküszöbölhetők.

Az ügyfelek, az ügyféltérben tartózkodó vétlen személyek felkészítése azonban - annak érdekében, hogy ne alakuljon ki extrém stressz-élmény egy esetleges bankrablás során történő váratlan alkalmazás során - nem megoldható. Következésképpen ugyanazok a hatások fogják érni a vétlen személyeket is, mint az elkövetőket. [9]

5.2. A hatásvizsgálat lefolytatása

Ezen fejezeten belül a hatásvizsgálatok időrendiségét, az alkalmazott szituációkat, módszereket, vizsgálati eljárásokat, személyi és technikai feltételeit, a szerepjátékkal kapcsolatos utasítások rendszerét, valamint a „fegyveres támadás" jellemzőit tárom fel.

5.2.1. A hatásvizsgálatok időrendisége

A ködgenerátor (füstágyú) pénzintézetekben és takarékszövetkezetekben történő alkalmazása során az egyes célcsoportokra kifejtett pszichikai hatásának vizsgálatára az elfogadott alapkutatási tervnek megfelelően 2009. szeptember 7-e és 11-e között került sor az Ady-ligeti Rendőr Szakközépiskola kiképző bázisán.

Ezt követően 2013. október - december hónapban többszöri szakmai munkamegbeszélés és konzultáció során újrafeldolgozásra került a korábban elkészített munkaanyag.

A szakmai anyag aktualizálását követően 2014. március 3-án a BM Nemzetközi Oktatási Központjában újabb hatásvizsgálatot végeztem, amelyre meghívást kaptak a magyarországi kereskedelmi bankok biztonsági vezetői. A hatásvizsgálat tárgya az eszköz telepítésnek sajátosságai volt.

Néhány héttel később, 2014. március 24-én újabb hatásvizsgálatot végeztem az Óbudai Egyetemen 27 fő bevonásával. A cél a kiváltott pszichés reakciók vizsgálata volt.

2014. április 8-án egy magyarországi kereskedelmi bankhálózat kijelölt bankfiókjában, teljesen reális banki körülmények között került tesztelésre a rendszer.

A vizsgálatsorozatok, valamint az azt követő utóvizsgálatok eredményeit a következőkben ismertetem.

5.2.2. A hatásvizsgálat során alkalmazott szituációk, módszerek és vizsgálati eljárások [10]

Az előre összeállított forgatókönyv alapján a kijelölt helyszíneken (fegyveres rablás 2 fő fegyveres elkövetővel) a résztvevők számára váratlan konfliktushelyzetet alakítottam ki (mintegy „szituációba" helyezve őket).

Az elkövetők arra kaptak feladatot, hogy az ügyféltérben lévő vétlen személyek, vagyonőrök, banki alkalmazottak, pénztáros megfélemlítésével, fenyegetés útján rabolják el a kasszában lévő pénzösszeget (fontos megjegyezni, hogy a szituációban résztvevő elkövetők és vétlen személyek sem tudták, hogy ködgenerátor kerül alkalmazásra).

Az elkövetők és a vétlen személyek közül kettőt-kettőt kardió-övvel láttam el, ami rögzítette a váratlan események bekövetkezése során kialakult stressz-hatás mértékét (szívfrekvencia).

A szituációt - mindaddig, amíg a szétáramló ködanyag erre lehetőséget adott -, videókamera rögzítette.

Az ügyféltérbe való behatolást követően az események alakulásától függetlenül a riasztó jelzéssel egy időben működésbe lépett a ködgenerátor (füstágyú).

Minden egyes szituáció végeztével a vizsgálatvezető és a részvevők strukturált, rögzített négyszemközti interjú keretein belül kiértékelték a történteket, majd ezt követően kérdőívet töltöttek ki (lásd: ennek a fejezetnek a végén!). [11]

5.2.3. A vizsgálatok feltételei

Személyi feltételek

A vizsgálatok személyi feltételeit ismerteti az **1. táblázat**.

Csoport / szerep	Létszáma [fő]	Korosztályi összetétel [év]	Foglakozás	Megjegyzés
Elkövetők	18	30-45	Jelenleg is aktív, illetve nyugállományú rendőrök	„Profik"
	18	19-25	Hallgató	Rendőr Szakközépiskola
Vétlen személyek I.	36	19-55	„Ügyfél"	Férfiak, nők vegyesen
Banki alkalmazottak	20	19-25	Hallgató	Rendőr Szakközépiskola

Folytatás a következő oldalon!

Csoport / szerep	Létszáma [fő]	Korosztályi összetétel [év]	Foglakozás	Megjegyzés
Vagyonőr	1	35	Vagyonőr	Minden esetben ugyanaz, külsős
Vétlen személyek II.	20-30	19-25	Hallgató	Rendőr Szakközépiskola, statiszták (nem vizsgáltam őket)

1. táblázat: A ködgenerátorral kapcsolatos vizsgálatok személyi összetétele. Egy szituációban részt vevők száma: 1 fő banki alkalmazott (pénztáros), 1 fő vagyonőr, 1-2 fő vétlen személy, 1-2 fő elkövető (mindegyikük vizsgált személy); szituációnként összesen: 4-6 fő.

Technikai feltételek

A vizsgálatok technikai feltételei a következők voltak:

- A rablások helyszínéül kialakított helyiségek. A kiképző bázison két rablásra kijelölt helyszín, egy „Postahivatal" és egy „Üzemanyagkút" került berendezésre. Mindkettőt 3 - 3 rögzített állású biztonsági kamerával és a hozzá tartozó mikrofonnal telepítettem. A ködgenerátor (füstágyú) a Postahivatalban a kiszolgáló pult, pénztárral szemben a falra, az Üzemanyagkút vonatkozásában a kiszolgáló pult, pénztár mögé, de szintén a falra került elhelyezésre.
- További technikai támogatottság, felsorolásszerűen:
  - zárt láncú kamera és videó rendszer (CCTV) a térben zajló események rögzítésére;
  - interjúk, tesztek zavartalan kitöltésre kialakított helyiségek, szükséges számú íróasztal, székekkel;
  - előre telepített ködgenerátor (helyiségenként különböző kapacitású) a hozzá tartozó egyéb berendezésekkel;
  - 3 db Polar RS 400-as pulzusmérő;
  - 1 db Notbook + Polar szoftver;
  - 1 db projektor;
  - 2 db maroklőfegyver (Simunation Glock 17 + lőszer).

5.2.4. A szerepjátékban részt vevők számára kiadott utasítások

Az egyes mozzanatok naponta 9.00, 10.30, 12.00, és 13.30 órakor (4 alkalommal) kerültek lebonyolításra. Így vált biztosítottá, hogy a különböző időpontban érkező szereplők

ne tájékozódhassanak a vizsgálatok részletei, sajátosságai felől. A helyiségek szellőzetése is közel 30 percet vett igénybe.

A szerepjátékban részt vevő csoportok tagjainak a következő utasításokat adtam ki:

- Elkövetők. A behatolást megelőzően az elkövetők vagy helyrajzvázlatról, vagy személyes bejárással felderíthették a behatolásra kijelölt helyiségeket. A rablást megelőzően tetszőleges idő állt rendelkezésükre, hogy egymás között elosszák és megbeszéljék a feladatokat. Mind a „profi" mind pedig az „amatőr" elkövetők számára kiadott instrukciók megegyezők voltak. A vizsgálatvezető, mint „megbízó", a következő instrukciókkal látta el az „elkövetőket": „*Jelenleg nagy mennyiségű készpénz van a kasszában. A feladat az, hogy azt megszerezzék. Kapnak marokfegyvert, amit használhatnak. Hatoljanak be és mindenkit parancsoljatok a földre. Váratlan esemény esetén tegyenek szabadon, saját belátásuk szerint.*"
- Pénztáros. A pénztáros, mint felkészített alkalmazott tisztában volt a ködgenerátor (füstágyú) alkalmazásának sajátosságaival. „*Ön jelenleg ennek a postahivatalnak (üzemanyagkútnak) az alkalmazottja. Most a napi ügymenetnek megfelelően zajlik az élet. Vásárlók érkeznek és távoznak, nézelődnek, vásárolnak, Ön pedig kérésüknek megfelelően kiszolgálja őket. Kérem, viselkedjen természetesen úgy, ahogy ezt a mindennapi életben is tenné. A helyiségben tartózkodó biztonsági személyzet végzi a saját munkáját, ezért Önnek az a dolga, hogy kizárólag a vendégekre, ügyfelekre figyeljen.*"
- Fegyveres vagyonőr. A fegyveres vagyonőr, mint felkészített alkalmazott tisztában volt a ködgenerátor (füstágyú) alkalmazásának sajátosságaival. „*Ön jelenleg az adott Postahivatalban (Üzemanyagkúton) lát el fegyveres szolgálatot. Feladata, hogy szavatolja a hivatal biztonságos működését az alkalmazottak és az ügyfelek testi épségét. Váratlan helyzetben, szituációban tegyen úgy, ahogy ezt a szabályzat előírja, ahogy Önt felkészítették: rablás észlelése esetén késlekedés nélkül nyomja meg a kezében lévő távirányító gombját, ami működésbe hozza a riasztóberendezést és ezzel egy időben a ködgenerátort, majd cselekedjen az adott helyzetnek megfelelően.*"
- Vétlen személyek. „*Önök jelenleg egy Postahivatalban (Üzemanyagkúton) éppen személyes ügyeiket intézik. Önökhöz hasonlóan további ügyfelek is*

lesznek a helyiségben, kérem, hogy viselkedjenek természetesen. Ha valami esemény történik, kérem, tegyenek saját belátásuk szerint."

5.2.5. A fegyveres támadás végrehajtása

A szituációra való felkészülés a helyszínek elfoglalásával, a feladatok pontosításával kezdődött. A támadók külön helyiségben kapták meg az instrukciókat, valamint a rabláshoz szükséges felszereléseket és fegyverzetet. A szituációra való felkészülést követően elindításra kerültek a pulzusmérők. Amikor a szituációban részt vevők jelezték, hogy felkészültek, a támadók jelzést kaptak arra, hogy megkezdhetik tevékenységüket.

A szituáció indítása a „*A helyiség mostantól Postahivatalként (Üzemanyag shop-ként) működik.*" mondattal történt. Ezt követően a támadók saját belátásuk szerint kezdték meg a behatolást és a rablást. Eközben a telepített videó kamerák - amíg az lehetséges volt - rögzítették a szituáció eseményeit. A szituációnak akkor volt vége, amikor az elkövetők elhagyták a terepet, vagy leállítottam azt.

A mozzanatok teljes időtartama 1-3 perc volt. A ködből a térben tartózkodókat a felkészített vagyonőr és jómagam kísértük ki. Ezt követően megtörtént a helységek átszellőztetése és a következő szituációra való felkészítése.

5.2.6. A kutatási anyag feldolgozásának folyamata

A kutatási anyag feldolgozásának alapját a kérdőívek, interjúk, pulzusmérők és a videofelvételek adatainak rendszerezése, elemzése és értékelése adta.

A kérdőívek értékelése

A vizsgálatban kétféle kérdőív eredményeit összegeztem, ezek az ún.:

1. „Elkövetői kérdőív" és
2. „Kérdőív vétlen személyek részére" (lásd: mindkettőt a fejezet végén!).

Az értékelhető „Elkövetői kérdőív"-ek száma 31 db volt. Ebből 17 fő „profi", míg 14 fő „amatőr" elkövető volt. Az eredményeket a következőkben lehet összefoglalni:

- Az elkövetők közül két fő válaszolt úgy, hogy tevékenységüket nem gondolták át a behatolás megelőzően, mintegy ad-hock cselekedtek.
- A ködanyag kiáramlása mindenkit váratlanul ért.
- A válaszadók úgy ítélték meg, hogy a köd közepes vagy annál kissé nagyobb mértékben befolyásolja tevékenységüket (egytől tízig terjedő skálán 6-os átlag).

- A kiáramló köd leginkább a látást és a térérzékelést csökkentette jelentős mértékben (szubjektív megítélésük alapján az egytől tízig terjedő skálán a látáscsökkenés 8,4-es átlagú, ami azt jelenti, hogy jelentős mértékben befolyásolta a köd a látást, míg a térérzékelés elvesztése 6,6-os átlag, közepes mértékűnél erősebb befolyásoltságot jelent).
- Az „Elkövetők" 73 % lenne olyan pénzintézetnek az ügyfele, ahol alkalmazzák a ködgenerátort (füstágyút), mint biztonságtechnikai eszközt.

Az értékelhető „Kérdőív vétlen személyek részére" száma 38 db volt. A kapott eredmény részleteiben:

- A megkérdezettek 79 %-a felkészült arra, hogy támadás fogja érni (tehát a résztvevők 21 %-át viszont teljesen váratlanul érte a fizikai támadás).
- A ködanyag kiáramlása 94 %-ban volt váratlan esemény.
- Az egytől tízig terjedő skálán 7,8-es átlaggal úgy ítélték meg, hogy a köd jelentős mértékben befolyásolja tevékenységüket.
- A kiáramló ködanyag leginkább a látást és a térérzékelést érintette. Szubjektív megítélésük alapján az egytől tízig terjedő skálán a látáscsökkenés 8-as (tehát jelentős mértékben befolyásolta a köd a látást), míg a térérzékelés elvesztése 6,65-os átlagú (közepesnél erősebb mértékű befolyásoltság).
- A „Vétlen személyek" 66 % lenne olyan pénzintézetnek az ügyfele, ahol alkalmazzák a ködgenerátor (füstágyú), mint biztonságtechnikai eszközt.

Összegzésképpen megállapítható, hogy az eszköz alkalmazásának tekintetében ez elkövetők és a vétlen személyek szubjektív megítélése csaknem azonos. A megkérdezettek kétharmada úgy ítéli meg, hogy az eszköznek helye van a pénzintézetekben, mint biztonságtechnikai berendezésnek.

Az interjúk értékelése

A hatásvizsgálat során összesen 70 fővel készítettem értékelhető, strukturált, négyszemközti interjút. Az elkészített interjúkat tartalom alapján elemeztem a következő szempontok figyelembevételével: a „ködgenerátor (füstágyú)" által a(z)

- elkövetőkben leggyakrabban kiváltott reakciók és érzések, valamint
- vétlen személyekben leggyakrabban kiváltott reakciók és érzések.

Az elkövetőkben leggyakrabban kiváltott reakciók

Elemezve a ködgenerátor elkövetőkre kifejtett hatását megállapítható, hogy a kiváltott reakciók nyolc jól elkülöníthető csoportba sorolhatók, nevezetesen:

1. Fokozott szenzitivitás, kiéleződés, az egymásra figyelés és a szituáció feletti kontroll.
2. Kognitív funkciók hanyatlása, cselekvőképesség romlása, blokk.
3. Feladás, a helyzetből való kilépés, illetve annak gondolata.
4. „Támadás-várás", felkészülés ellentámadásra.
5. Fokozott biztonságra törekvés, a helyszín elhagyása.
6. A cselekvés felgyorsulása.
7. Indulat és enyhe fokú agresszió.
8. Elbagatellizálás, mint „*én*védő" mechanizmus.

Egyértelműen megállapítható, hogy az elkövetők által adott reakciók több mint 63 %-a a biztonsági szükséglet kielégítésére irányul, míg mindösszesen az adott reakciók nem egészen 6 %-át jellemzi az indulatosság.

Az elkövetőkben leggyakrabban kiváltott érzések

A ködgenerátor (füstágyú) elkövetőkre kifejtett hatását tovább vizsgálva megállapítható, hogy a működés által kiváltott érzések is nyolc jól megfogalmazható csoportot képeznek, ezek:

1. Meglepődöttség, váratlanság, megdöbbenés.
2. Bizonytalanság, zavartság, kiszámíthatatlanság.
3. Fokozott feszültség, izgalom, aggodalom.
4. Ijedtség.
5. A félelem különböző formái (ellentámadástól, ködtől).
6. Rövid idejű pánik, vagy pánikszerű érzés.
7. Bezártság.
8. Bosszú.

Érdekesség, hogy támadó jellegű, a vétlen személyeket veszélyeztető érzések (bosszú) százalékban kifejezett nagysága az összes megélt érzéseknek mindössze 2 %-a.

A vétlen személyekben leggyakrabban kiváltott reakciók

A vétlen személyek körében leginkább megjelenő reakciók négy elkülöníthető kategóriába sorolhatók, ezek:

1. Fizikai cselekvésképtelenség (42 %).
2. Fokozott figyelem és a menekülési lehetőségek feltérképezése (30 %).
3. Önvédelem (14,5 %).
4. Óvatosság (14,5 %).

Hasonlóság az elkövetők mutatott reakcióihoz az, hogy a reakciók közel 60 %-a a biztonságszükséglet kielégítéséből fakad.

A vétlen személyekben leggyakrabban kiváltott érzések

A technikai berendezés által kiváltott érzések a fentieknél sokkal szerteágazóbbak. Tizenegy jól elkülöníthető kategóriába sorolhatók, úgymint:

1. Félelem (lövéstől, bent rekedéstől).
2. Nyugodtság.
3. Meglepődöttség.
4. Zavartság.
5. Ijedtség.
6. Bizonytalanság.
7. Kíváncsiság.
8. Izgalom.
9. Pánik.
10. Rossz (kellemetlen) érzés.
11. Kiszolgáltatottság.

Az értékelés szempontjából döntő jelentőségű, hogy a technikai berendezés működése során érintett vétlen személyek körében kialakuló érzések közel 28 %-a a félelem és a pánik volt együttesen. Ezzel szemben a más jellegű érzések - meglepődöttség, zavartság, ijedség, bizonytalanság, kíváncsiság, stb. - 72 %-t tettek ki.

Következtetésképpen megállapítható, hogy a kiváltott érzések egyharmada a félelem, míg kétharmada más jellegű érzések (köztük 16 % a megnyugvás) a második leggyakrabban megnyilvánuló érzelmi reakció.

A pulzusmérők adatainak értékelése

A kutatás során Polar RS 400-as pulzusmérő készülékeket alkalmaztam. A pulzusszám emelkedése jól tükrözi a kiváltott és átélt stressz mértékét. A vizsgálatok során 51 személy (24 fő elkövető és 27 fő vétlen személy) pulzusszámát rögzítettem különböző szituációkban.

Az adatok értékelésekor a következő megállapításokra jutottam:

- A vizsgált állománykategóriák kiinduló pulzusszáma a pulzusmérők felhelyezésekor csaknem megegyező volt. A vizsgált személyek ekkor már tisztában voltak feladatukkal. A feladat végrehajtása során kialakult izgalom és vélhetően a ködgenerátor (füstágyú) alkalmazásának váratlansága inkább az elkövetőknél okozott nagyobb stressz-hatást.
- Az elkövetők vonatkozásában a megemelkedett átlagos pulzusszám 160 volt. Ez jelentős emelkedés, viszont az ő esetükben ez még nem jelent extrém stresszt.
- A videofelvételekkel való összevetés alapján a viselkedéskontroll folyamatosan megtartott volt.
- A vétlen személyek, ügyfelek vonatkozásában az átlagértékek csúcsértékei 130 körül mozogtak. A közel 100-as átlag pulzusszámhoz képes az emelkedés nem tekinthető számottevőnek.

Összességében megállapítható, hogy a vizsgált populáció vonatkozásában sem az elkövetői oldalon, sem pedig az ügyfelek részéről nem alakult ki extrém stressz. Az egyéni, négyszemközti interjúk tapasztalatai is megerősítik, hogy mindkét csoport részéről a viselkedéskontroll megtartott volt.

A ködgenerátor által kiváltott pszichés stressz a vizsgálatban résztvevő vétlen személyek körében nem volt olyan mértékű, hogy az kóros pszicho-fiziológiai következményekhez vezethetett volna.

A videofelvételek értékelése

A videofelvételek összefoglaló paraméterei a következők voltak:

- kutatási napok száma: 5,
- mozzanatok száma naponta: 4,
- mozzanatok száma a kutatás során: 20,
- kameraállások száma naponta, mozzanatonként: 14,
- rögzített felvételek száma összesen: 70.

A videofelvételek tapasztalatainak összegzése:

- Úgy a profi, mint az amatőr elkövetők csakis és kizárólag figyelmeztetés, pszichikai ráhatás céljából használták fegyverüket, emberre célzott lövést az élet kioltásának céljából nem adtak le.

- Fizikai erőszak alkalmazását három esetben regisztráltam. Két esetben a vétlen személyek részéről ellenszegülés volt tapasztalható, míg egy esetben az elkövető részéről látszólag indokolatlan volt az erőszak alkalmazása (vélhetően a magas stressz élmény hatására az elkövető mintegy „kimozogta magából" a feszültséget).
- A mozzanatok során az élet kioltásával való fenyegetőzés két esetben volt tapasztalható.
- Túszejtésre nem került sor, az elkövetők minden esetben elhagyták a cselekmény helyszínét, nem rekedtek az ügyféltérben.
- A pénzintézet elleni tízszeri támadás során az elkövetők 3 esetben jutottak el a trezorig.
- Az elkövetők 20 mozzanatból 6 esetben teljesen elálltak eredeti szándékuktól és elmenekültek a helyszínről.
- A mozzanatok során a vétlen személyek minden esetben eleget tettek az elkövetők utasításainak.
- Aktív ellenszegülés, ellentámadás egy esetben sem volt tapasztalható. Két esetben fordult elő passzív ellenállás a pénztárosok részéről (egy esetben nem „pakolta" a pénzt, míg egy másik esetben nem találta a trezor kulcsát).
- Pánik egyetlen vétlen személy vonatkozásában sem alakult ki. 1 fő esetében tapasztaltam nagyfokú ijedtséget, de a viselkedéskontroll az ő esetében is megtartott volt.
- A vétlen személyek pontosan az elkövetők utasításai alapján cselekedtek, elfogadva helyzeti előnyüket és domináns viselkedésüket.

5.2.7. A hatásvizsgálat eredményeinek összefoglalása

A lefolytatott vizsgálatsorozat eredményeit alapul véve megállapítható, hogy:

1. A rövid idő alatt váratlanul kiáramló nagymennyiségű ködanyag az elkövetők körében meglepődöttséget, zavart okoz, ami pillanatnyi megtorpanást, a cselekvőképesség csökkenését eredményezi.
2. A ködanyag néhány másodperc alatt jelentős mértékben csökkenti a látás-, és a térben való orientáció képességét, ami tovább fokozza a kialakult stressz mértékét.

3. Mindezeknek köszönhetően az elkövetők figyelme elsősorban egymásra, valamint a helyiség mielőbbi biztonságos elhagyására, a menekülési útvonal biztosítására irányul.
4. A ködgenerátor (füstágyú) működése által a vétlen személyek körében kiváltott pszichés stressz nagysága általában nem éri el az extrém stressz-hatás mértékét. Az értékelés szempontjából döntő jelentőségű, hogy a vétlen személyek körében kialakuló érzések egyharmada a félelem, míg kétharmada más jellegű érzések - meglepődöttség, zavartság, ijedség, bizonytalanság, kíváncsiság -, köztük a köd kiváltotta megnyugvás, a második leggyakrabban megnyilvánuló érzelmi reakció. [12]
5. Az akció közben folyamatosan kiáramló és erősödő köd anticipált félelmeket[5] generál. Az így kialakult komplex stressz élmény a testi épség veszélyeztetettsége miatt inkább a biztonság megőrzésére, a menekülésre, mintsem a megküzdésre készteti az elkövetőket. [13]

5.3. Az 5. fejezet összefoglalása

A kutatás eredményeit alapul véve elmondható, hogy a ködgenerátor (füstágyú) körültekintő és szakszerű alkalmazása lehetőséget nyújthat pénzintézetek, pénztárak, kasszák és más nagy értekkel bíró üzletek elleni támadások elhárítására, megszakítására a térben tartózkodó vétlen személyek biztonságának fenntartása mellett.

Ugyanakkor teljes mértékben nem zárható ki annak lehetősége, hogy az eszköz alkalmazása - úgy az elkövetőkben, mint a vétlen személyek körében - nem várt reakciókat, pszichoszomatikus tüneteket váltson ki. Ennek vizsgálata tehát további kísérletek, témaspecifikus szituatív elemeket tartalmazó szituációk hatásmechanizmusainak elemzési feladata. [14]

Ezen kísérleti szituációk lebonyolítása során elengedhetetlen szakértői támogatás igénybevétele. A biztonságtechnikai szakértők mellett azonban - az elsődleges kísérleti körülmények generálta pszichés tünetek tapasztalatai alapján - szükséges pszichológus, pszichiáter, klinikai szakpszichológus bevonása is a folyamatba.

[5] Vannak veleszületett félelmek. Ezek a születést követően azonnal jelentkezhetnek, létrejöttükhöz nincs szükség előzetes tapasztalásra, azaz kognitív elaborációra és az eseménnyel egy időben azonnal fellépnek. Ilyenek a hangos zajokra, fájdalomra, hirtelen zuhanásra, váratlan mozgásra jelentkező félelmek. Köztudott, hogy gyermekkorban a félelmek fejlődésen mennek át. Bizonyos félelmek megjelennek, majd elmúlnak és a helyükbe újabbak lépnek. Ezek a korspecifikus, azaz az adott életkorra jellemző félelmek.

Az általam lebonyolított kísérletsorral bizonyítottam, hogy az aktív bankbiztonsági eszközrendszer alapvető és hatékony eleme lehet a ködgenerátor. Ugyanakkor a technikai paramétereknek való megfelelés nem elegendő az eszköz általános alkalmazásának bevezetéséhez. Az eszközzel való érintkezés humánkockázata, mind elkövetői, mind vétlen oldalról további, mélyebb pszichoszomatikus szintet érintő vizsgálatokat követel meg.

Tisztelt Válaszadó[6]!

A következőkben arra szeretnénk felkérni, hogy az alábbi egyszerű kérdőív kitöltésével legyen segítségünkre a látott eljárás hatékonyságának felmérésében. A látottak és tapasztaltak alapján kérjük, név nélkül, őszintén és befolyásmentesen válaszolja meg a következő kérdéseket! Válaszait köszönjük!

1. **A következő 0-tól 10-ig terjedő skálán kérem, jelölje meg, hogy milyen mértékben változtatta meg a hatás az Ön** (egyáltalán nem = 1, közepesen = 4…6, nagymértékben = 10)**:**

Látás:	0	1	2	3	4	5	6	7	8	9	10
Tájékozódási képesség:	0	1	2	3	4	5	6	7	8	9	10

2. **A következő 0-tól 10-ig terjedő skálán kérem, jelölje meg, hogy milyen mértékű volt Önben a** (nem tapasztaltam = 0, erősen éreztem = 10)**:**

Meglepődöttség:	0	1	2	3	4	5	6	7	8	9	10
Ijedtség:	0	1	2	3	4	5	6	7	8	9	10
Félelem:	0	1	2	3	4	5	6	7	8	9	10
Pánik:	0	1	2	3	4	5	6	7	8	9	10

3. **Alkalmasnak tartja Ön az alkalmazott biztonságtechnikai berendezést arra, hogy bankokban és pénzintézetekben alkalmazzák?**

Egyértelműen igen: X
Módosításokkal igen: X
Nem igazán: X
Egyértelműen nem: X

4. **Vannak-e aggályai, kifogásai a berendezés alkalmazását illetően, ha igen kérem, fogalmazza meg őket!**

……
……

5. **Kérem, fogalmazza meg pozitív észrevételeit, javaslatait a berendezés alkalmazását illetően!**

……
……

[6] „Vétlen személyek” kérdőíve

Tisztelt Válaszadó[7]!

Az alábbiakban felteszünk Önnek néhány kérdést. Lesz, amelyekre **igen**nel vagy **nem**mel (aláhúzással vagy bekarikázással) lehet válaszolni, de lesznek olyan kérdések is melyek ún. „**kifejtős**ek". Kérjük őszintén és befolyásmentesen válaszoljon. Válaszait köszönjük!

1. **Még a szituáció megkezdését megelőzően átgondolta, hogy mit és hogyan fog cselekedni?**
   Igen Nem

2. **Váratlanul érte a köd kiáramlása?**
   Igen Nem

3. **Egytől tízig terjedő skálán kérem, jelölje, hogy a köd kiáramlása milyen mértékben befolyásolta az Ön tevékenységét** (egyáltalán nem = 1, közepesen = 4…6, nagymértékben = 10)**?**
   1 2 3 4 5 6 7 8 9 10

4. **A köd megjelenésekor mire figyelt leginkább?**

……
……
……

5. **Kérem, írja le azokat az érzéseket, amelyek leginkább jellemezték az Ön állapotát a ködgenerátor (füstágyú) alkalmazásakor és azt követően!**

……
……
……

6. **Milyen mértékben korlátozta különböző érzékszerveit a kiáramló ködanyag** (egyáltalán nem = 1, közepesen = 4…6, nagymértékben = 10)**?**

Látás:	1	2	3	4	5	6	7	8	9	10
Hallás:	1	2	3	4	5	6	7	8	9	10
Térérzékelés:	1	2	3	4	5	6	7	8	9	10

7. **Lenne Ön egy olyan pénzintézetnek az ügyfele, ahol ködgenerátort (füstágyút), mint biztonságtechnikai rendszert üzemeltetnek.**
   Igen Nem

8. **Kérjük, mondja el véleményét a ködgenerátor (füstágyú) alkalmazását illetően!**

……
……
……

[7] „Elkövetők" kérdőíve

A KUTATÓMUNKA ÖSSZEGZÉSE

Kutatásomban történeti meghatározását adtam a magyarországi pénzintézeti, és konkrétan a pénzintézeti biztonság fogalmának. Áttekintettem a mai magyar pénzintézeti biztonság rendszerelemeit, jellemző működési metódusait és rávilágítottam ezek gyengeségeire.

Kifejtettem a technikai eszköz-innovációs folyamat szükségességét. Ennek során rámutattam a bankszektor biztonságfogalmának átalakulására, melyben a pénzintézetek aktív védelmének paradigmaváltását elsődleges fontossággal emeltem ki.

Elemeztem a magyarországi pénzintézetek működési biztonságának szignifikáns jellemzőit, melyben felvázoltam a folyamatos átalakulás elemeit a védekezés módszerei és eszközei tekintetében. Kiemeltem a magyarországi sajátosságok közül a speciálisan, bűncselekmény-specifikus prevenciós megoldások alkalmazásának gyakorlatát, amely az új, erőszakos jellegű deliktumok megjelenésével biztonságtechnikailag egyértelműen kiegészítésre szorul.

Rámutattam, hogy a bankbiztonsági szabályzók egységesítésére kell törekedni, amelyben az egységes szabályozási elvek, törvények, jogszabályi alapvetések jelentik az első lépcsőt.

Elemeztem a pénzintézetek kárára elkövetett jellemző bűncselekményeket és elkövetési módokat. Mindezek alapján meghatároztam a fő biztonságpolitikai célterületeket, melyek: a pénzintézetek technikai védelme, benne az eszköz-innovációs elemek és emellett az élőerős őrzés előírásai, feladatai.

Megállapítottam, hogy szükséges a védelmi koncepció terén is paradigmaváltást végrehajtani, mivel a társadalmi folyamatok generálta bűncselekményi, bűnözői átstrukturálódás az elkövetési módokat, és az elkövetés eszközét és a támadott értékeket is átalakította. A banki szektor biztonságpolitikájában elsődlegessé kell válnia az aktív biztonsági eszközök alkalmazásának. A jelenleg rendelkezésre álló, ismert fizikai beavatkozó eszközök mellett a biztonságtechnika eszközrendszerében meg kell jelenni a bűncselekmény folyamatába történő beavatkozást elősegítő, elvégző eszközöknek.

Új tudományos eredmények (tézisek)

1. **tézis: A pénzintézetekben optimálisan alkalmazható biometrikus azonosítási módszerek kiválasztására megadható feladatorientált szempontrendszer.**
   Az első tézishez: ezt kidolgozva megállapítottam, hogy a biometrikus azonosítási módszerek közül, a pénzintézeti körülményeket figyelembe véve leginkább az érhálózat (tenyér és/vagy ujj) alapú módszer alkalmazható. Ez az egyedüli módszer ugyanis, amely szigorúan belső biometrikus azonosítót használ, az eltulajdoníthatóságot, másolást szinte lehetetlenné teszi, a minta gyermekkortól stabil, időintervallum tekintetében változásmentes, a biometrikus adat beolvasása után a válasz másodpercekben mérhető. A felhasználói oldal tekintetében ez az érintés nélküli technológia teljes mértékben elfogadott. Idegen, hamis minta bevitele teljesen kizárt.
2. **tézis: A jelenleg forgalomban lévő infravörös kamerák (hőkamerák) közül egy sem alkalmas a dinamikus testhőváltozás detektálására valóságos körülmények között, azaz ruházatot viselő ember esetében.**
   A második tézishez: ennek igazolására egyedi, specifikált méréseket végeztem a pénzintézeti biztonsági szempontokat figyelembe vevő infravörös sugárzási mérések terén. Ennek során vizsgáltam az emberi testet, mint infravörös-sugárforrás (hőkibocsátó anyag) detektálásának lehetőségét, és a rögzített kép értékelésének biztonsági szempontú felhasználhatóságát. Megállapítottam, hogy a legérzékenyebb infravörös kamerák sem alkalmasak (egyelőre) - még laboratóriumi körülmények között sem - a feltételezéseimben megfogalmazott kimutatásokra. Ennek oka elsősorban a ruházat árnyékoló hatásában keresendő. Ahhoz, hogy az elkövetésre alkalmas eszköz (fegyver) rejtett jelenléte kimutatható legyen (pl. a feltételezett elkövető ruházata alatt), az ügyféltérbe történő belépésekor még számos vizsgálat, kísérlet lefolyatatása szükséges.
3. **tézis: A ködgenerátor (füstágyú) pénzintézeti aktív beavatkozó eszközként alkalmazható.**
   A harmadik tézishez: saját kutatást, kísérletsorozatot folytattam le az innovatív, aktív biztonságtechnikai eszköz, a ködgenerátor (füstágyú) pénzintézeti környezetben történő alkalmazási metodikájára. Ugyanakkor kontrollinterjúkkal, és az alkalmazási szimuláció kiértékelésével feltártam, hogy további vizsgálatok szükségesek a humánkockázat kezelésére, különös tekintettel Magyarország ak-

tuális korfájára. Mivel a helyszínen tartózkodó vétlen személyek vonatkozásában szimulációs gyakorlatokat kell elvégezni az esetlegesen őket ért poszttraumás stressz-szindróma, illetőleg egyéb negatív pszichés hatások elkerülése érdekében.

Az általam lebonyolított kísérletsorral bizonyítottam, hogy az aktív pénzintézeti biztonsági eszközrendszer alapvető és hatékony eleme lehet a ködgenerátor. Ugyanakkor a technikai paramétereknek való megfelelés nem elegendő az eszköz általános alkalmazásának bevezetéséhez. Az eszközzel való érintkezés humánkockázata, mind elkövetői, mind vétlen oldalról további, mélyebb pszichoszomatikus szintet érintő vizsgálatokat követel meg.

A tudományos eredmények gyakorlati hasznosíthatósága

Doktori értekezésem elkészítése során megfogalmaztam olyan célokat, amelyek egyértelműen a gyakorlati hasznosíthatóságot szolgálják. Elsődleges fontosságúnak tartom a technikai eszközfejlesztést, amellyel a biztonsági szint emelhető.

1. A pénzintézetek kialakulásának történeti áttekintése, a pénzintézeteket érintő nemzetközi kitekintés, a levont következtetések és elemzések alkalmassá teszik a disszertáció oktatásban történő felhasználását, és a gyakorlatban tevékenykedők szakmai ismereteinek bővítését is. Ugyanakkor a terület „civil” érintettjeinek nagy száma, illetőleg a pénzintézettel összefüggésben elkövetett bűncselekmények civileket érintő jellege folytán társadalmi tájékoztatás alapjául is szolgálhat. Ebben tudatosítani szükséges a lakossággal a biztonsághoz fűződő aktív szemlélet fontosságát, a bűncselekményi elkövetéseket figyelembe vevő védelmi politika tudatos alakításának szükségességét és az ehhez elengedhetetlen eszközinnovációs fejlesztések megvalósítását.

2. A pénzintézeti környezet biztonságának megteremtésében kiemeltem az aktív eszközalkalmazás fontosságát. Ezen elv alapjául szolgálhat egy hatékonyabb pénzintézeti biztonsági koncepció kialakításának. Az eddigi passzív megközelítést a preventív jellegű, de aktív szemléletnek kell felváltania, amely mind az élőerő protokolljainak, mind az alkalmazott biztonságtechnikai eszközrendszer változásához is hozzájárul. Ugyanakkor az értekezés a pénzintézeti jogszabályi környezet és az egyes területek normakontrolljai tekintetében is változást generálhat.

3. Megállapításaim alapján a ködgenerátor (füstágyú) nagy hatékonyságú, pénzintézeti, aktív beavatkozó eszközként alkalmazható. Ugyanakkor a hőkamerás vizsgálatsorozat eddigi tapasztalatai szintén bevonhatók a pénzintézeti biztonsági szemléletrendszerbe.
4. Az általam személyazonosításra kidolgozott, feladatorientált szempontrendszer, a biometrikus adatok pénzintézeti alkalmazására átstrukturálhatja a pénzintézeti szektor személyazonosítási metodikáját. A fejlődés, eszköz-innováció továbbgondolásával pedig nem kizárólag a pénzintézeti jelenléttel összefüggésben válhat alkalmazhatóvá az érhálózat azonosítás, hanem az internet alapú szolgáltatások esetében is.

Javaslat a kutatás továbbfolytatására

A lefolytatott kutatásaim és levont következtetéseim alapján az alábbi területek kutatását tartom indokoltnak, időszerűnek:

1. Tovább kell folytatni a pénzintézeti aktív biztonsági eszközök terén a hőkamerával végzett vizsgálatokat. Ezek elsődleges lebonyolítása laboratóriumi körülmények között szükséges, amelyekből nyert mérési adatok pozitív értékelését követően gyakorlati közegben történő tesztelése is elengedhetetlen.
2. Folytatni szükséges a pénzintézeti aktív biztonságtechnikai eszközrendszer bővítését, ezzel egy időben szükséges a jogszabályi háttér, a speciális területi protokollok kidolgozása.
3. Elemezni kell a pénzintézetek biztonsági elemeiben bekövetkezett változások hatását a felfedett bűncselekmények elkövetési módszereire, az elkövetési magatartásokra, illetőleg azt, hogy az új, aktív biztonsági elemek milyen bűncselekményi kategória, típus elkövetésére gyakorolnak befolyást. Milyen biztonsági szintnél lehet azt mondani, hogy a ráfordított anyagi forrás már nincs összhangban a várható biztonságnövelő hatással.
4. Vizsgálni szükséges a biometrikus azonosító jegyek pénzintézeti környezetben történő alkalmazásának eszköz-specifikus szempontrendszerét és annak eredményeivel összefüggésben az ellenőrzéshez szükséges technikai és in-

formatikai feltételek, valamint eszközök és hálózatok meghatározását, fejlesztését, alakítását.

FELHASZNÁLT IRODALOM

A BEVEZETÉS-hez

[1] Christián László: A magánbiztonság megközelítésének egyes aspektusai. In: Pro Publico Bono, Magyar Közigazgatás, 2014/4., 21-30. oldalak

[2] A magánbiztonság elméleti alapjai (egyetemi jegyzet), szerk.: Christián László, NKE RTK MÖRT, NKE, Budapest, 2014.

[3] http://www.uzletihirszerzes.hu/szemely-es-vagyonvedelem/2276-vltozsra-van-szksg-a-bankbiztonsg-terletn.html, letöltve: 2015. szeptember 1.

Az 1. FEJEZET-hez

[1] Hegedűs Henrik: A biztonság fogalmának tágabb és szűkebb értelmezése, a humán-biztonság, avagy egy konferencia tanulságai; Humánstratégia a Magyar Honvédségben konferencia, 2008. február 14., Zrínyi Miklós Nemzetvédelmi Egyetem,Díszterem

[2] Vasvári Ferenc: Biztonságtudományi ismeretek, Budapest, Zrínyi Miklós Nemzet-védelmi Egyetem, 2008., 122. oldal.

[3] Dr. Hadnagy Imre József: A biztonság korszerű értelmezése - avagy a biztonság ma már sokkal bizonytalanabb, mint korábban bármikor, http://www.vedelem.hu/letoltes/tanulmany/tan135.pdf; letöltve: 2015. október 8.

[4] Gazdag Ferenc (szerk.) [2011]: Biztonsági tanulmányok - biztonságpolitika. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 83-89. oldalak

[5] A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel, In: Gaál Gyula, Hautzinger Zoltán (szerk.): Modernkori veszélyek rendészeti aspektusai, Pécsi Határőr Tudományos Közlemények, XV. Pécs, 2015, 57-64. oldalak, ISSN: 1589-1674

[6] Hilborn, R. C. (2004.): „Seagulls, butterflies, and grasshoppers: A brief history of the butterfly effect in non linear dynamics". American Journal of Physics 72, pp. 425-427; Devaney, R. L.: Introduction to Chaotic Dynamical Systems, Westview Press, 2003, ISBN 0-8133-4085-3

[7] Vasvári Ferenc, Rávai Attila, Kerek Tamás, Fodor Valéria: Kockázatelemzés I, 2003, Budapest, Honvédelmi Minisztérium, 102. oldal

[8] Szügyi György: A kockázatmenedzsment 21. századi sajátosságai a humán erőforrás kezelésének szempontjából, Humánpolitikai Szemle, 18. évf. 9. sz. /2007, 11-26. oldalak

[9] Péczeli Anna: A humán biztonság elmélete és gyakorlata Kanada és Japán példáján, Grótius, 2012

[10] Kiss Péter: Humánbiztonság – módszerek alkalmazása, Információbiztonság, 2008/május, 6-7. oldalak

[11] Vasvári György: A társadalmi és szervezeti (vállalati) biztonsági kultúra, Ad Librum Kiadó, 2009

[12] Lindner Sándor: Munkahelyi kockázatok kezelése munkaadói nézőpontból, Polgári Szemle, 2015. június, 11. évfolyam, 1-3. oldalak

[13] Borai Ákos: Koncepció a polgári biztonságvédelmi tevékenység szabályozására. 9. sz. előtanulmány az átfogó rendészeti stratégia társadalmi vitájához. A Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Budapest, 2008, 9-10. oldalak

[14] Szabó Lajos - Szigeti Lajos: Magánbiztonság, rendészet, rendvédelem, http://www.pecshor.hu/periodika/XII/szabszig.pdf, letöltve: 2015. október 8.

[15] Tóth Attila - Tóth Levente: Biztonságtechnika, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2014

[16] Dr. Lukács György-Gábor László (szerk.): Új Vagyonvédelmi Nagykönyv, CEDIT 2000 Kft., Budapest, 2002, ISBN 963 8180 39 0

[17] http://www.munkajog.hu/rovatok/munkahely/ujraszabalyoztak-az-uzleti-titok-es-know-how-megserteset; letöltve: 2014. március 3. http://www.ugyvedvilag.hu/rovatok/szakma/az-uzleti-titok-vedelme-es-a-kozerdeku-adatok-nyilvanossaga; letöltve: 2015. március 5.

[18] Dr. Lukács György - Dőring András - Hell Péter: Vagyonvédelmi rendszerek I., ÓE-KVK, Budapest, 2015

[19] Az üzleti hírszerzés és az ipari kémkedés Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság-, és Társadalomtudományi Kar Információ-, és Tudásmenedzsment Tanszék Biztonságmenedzsment kutató csoport, Készítette: Erdősi Péter, CISA 2005

[20] Fülöp Gyula: Stratégiai menedzsment, Elmélet és gyakorlat, Perfekt Kiadó, 2008

[21] Szövényi György: Biztonságvédelmi kézikönyv, Budapest, KJK-Kerszöv, 2000

[22] ENYÜBS (Egységes nyomozóhatósági és ügyészségi bűnügyi statisztika); http://crimestat.b-m.hu/Default.aspx, letöltve: 2015. szeptember 10.

[23] 2005. évi CXXXIII. törvény; 2013. évi L. törvény; 2013. évi V. törvény - a Polgári Törvénykönyvről

A 2. FEJEZET-hez

[1] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[2] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú melléklete

[3] Tomka Béla: A magyarországi pénzintézetek rövid története 1836-1947, Aula Kiadó, 2000

[4] Márkus Csaba: Magyar biztonságtechnika I., Fejezetek a magyar biztonságtechnika történetéből, SLV Press Kiadó 2009

[5] 20/2011. (X. 07.) ORFK utasítása a támadásjelző rendszer működtetéséről,ORFK Tájékoztató (OT), 2011/14. szám, Budapest, 2011. október 13.

[6] Havass Miklós: A számítógéptől az információs társadalomig, Informatikai Tudományok, 2003. november 24.

[7] Muha Lajos - Tóth Georgina Nóra: A bankbiztonság vizsgálata kockázatelemzéssel, Hadmérnök VI. évfolyam 4. szám, 2011.december, 204-215. oldalak

[8] Gazdag Ferenc: Biztonsági tanulmányok - Biztonságpolitika, ZMNE, Budapest, 2011, 37-46. oldalak, ISBN 978-615-5057-23-6

[9] 2013. évi CCXXXVII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról

[10] ENYÜBS Egységes nyomozóhatósági és ügyészségi bűnügyi statisztika, http://crimestat.b-m.hu/Default.aspx, letöltve: 2015. szeptember 10.
2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
22/2006.(IV.25.) BM rendelet a személy-, és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról
68/2012. (XII.14.) BMrendeleta rendészeti feladatokat ellátó személyek, a segédfelügyelők, valamint a személy- és vagyonőrök képzéséről és vizsgáztatásáról

[11] 2011. évi CXXVIII. Törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról és ennek végrehajtásáról szóló 234/2011. (XI. 10.) kormányrendelet 1. § 25. pontja

[12] Magyar Zöld könyv, 2005. november 17., www.vedelem.hu

[13] Amszterdami Szerződés (az európai integráció alapvető szerződéseinek egyike, amit 1997. október 2-án írtak alá, és 1999. május elsején lépett hatályba), aminek folytatásaként aztán a tagállamok közötti bűnmegelőzési célú együttműködést erősítendő, az EU Tanácsa 2001. május 28-án határozatot fogadott el az Európai Bűnmegelőzési Hálózat felállításáról

[14] Dénes Tamás: Kódolatlan gondolatok eVilág, III.évfolyam, 9.szám, 2004. szeptember

[15] Twitchell, D. P.: Social and Organizational Liabilities in Information, Security, Illionis State University, 2009

[16] Váczi Dániel: A bankok speciális támadási felülete (The bank's special attack surface Social engineering), szakdolgozat az Óbudai Egyetemen, 2012

[17] MNB 34. Módszertani segédlet,https://www.mnb.hu/; letöltve: 2014. október 11.

[18] Tóth Attila - Tóth Levente: Biztonságtechnika,Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2014

[19] Dr. Lukács György - Dőring András - Hell Péter: Vagyonvédelmi rendszerek I., ÓE-KVK, Budapest, 2015

[20] Kovács Tibor: Egy elképzelt bankfiók elektronikai védelmének megtervezése, 6. Nemzetközi Mechatronikai és Biztonságtechnikai Szimpózium, Budapesti Műszaki Főiskola, 2006. november 10, CD ISBN 978-963-7154-59-1

[21] Tóth Attila - Tóth Levente: Biztonságtechnika Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2014

[22] Tóth Attila - Tóth Levente: Biztonságtechnika Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2014

[23] Dr. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései c. PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009

[24] Dr. Lukács György - Dőring András - Hell Péter: Vagyonvédelmi rendszerek I., ÓE-KVK, Budapest, 2015

[25] Tóth Attila - Tóth Levente: Biztonságtechnika Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014

[26] Tóth Attila - Tóth Levente: Biztonságtechnika,Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014

[27] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
22/2006.(IV.25.) BM rendelet a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység
27/1998. (VI. 10.) BM rendelet a fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról
1997. évi CLIX. Törvény a fegyveres biztonsági őrségről

[28] Dr. Görög Mihály: Bevezetés a Projekt Menedzsmentbe, Aula Kiadó, Budapest, 2001

[29] MNB tanulmányok, http://www.mnb.hu/kiadvanyok/elemzesek-tanulmanyok-statisztikak/mnb-tanulmanyok, letöltve: 2015. november 10.

[30] Kovács Levente: „Az európai pénz-, és elszámolás-forgalom jövője", szakkönyv, lektor: Kocziszky György, Kiadó: Miskolci Egyetem, 2010, 148. oldal; ISBN: 978-963-661-945-9

[31] A Kormány 1035/2012. (II. 21.) Korm. Határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 28-38. oldalak

[32] Dr. Szelid Zoltán: Lehetséges rendkívüli események és ennek kezelése a védett objektumon belül, NSZFI Budapest 2008.

[33] 2012. évi C. törvény a Büntető Törvénykönyvről

[34] 15/2013. ORFK utasítás az általános rendőrségi feladatok ellátására létrehozott szerv ügyeleti szolgálata és a közreműködésével teljesítendő jelentési és tájékoztatási kötelezettség rendjéről

[35] 20/2011. (X. 07.) ORFK utasítása a támadásjelző rendszer működtetéséről, ORFK Tájékoztató (OT) 2011/14. szám, Budapest, 2011. október 13.

[36] Sík Zoltán Nándor: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában
http://old.ivsz.hu/resource.aspx?ResourceID=GetDocStoreFile&EntryID=3353; letöltve: 2013. december 17.
Vígvári András: Pénzügy(rendszer)tan, Akadémiai Kiadó, Budapest, 2009, ISBN 978-963-05-8595-8

[37] Dr. Haig Zsolt - Dr. Kovács László: Fenyegetések a cybertérből
http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=57; letöltve: 2013. december 17.

[38] Dr. Kovács László - Dr. Krasznay Csaba: Digitális Mohács - kibertámadási forgatókönyv Magyarország ellen
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csabadigitalis_mohacs_.pdf, letöltve: 2013. december 10.

[39] Sík Zoltán Nándor: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában

http://old.ivsz.hu/resource.aspx?ResourceID=GetDocStoreFile&EntryID=3353; letöltve: 2013. december 17.

[40] Nagy Rudolf: A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása, PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem Hadmérnöki Doktori Iskola, 2011

[41] Kónya Tamás: Nagy megbízhatóságú elektronikus rendszerek elmélete, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2007

[42] IT Alapismeretek, Informatikai és Hírközlési Minisztérium, www.ihm.gov.hu, letöltve: 2015.október 10.

[43] Pádár Péter: Üzletmenet folytonosság menedzsment http://www.szintezis.hu/upload/bcm_uwe4-0_termekismerteto.pdf, letöltve: 2015.október 15.

[44] Az informatikai biztonság kézikönyve, szerkesztette: Muha Lajos, Verlag Dashöfer Szakkiadó, 2007

[45] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: A KIB 25. számú ajánlása 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió, Miniszterelnöki Hivatal, 2008
Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Miniszterelnöki Hivatal, 2008

A 3. FEJEZET-hez

[1] ENYÜBS Egységes nyomozóhatósági és ügyészségi bűnügyi statisztika. http://crimestat.b-m.hu/Default.aspx, letöltve: 2015. szeptember 10., http://www.police.hu/

[2] Betöréses lopás-, és rablásbiztosítás technikai feltételei (AJÁNLÁS), (telephelyek és létesítmények, helyiségek őrzésének, vagyontárgyak tárolásának, szállításának szabályai), Módosítva: Budapest, 2015. április 24., http://www.pluto.hu/_A/A2.html, letöltve: 2015. november 17.

[3] Kovács Tibor - Milák István - Otti Csaba: A biztonságtudomány biometriaiaspektusai, http://www.pecshor.hu/periodika/XIII/kovacsti.pdf

[4] MEB 2014 - 12th International Conference on Management, Enterprise and Benchmarking, Budapest, Hungary, 2014.május 30-31. - Őszi Arnold: Az e-kereskedelem elvárásai a biometriával szemben - Magyar nyelvű konferencia előadás, konferencia kiadványban lektorált magyar nyelvű tudományos cikk, HU ISSN 2061-9499

[5] 6698-16/2011. Országos Rendőr-főkapitányság és a Magyar Bankszövetség között kötött együttműködési megállapodás ORFK Tájékoztató (OT) 2011/4. szám (2011. május 6.)

[6]Arcfelismerő technológia http://richpoi.com/cikkek/infotech/terfigyelo-kamerak-es-arcfelismero-technologia.html,http://www.gyartastrend.hu/nyarimuszak/cikk/kikemlelik_minden_lepesunket, letöltve: 2014. július 7.

[7] MÓDSZERTANI ÚTMUTATÓ A rendőrség bűnmegelőzési tevékenységéről szóló 20/2010 (OT. 10.) ORFK utasítás 36. pontjához

[8] Sipos Jenő: Alternatív (nem halálos) fegyverek Hadmérnök IV. évfolyam 1. szám, 2009. március, letöltve: 2014. június 10.

[9] Szalai János: Speciális erődítési létesítmények terrorista akciók elleni védelme Kard és toll, 2006/1., 66-74. oldalak

[10] Keresztes József: Újfajta kényszerítő eszközök alkalmazásának lehetőségei a fegyveres biztonsági őri munkában, Fegyveres Biztonsági Őrségek VI. Országos konferenciája, 2013. április 11-12., Kiskőrös

[11] Hirdetmény az OTP Bank Nyrt. ügyfél-azonosítási rendjéről https://www.otpbank.hu/static/portal/sw/file/Ugyfelazonositas_H_hun_20130809.pdf, letöltve: 2015. október 17.

[12] Kovács Tibor - Milák István - Otti Csaba: A biztonságtudomány biometriaiaspektusai, http://www.pecshor.hu/periodika/XIII/kovacsti.pdf

[13] Magánbiztonsági képzés – nem középiskolás fokon. IN: Biztonságpiac évkönyv, 2015., 119-120. oldalak

A 4. FEJEZET-hez

[1] Jain, A. K. – Flynn,P. – Ross, A. A.: Handbook of Biometrics Springer Science + Business Media, LLC., 2008

[2] Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök VI. évfolyam 1. sz., 24-25. oldalak, letöltve: http://hadmernok.hu/2011_1_bunyitai.pdf, letöltve: 2014.október 20.

[3] Nadort, A.: The Hand Vein Pattern Used as a Biometric Feature, Vrije Universiteit, Amsterdam, 2007

[4] Kovács Tibor: A biometrikus azonosítás alapjai, Óbudai Egyetem Bánki Donát Gépész és Biztonságtecnikai Mérnöki Kar, Alkalmazott Biometria Intézet, (Applied Biometrics Institute – ABI), digitális jegyzet, 2015

[5] Jain, A. K. – Flynn,P. – Ross, A. A.: Handbook of Biometrics Springer Science + Business Media, LLC., 2008

[6] Kovács Tibor: A biometrikus azonosítás alapjai, Óbudai Egyetem Bánki Donát Gépész és Biztonságtecnikai Mérnöki Kar, Alkalmazott Biometria Intézet, (AppliedBiometrics Institute – ABI), digitális jegyzet, 2015

[7] Balla József: Biometrikus adatok a személyazonosításban http://www.pecshor.hu/periodika/XIV/ballaj.pdf; letöltve: 2014. október 20.

[8] Ősz Arnold - Leung Yuen Ting - Kovács Tibor: Biometrikus azonosító eszközök műszaki paramétereinek függése az alkalmazási körülményektől, előadás, 14. dia, Magyar Tudomány Ünnepe 2011., Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[9] Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására; Minőségés Megbízhatóság; nemzeti minőségpolitikai szakfolyóirat, kiadja: az European Organization for Quality (EOQ) Magyar Nemzeti Bizottsága, XLVI. évf. 2012. / 5. sz., 252-257. oldalak, ISSN: 0580-4485

[10] Földesi Krisztina: Kutatás a biometrikus azonosításhoz kapcsolódó averziók feltárására (A tudomány szolgálatában IX.. Ph.D. Konferencia előadásai, Budapest, 2014. október. 29.), II. Kötet Szerkesztette: Dr. Koncz István - Szova Ilona, 115-127. oldalak, Kiadja a Professzorok az Európai Magyarországért Egyesület, ISBN: 978-963-89915-4-6

[11] Fluke Corporation, BAE Systems, Raytheon, L-3 Communications Infrared Products, DRS Technologies, FLIR Systems, InfraredVision Technologies Corporation, NEC, Institut National d'Optique (INO), Honeywell, ULIS-IR

[12] Kovács Tibor - Milák István - Otti Csaba: A biztonságtudomány biometriai aspektusai, http://www.pecshor.hu/periodika/XIII/kovacsti.pdf; letöltve: 2014. október 3.

[13] Hőkamerák a biztonságtechnikában http://www.securinfo.hu/termekek/videotechnika/778-hokamerak-a-biztonsagtechnikaban-5-gyakorlati-alkalmazasok; letöltve:2015. február 12.

[14] Radford, W. – Wyles, R. – Varesi, J. – Ray, M., - Murphy, D.: :Sensitivity Improvements in Uncooled Microbolometer FPAS

[15] http://lemil.blog.hu/2014/01/24/merfoldkovek_es_erdekessegek_a_technikai_vedelemben; letöltve: 2015. szeptember 19.

[16] Daruka Norbert: Robotok a repülőtéri biztonságért Repüléstudományi Közlemények, Különszám, 2011. április 15.

[17] Cardoso, H. V. - Diniz, L. M. - Tolnai András: A robotino oktatói robot kamerakép feldolgozásának és színfelismerésének elemzése, XX. Fiatal Műszakiak Tudományos Ülésszaka, 2015 Kolozsvár, 111–114. oldalak, http://hdl.handle.net/10598/28604; letöltve: 2015. október 2.

[18] Új videó adatelemzési módszer, http://www.vivotek.hu/a-vivotek-forradalmian-uj-video-adatelemzo-megoldassal-robbant-be-a-piacra-2/; letöltve:2015. október 9.

[19] Rohr Linda: Quo Vadis IP CCTV, Magyar Biztonságtechnikai Magazin, 2011. II. szám

[20] Innovációgátló biztonság? http://www.bankkartya.hu/hirkategoria/hirek/cikk/innovaciogatlo-biztonsag; letöltve: 2015. november 19.

[21] Biometrkus azonosítás. A jövő már a jelenben, http://www.origo.hu/tudomany/20071105-biometrikus-azonositas-jovo-mar-a-jelenben.html; letöltve: 2014. január 21.

[22] Kovács Tibor: Biometrikus azonosítás, egyetemi digitális jegyzet, Óbudai Egyetem, 2015

[23] Tihanyi Norbert - Vargha Gergely - Frész Ferenc: Biztonsági tesztelés a gyakorlatban, Nemzeti Közszolgálati Egyetem, Magyar Program, Budapest, 2014, ISBN 978-615-5491-59-7

[24] Bűnügyi nyilvántartás, biometrikus adatok, Képviselői Információs szolgálat, Infojegyzet, 2015/42., 2015. szeptember 17

[25] Schutzbach Mártonné: Az informatikai biztonság általános koncepciója és gyakorlata a védelmi szférában, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003, 155. oldal

[26] Kovács - Leung - Őszi: Biometrikus azonosító eszközök műszaki paramétereinek függése az alkalmazási körülményektől, előadás az Óbudai Egyetemen, Budapest, a Magyar Tudomány Ünnepe keretében, 2011

Az 5. FEJEZET-hez

[1] www.index.hu/gazdasag/magyar/bankbi090129

[2] http://hvg.hu/itthon/20090924_budapest_uj_bankbiztonsagi_rendszer, letöltve: 2010. szeptember 3.

[3] http://crimestat.b-m.hu/Default.aspx, letöltve: 2014. november 10.

[4] http://bbterkep.police.hu/mapdisplay/bu.html, letöltve: 2015. augusztus 12.

[5] http://www.uzletihirszerzes.hu/szemely-es-vagyonvedelem/2276-vltozsra-van-szksg-a-bankbiztonsg-terletn.html, letöltve: 2015. február 5.

[6] Vasvári György CISM: Bankbiztonság Információs Társadalomért Alapítvány, Infota Kiadó, 2006

[7] Philip Zimbardo: A Lucifer hatás, Ab Ovo Kiadói Kft., 2012

[8] Judith Herman: Trauma és gyógyulás, Háttér Kiadó, 2011;

[9] Dr. Vikár András: Pszichodráma - a komoly játék, Medicina Könyvkiadó Zrt., 2007

[10] Moreno Jacob L.: Gruppenpsychotherapie und Psychodrama - Einleitungin die Theorie und Praxis, Thieme Georg Verlag, 2007

[11] Sarkady K. - Frenkl S.: Hogyan folytatódik Freud szabad-asszociációs módszere? A protagonista-centrikuspszichodráma játék, Mental Port, 2009

[12] Juhász Márta - Soós Júlia: Magas kockázatú munkakörökben dolgozó teamek kommunikációs stratégiája a stresszel való hatékony megküzdésben,In: Humánpolitikai szemle, 2007. (18. évf.) 5. sz., 3-14. oldalak

[13] Wilkinson, Greg: A stressz, Budapest, Pannonica, 2002

[14] Fialka György: A pénzintézetek technikai biztonságának történeti fejlődése és jövője, Hadmérnök 86. V. évfolyam 2. szám.