Radomír ŠČUREK[1]

OCHRANA OSOB A MAJETKU NA LETIŠTI POMOCÍ HODNOCENÍ CESTUJÍCÍCH

Abstrakt

Příspěvek popisuje problémy předběžného hodnocení cestujících v letecké dopravě za účelem zvýšení bezpečnosti civilní letecké dopravy. Seznamuje s možnostmi vyhledávání potencionálních pachatelů protiprávních činů podle jejich fyzických a psychických projevů před a v průběhu vlastního odbavení na letišti.

Klíčová slova: Typping (Behavior Detection Officers), Profiling (Advente passenger informatik) elektronická letenka, Bezpečnostní dotazování na osobu a zavazadla., Technologie Malintend (špatný úmysl)

Úvod

Oproti jiným způsobům dopravy, mají cestující v letecké dopravě nízkou míru anonymity, v závislosti na opakovaných kontrolách totožnosti cestujících. Cestující poskytuje dopravci své jméno a příjmení, existují záznamy o objednávce a zaplacení letenky, při vstupu do tranzitního prostoru a následně do letadla jsou cestujícím kontrolovány cestovní doklady, některé státy vyžadují po cestujících údaje o národnosti, bydlišti, místě pobytu v cizí zemi, dokonce i o profesi a tyto údaje jsou uschovány v databázi.

Databáze cestujících

Rozeznáváme údaje PNR (Passenger name rekord), což je digitální záznam o cestujícím, o jeho cestě konkrétní leteckou společností. Databáze PNR jsou určeny pro letecké společnosti, které jsou spravovány centrálně v databázi CRS (Computerized reservation systém), počítačové databázi rezervačního systému, tento systém využívá také název globální distribuční systém se zkratkou GDS (Global distribution systems). Mezi nejrozšířenější globální distribuční systémy patří ve Spojených státech užívaný systém SBRE a GALILEO/APOLLO. V Evropě se využívá systém AMADEUS, který využívají České aerolinie, nebo WORLDSPAN.

Záznam ve shora uvedené databázi je proveden vždy současně s rezervací letenky. Jakmile systém záznam vytvoří, vygeneruje současně auditní protokol, do kterého se zaznamenávají veškeré změny záznamu. Také se zde postupně ukládají údaje o čase, místě rezervace, uživatelském identifikačním čísle, údaje o zprostředkovateli, cestovní kanceláři a konkrétní osobě, která provedla do systému záznam, stejně jako jméno cestujícího, nebo subjektu, který později provedl změnu rezervace. Data jsou předána ve společně mezinárodní dohodnuté formě, resp. Formátu, který se nazývá AIRIMP.

Pokud se jedná o pravidelného zákazníka letecké společnosti, je mu vytvořen profil, kde se přidávají jednotlivá data o následující cestě. Tento profil často zahrnuje čísla kreditních karet, čísla pasů, elektronické adresy, telefonní čísla, adresa, informace o rodinných příslušnících, poznámky o preferovaném jídle a sedadle v letadle, zdravotním stavu a poznámky z cestovní kanceláře například typu:“stále si mění čas odletu, rád se dohaduje

[1] doc. Mgr. Ing., Ph.D., VŠB – TUO, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Lumírova 13, 700 30 Ostrava – Výškovice, e-mail: radomir.scurek@vsb.cz

o místě“ a podobně. Z distribučního systému lze také vyčíst, zda se cestující někdy nedostavil k odletu. Většina dat zadaných do digitálního záznamu o osobě cestujícího nejsou vkládány leteckými společnostmi, ale cestovními kancelářemi nebo samotným cestujícím za účelem zvýšení komfortu cestování.

V současnosti se zvýšenými riziky rozeznáváme rovněž tzv. další informace o cestujícím, označené API (Advente passenger information). Tyto údaje jsou požadovány imigračními úřady některých států. Pokud letecká společnost tyto údaje o cestujícím neposkytne, hrozí jim pokuty, nebo i zákaz vstupu do vzdušného prostoru dané země. Mezi tyto údaje patří zpravidla data obsažená v cestovních dokladech, navíc pak údaje o trvalém bydlišti, délce plánovaného pobytu, nebo telefonní kontakty. Na rozdíl od PNR neslouží API žádným obchodním účelům.

Letecké společnosti mají dvě možnosti, jak poskytovat požadovaná data bezpečnostním složkám státu do kterých létají. Jedná se o způsoby PUSH (tlačit) a PULL (táhnout). Nejpoužívanější je systém PUSH, který spočívá v tom, že letecká společnost shromáždí veškerá data o cestujících a daném letu ve svých databázích a zpravidla ještě před odletem je odešle bezpečnostním složkám daného cílového státu. V systému PULL jsou informace shromážděné v databázích letecké společnosti a bezpečnostní orgány cílové země mají přístupová hesla a sami si potřebné údaje v databázi letecké společnosti kdykoliv vyhledají.

Za účelem boje proti nedovolenému přistěhovalectví a zdokonalení hraniční kontroly byla vydána směrnice Rady EU č. 82/2004, která ukládá leteckým dopravcům povinnost poskytnout o každém cestujícím **devět základních údajů**. Jedná se o číslo a typ použitého cestovního dokladu, státní příslušnost, jméno a příjmení, datum narození, údaj o hraničním přechodu na území členského státu EU, kódové číslo letu, čas odletu a příletu, celkový počet osob přepravovaný daným letem, počáteční místo nástupu na palubu letadla. V České republice byla tato povinnost zavedena od 1. 7. 2006 v rámci novely zákona č. 49/1997 Sb., o civilním letectví ve znění změn a doplnění. Vzhledem k náročnosti na zpracování vyžaduje Policie České republiky tyto údaje pouze od dopravců létajících z rizikových destinací, tedy ze zemí s největším počtem ilegálních emigrantů. Údaje o cestujících nejsou využívány jen pro operativní bezpečnostní složky daného státu, ale k identifikaci obětí leteckých nehod.

Ve Spojených státech amerických (USA) jsou data cestujících směřujících do jejich země podrobena navíc další dvojstupňové kontrole. V prvním stupni jsou letecké společnosti povinny prověřit, zda některý z cestujících nebo z členů posádky není zařazen na seznamech nežádoucích osob. Tyto seznamy jsou označeny NO FLY nebo SELECTEE list. Jde o seznamy podezřelých z terorismu, které jsou poskytnuty bezpečnostními složkami USA leteckým společnostem včetně aktualizací. Pokud letecká společnost nalezne na seznamech takového cestujícího, je povinna prostřednictvím zastupitelského úřadu informovat bezpečnostní úřady USA. Takoví cestující nejsou na palubu letadla vpuštěni, nebo na základě instrukcí bezpečnostních složek bez upozornění dopraveni na území USA a zde jsou podrobeni zvláštním opatřením.

Druhý stupeň prověření cestujících do USA je prováděn těsně před odletem letadla. Musí být již odeslána, nebo zpřístupněna API data do Národního sledovacího centra USA (National Tracking Centre), které opět prověřuje seznamy cestujících a porovnává je se seznamy NO FLY nebo SELECTEE. Pokud jsou takoví cestující i přes kontrolu leteckých společností zjištěny je upozorněno Středisko pro informace o teroristech USA (Terrorist Screening Centre), které vydá doporučení, zda osoba nebude vůbec vpuštěna, nebo po příletu zatčena, či jen sledována. Podle toho v jaké fázi se letadlo nachází, může být let odkloněn, nebo nařízeno vrátit se do výchozí destinace. Údaje API jsou vyžadovány i v případech, kdy letadlo jen nad územím USA přelétá.

Zavedení systému předběžného hodnocení cestujících

Vzhledem k rostoucím nárokům na bezpečnost letiště se klade důraz na vývoj a zavádění integrovaného bezpečnostního systému, který je napojen na odbavovací, bezpečnostní a vyhledávací systémy (SITA). Nyní letecké společnosti předávají jen jméno, datum narození a podrobnosti o příletu a odletu cestujících kvůli imigračním kontrolám Nový systém má za úkol shromáždit všechna data o cestujících z různých zdrojů dopravců, aby bylo možné provést identifikaci cestujících a jejich zavazadel. Tato data by měla být uchovávaná pro bezpečnostní složky (cizinecká policie) a průběžně doplňována podle aktivit cestujícího a využívána při následných odbaveních.

Prvním systémem hodnocení cestujících v letecké dopravě z hlediska možných rizik násilných činů, byl systém CAPPS (počítačový systém předběžného hodnocení cestujících), vytvořený ve druhé polovině 90. let minulého století v USA. Tento systém byl založen na analyzování údajů o cestě, které běžně shromažďují letecké společnosti. Současně se objevily úvahy o zavedení osobních dokladů s biometrickými údaji. Byly navrhovány tzv. „neinvazivní senzory“, resp. skenery mozkové aktivity, umístěné na bezpečnostních rámech, s jejichž pomocí by bylo možné zjistit, zda někdo z cestujících neplánuje něco protiprávního. Systém CAPPS byl provozován FBI (Federální úřad pro vyšetřování USA) a FAA (Federální úřad pro letectví USA) a do plného provozu byl spuštěn v roce 1997. Pokud byl některý z cestujících vybrán jako potencionální bezpečnostní hrozba, byla jeho zavazadla podrobena důkladnější kontrole. Cestující sám žádnou podrobnější prohlídkou neprocházel. To se ukázalo být slabinou systému CAPPS, protože ten 11. září 2001 správně identifikoval většinu atentátníků jako potencionální hrozbu, ale protože jejich zavazadla prošla kontrolou bez problémů, byli všichni vpuštěni na palubu letadel. Po útocích z 11. září 2001 bylo zřejmé, že dosavadní bezpečnostní systémy v letecké dopravě jsou snadno překonatelné. Proto byl navržen systém CAPPS II, jehož podstata spočívala v tom, že údaje o cestujícím, získané při koupi letenky, jsou porovnány s údaji, uloženými ve státních a komerčních databázích. Přitom by se ověřovala totožnost, zjišťovaly se předchozí kriminální aktivity, ale také to, zda daný cestující nemá možné vazby na teroristy. Přesný algoritmus je utajen. Ve výsledku je cestující s pomocí barevné škály ohodnocen z hlediska možné rizikovosti a toto hodnocení se zasílá zpět letecké společnosti.

Návrh na zavedení systému CAPPS II počítá s procházením řady databází, obsahujících soukromé údaje, čímž vzbuzuje protesty ochránců lidských práv, zavedení tohoto systému bylo proto v srpnu 2004 pozastaveno. Na začátku roku 2005 byl CAPPS II nahrazen novým programem „Bezpečný let“, který má úkoly podobné jako CAPPS II. Vzhledem k pokračujícím obavám z narušování soukromí však ani tento program není plně funkční a jeho zavedení je v USA plánováno na rok 2010.

Evropská databáze otisků prstů EURODAC

Na základě nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 20001) byla na území Evropské unie zavedena evropská databáze otisků prstů EURODAC, jež je vytvořena s cílem napomáhat při určování, který členský stát EU je příslušný k posouzení žádosti o azyl a současně usnadňovat naplňování společné azylové politiky a bezpečnostních kontrol nejen na letištích v Schengenském prostoru. Tento systém sestává z centrální databáze otisků a sítě národních přístupových míst sloužících k předávání údajů mezi členskými státy. S touto databází jsou propojena i pracoviště Policie ČR na letišti.

EURODAC je v současné době již neodmyslitelnou součástí společné azylové politiky EU, která se stává, vzhledem ke svobodě pohybu v rámci tohoto společenství, nezbytností. Za situace, kdy mezi členskými státy existuje minimální hraniční kontrola a lidé mohou

bez překážek volně cestovat z jednoho členského státu EU do druhého, je sjednocení pravidel a výměna informací jediným způsobem, jak zajistit určitou rovnováhu v přístupu k otázkám uprchlíků a migrantů v rámci EU.

Kromě členských států EU se k systému EURODAC připojily také Norsko a Island; naopak ze stávajících evropských zemí tento systém nevyužívá Dánsko.

S účinností od roku 2003 jsou tedy v rámci azylového řízení v každém členském státě snímány otisky prstů všech žadatelů o azyl starších 14 let, přičemž stejný postup platí pro osoby podávající žádost na území EU i mimo ně (na zastupitelských úřadech). Dalšími osobami, jejichž otisky prstů jsou porovnávaný se záznamy v EURODAC, jsou cizinci (tj. občané tzv. třetích zemí) zadržení v souvislosti s neoprávněným překročením vnější hranice evropského prostoru a dále cizinci, kteří se nedovoleně (bez řádného povolení) zdržují na území některého členského státu.

Otisky prstů těchto osob jsou následně v digitální formě posílány do zmíněné centrály EURODAC, kde jsou automaticky porovnávány s otisky, jež byly do databáze zařazeny již dříve. Tento postup umožňuje příslušným úřadům zjistit, zda se dotyčná osoba již v některém jiném členském státě v minulosti neucházela o azyl, čímž je usnadněno rozhodování, která členská země se má daným případem zabývat, a současně zabraňuje osobám, které by žádosti o azyl chtěly zneužívat, aby se obracely na další členské státy poté, kdy byla jejich žádost v jedné zemi odmítnuta, nebo aby systém zatěžovaly opakovaným podáváním žádostí.

Nedílnou součástí systému EURODAC jsou striktní pravidla zajišťující ochranu lidských práv a občanských svobod, včetně ochrany osobních údajů. Výše citované nařízení jasně specifikuje, že otisky lze využít výhradně pro účel azylového řízení, přičemž k údajům o otiscích nejsou připojovány další identifikační údaje. Obsahem záznamu v EURODAC jsou tedy údaje o otiscích prstů, název členského státu, který je vložil a datum a místo podání žádosti o azyl, tj. datum sejmutí otisků a dále informace o zemi původu a pohlaví žadatele.

Dohledem nad využíváním osobních údajů uchovávaných v systému EURODAC je v každé členské zemi pověřen nezávislý dozorový úřad (v České republice je jím Úřad pro ochranu osobních údajů). Za kontrolu činnosti centrály zodpovídá Evropský inspektor pro ochranu údajů (European Data Protection Supervisor), jenž je garantem toho, že při využívání tohoto systému nedochází k porušování práv žadatelů o azyl.

Vývoj směřuje k zavedení systému iBorders, který sceluje rezervační systémy aerolinií, státu a cestovních kanceláří a navádí je na celosvětový distribuční systém GDS (Global Distribution Systém) spojený se sítí SITA. Tento systém obsahuje potřebná data o odlétávajících, tranzitních a přilétávajících cestujících a lze ho využít na celý odbavovací proces. V systému je využita evidence potřebná pro registraci a kontrolu cizinců při vstupu do jednotlivých států tzv. ETA (Elektronic Traveler Authorization). Jde vlastně o dotazník, tzv. příletová vstupní karta, kterou je nutné vyplnit před vstupem do země. Vyplněný dotazník se zpracuje a elektronicky uloží pro další využití. Do budoucna bude dotazník ETA obsahovat i bio-data. Cestující může dotazník vyplnit ještě v cestovní kanceláři nebo přes internet z domova ještě před odletem. Parametry se v systému dostanou k aerolinkám, do cestovních kanceláří a k bezpečnostním službám letiště. Po příchodu cestujícího na letiště a načtení jeho letenky u odbavení budou jeho údaje aktivovány v systému iBorders, ten vyšle parametry do odbavovacího systému tzv. Departure Control Systém (DCS). Cestující je odbaven pružněji a efektivněji projde přes kontrolní body, bezpečnostní, pasové a celní přepážky.

Další možností je, že cestující na základě biometrických metod absolvuje odbavení samoobslužně u tzv. Aiport Connect Kiosk napojeného na iBorders systém. K identifikaci cestujícího a srovnání jeho identifikačních parametrů uložených v systému iBorders může být využito načtení lidské tváře (parametry lebky), dále načtení otisků prstů, načtení oční rohovky. Údaje budou také uloženy na identifikačním průkazu cestujícího. Při shodě

s fyzickou skutečností, daty na identifikační kartě a údaji v iBorders systému bude cestujícímu vydán barevně nebo jinak označený palubní lístek. Dále samolepící označení zavazadel a oděvu cestujícího s opticky rozpoznatelnými znaky (OCR – Optical Caharacter Recognition), kterými cestující sám označí sebe a svá příruční zavazadla a při průchodu letištěm, či odbavení zavazadel bude automaticky kontrolována poloha cestujícího a jeho zavazadel pomocí radiových vln. Poloha je ověřována duálně prostřednictvím infračervených čteček čárového kódu. Dodatková kontrola polohy cestujícího může být provedena identifikací polohy podle signálu vydávaného z mobilního telefonu při přechodu přes kontrolní jednotky. Na palubní vstupence se rovněž vytiskne podoba cestujícího k fyzické kontrole provedené personálem. Pro efektivní využití tohoto systému je nutné načíst data pravidelných cestujících, aby nemuseli vyčkávat ve frontách na odbavení a sami, ve vlastním zájmu pak využili k odbavení služby Aiport Connect Kiosk. Celkem 19 různých dat se shromáždí ve společné centrální databázi členských států. V budoucnu by se k tomu měly připojit čísla a platební informace, data rezervací a vydání letenky, adresa kupujícího či informace o prodejci, zavazadle či místě v letadle. Celkem by data mohla být uchovávána až třináct let.

Při odbavování zavazadel lze využít obdobný systém nazvaný „Bag Manager“. Systém umožní sledovat zavazadlo po celou dobu jeho přepravy do cílové destinace. Údaje o zavazadle se načítají radiovým přenosem a příručními archivačními zařízeními. Na odbavovací přepážce je na zavazadlo připevněn zavazadlový lístek a zavazadlo je zaneseno do Departure Control Systému (DCS) a do Bag Manager systému. Načtením zavazadla pak započne sledovací proces zavazadla. Zavazadlo prochází bezpečnostní kontrolou, poté zavazadlo putuje do třídírny a zde je sortováno podle určené destinace a nakládáno jako volně ložené, nebo do kontejneru, zde je zaznamenána jejich přesná poloha. Pak je přes rampy nakládána do letadel a pomocí ručních snímačů je naložení potvrzeno do systému. Jsou zaznamenány také údaje o poloze zavazadla v letadle. Vše je zasláno do cílové destinace. Je zaváděná služba, kdy lze zjistit polohu zavazadla pomocí WAP, SMS nebo internetu.

Na některých letištích lze cestující odbavit bez papírové letenky a palubní vstupenky. Postačí vykázat se kódem, jenž pasažérovi v rámci systému rezervace zašle letecká společnost na mobilní telefon. Při příchodu do odbavovací haly cestující přiloží displej mobilu čtecímu zařízení a formality jsou vyřízeny (kód tvoří směs černobílých čtverců).

Zaváděny jsou systémy analýzy cestujících školeným personálem již na odbavovacích přepážkách provozovatele letiště, kteří zhodnotí chování cestujícího, jeho vzhled, dokumenty a zadají základní bezpečnostní otázky. Vhodné je zavedení bezpečnostního dotazování cestujícího na obsah jeho zapsaných zavazadel, v případě zjištění nejasností zajistit zvláštní označení zapsaného zavazadla. Provádět také typování podezřelého chování cestujících příslušníkem bezpečnostní ostrahy vydávajícího se za klienta a to buď neskrytě s preventivním účinkem a současně skrytě. Zjevná prohlídka působí preventivně, ale rozladí běžné klienty a útočník si zvolí po jejím zjištění jiný způsob průniku. Vychází se z předpokladu, že osoba, která přenáší nebezpečný předmět je neklidná, roztěkaná, uhýbá pohledem očí a rozhlíží se okolo sebe více než ostatní cestující a další.

Minimalizace nelegální manipulace se zavazadly

Nelegální manipulace se zavazadly cestujících je častým problémem a snahou vedení letišť je tento jev snížit na minimum. Je to jev, který se týká letecké dopravy obecně, kdekoli na světě. Přesto rozdíly v počtu zavazadel, u kterých byla zjištěna nelegální manipulace na evropských linkách, a při letech, které směřují například do afrických destinací, umožňují dovodit, že k manipulaci dochází nejčastěji mimo Evropu. Pro každé letiště je obtížné

objektivně určit, ve které destinaci k nepovolené manipulaci došlo, zda v odletové či cílové, a proto se statisticky porovnává, zda se počet zavazadel, u kterých byla zaznamenána neautorizovaná manipulace, změnil například s nástupem letního období, kdy je zvýšená frekvence letů do určitých rekreačních oblastí. Na letištích se uplatňují opatření snižující možnost nelegální manipulace se zavazadly cestujících. Jedním z opatření je, že všichni zaměstnanci letiště i zaměstnanci dalších subjektů, kteří pracují v areálu letiště, musí mít čistý trestní rejstřík. Osoby, které se pohybují v tzv. citlivých zónách, do nichž patří jak tranzitní prostor a třídírna zavazadel, ale i odbavovací plocha pro letadla nebo paluby letadel, jsou navíc prověřováni Národním bezpečnostním úřadem. Dále se používá nový kamerový systém, který zabírá celý prostor třídírny a její zaměstnanci jsou tak pod trvalou kontrolou, včetně namátkových prohlídek po skončení nakládky. Kontrola zaměstnanců má probíhat tak, že bezprostředně po skončení nakládky je náhodně vybraný tým nakladačů odvezen přímo od letadla a podroben kompletní osobní kontrole, která je zaměřena i na osobní šatní skříňky, služební i speciální vozidla a mobilní prostředky nakládání. Pracoviště monitorující obsah zavazadel musí být zdí odděleno od pohybu zavazadel a obsazení pracovních směn musí být soustavně a náhodně obměňováno. Účinným bezpečnostním opatřením je umísťování autorizovaných nálepek s čárovými kódy na všechna zavazadla, která prošla detekční kontrolou. Bezpečnostní management letiště kontroluje proces nakládky a vykládky na odbavovací ploše, a informace se srovnávají s údaji z kódů zavazadlových štítků. Kontroly jsou zaměřeny zejména na letadla směřující do oblastí, z nichž je hlášen častější výskyt neautorizované manipulace se zavazadly.

Účinným preventivním opatřením je rovněž balení bagáže samotnými cestujícími do plastikových folií. Nepřetržitá služba tohoto druhu, by měla být zavedena v odletové hale. Situaci lze také ovlivnit tím, že v zavazadlech, která si neberou cestující do kabiny letadla, nemají být uloženy cenně věci a finanční hotovost. Neautorizovanou manipulaci se zavazadly lze omezit pečetěním všech kontejnerů se zavazadly včetně balení celých palet se zavazadly směřujícími do jedné destinace do fólie z umělé hmoty.

Detekční kontrola systémem Malintend

Malintend, neboli „Zlý úmysl“ je přístroj, který dokáže pomocí citlivých senzorů na dálku detekovat stav mysli člověka či jeho špatný úmysl vůči okolí. Zařízení má pomoci v boji s protiprávními činy a na letištích zmenšit fronty na odbavování a dovolit cestujícím brát si do letadla tekutiny.

Běžným standardem je v dnešní době při bezpečnostních kontrolách detekční kontrola, založena na kontaktním přístupu, tzn. kontaktu cestujícího s kontrolním objektem (WTMD, RTG, ruční detektory). Cílem kontrol je odhalit skryté předměty, které může mít kontrolovaná osoba u sebe a s nimiž může pokusit o spáchání protiprávního činu. Systém Malintend detekuje osobu na dálku, tzn. bezkontaktně na základě chování. Využívá k tomu fyziologickou a behaviorální technologii. Osoba vysílá nonverbální podněty, které předcházejí jejím úmyslům. Přístroj je naprogramován na detekci špatných úmyslů, tzn. těch, které mohou předpovídat spáchaní protiprávního činu. Z tohoto hlediska tedy pouze na screening osob a nikoliv použít k detekci zavazadel.

Detekce Malintend funguje pomocí jemných senzorů, které na dálku analyzují tělesnou teplotu, srdeční rytmus a dýchání. Tyto faktory a signály jsou lidským okem většinou nepostřehnutelné. Osoby se zlými úmysly mají v těchto faktorech odchylky a na jejich detekování a následné analýze je systém postaven. Senzory identifikují, že se některý lidský faktor vzdaluje od standardní hodnoty, přenášejí tato data k analýze. Po vyhodnocení může být osoba označena jako podezřelá a podstoupí další testy. Během těchto testů přístroj snímá obličej podezřelého a zařízení čte z jeho mikro pohybu obličejových svalů a pokouší se

rozpoznat pocity, nálady a záměry osoby. Další část měření je provedena pomocí očního snímacího zařízení a feromonové technologie k rozboru tělesného pachu. Pokud je osoba uřícená, přetížená nebo úzkostlivá, může vysílat shodné signály s těmi, které by měl potenciální pachatel, ale systém dokáže odhadnout rozdíl mezi trýzněným cestujícím a teroristou. Bezpečně zařadí i osoby, které se i v klidovém stavu více potí. Systém je schopen rozpoznat, definovat a měřit sedm primárních emocí a emocionální podněty, které se odrážejí ve stahováních obličejových svalů. Malintend tyto emoce identifikuje v reálném čase. Celý systém je časově navržen tak, aby provedl testovanou osobu přes bezpečnostní kontrolu v intervalu dvou až čtyř minut, a často i rychleji. Nejde však o polygraf, jelikož osoby nemusí být fyzicky připojeny k zařízení a senzory dělají všechna snímání bez fyzického kontaktu. Zařízení mohou být implementována biologickými, radiologickými a explozivními snímači.

Závěr

Výzkum směřuje k tomu, aby bylo zařízení vybaveno senzory sledující další faktory, např. tělesné pohyby a počítá se také s implementováním biologických, radiologických a explozivních snímačů. V současné době je hlavním záměrem potenciální lidskou hrozbu detekovat a osobu co nejrychleji vyčlenit od ostatních osob a od všech možných dostupných zdrojů, aby bylo pro své okolí co nejméně nebezpečná. Objevují se rovněž názory, že jsou osoby podrobovány nedobrovolné lékařské prohlídce a po zpracování naměřených hodnot psychosomatických faktorů, mohou být tyto údaje následně zneužity. Tyto záznamy však nejsou ukládány a data jsou okamžitě smazána. Faktem zůstává, že jako daň k pokroku může existovat přímá úměra mezi mírou technického zabezpečení osob a majetku a současně určitým omezením jejich soukromí.

Literatura

[1] KULČÁK, L., KERNER, L., SYKORY, V.: Provozní aspekty letišť, ČVUT Praha, Dopravní fakulta, skripto, 1. vydání, 2003, ISBN 80–01-02841–0

[2] ROŠ.: [online].: Američané testují zařízení pro čtení myšlenek. Deník Právo, Novinky. Dostupné na WWW: http://www.novinky.cz/zahranicni/amerika/150387-americane-testuji-zarizeni-pro-cteni-myslenek.html

[3] ŠČUREK, R.: Nové technické prostředky k usměrnění davu a k zajištění ochrany veřejného pořádku ve shromažďovacích centrech. In Sborník přednášek mezinárodní konference Požární ochrana 2004, Ostrava, VŠB-TUO, SPBI a HZS Moravskoslezského kraje, 14. – 15. 9. 2004, ISBN 80–86634-39–6

[4] ŠČUREK, R.: Stanovení rizik a zajištění bezpečnosti letiště před protiprávními činy. Habilitační práce, FBI VŠB-TU, Ostrava, 2008

[5] TUREČEK, J.: Technické prostředky bezpečnostních služeb II – Detektory pro bezpečnostní prohlídku osob, zavazadel a zásilek. Praha, PA ČR, 1998, 100 stran, ISBN 80–85981-81–5