# DETEKCE PODEZŘELÉHO CHOVÁNÍ

Nikola Čajková

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Nad Stráněmi 4511, 760 05 Zlín
*n_cajkova@utb.cz*

**Abstrakt:** Tento článek se soustředí na detekci podezřelého chování, popisuje metody a specifické technologie, pomáhající v problematice odhalení útočníka. Detekce podezřelého chování patří mezi proaktivní bezpečnostní metody odhalující možnou hrozbu útoku. Smysl detekce spočívá v co nejrychlejším identifikování podezřelé aktivity, která předchází útoku. Díky včasnému odhalení může bezpečnostní systém teroristický útok nebo kriminální čin zcela odvrátit, anebo minimálně velmi zkomplikovat útočníkům dosáhnutí jejich cíle.

**Klíčová slova:** Měkké cíle, podezřelé chování, prevence, technologie

**Abstract:** This article focuses on the detection of suspicious behavior and describes methods and specific technologies that help in the issue of detecting an attacker. Detection of suspicious behavior is one of the proactive security methods that detect a possible threat of an attack in time. The purpose of detection is to identify the suspicious activity that precedes the attack as quickly as possible. Thanks to early detection, the security system can completely avert a terrorist attack or criminal act - or at least make it very difficult for attackers to reach their target.

**Key words:** Soft Target, Suspicious Behavior, Prevention, Technology

## ÚVOD

V dnešním světě je velmi důležitá prevence, což platí dvojnásob, pokud se jedná o odvrácení teroristického útoku, či trestného činu. Záměrem je tedy zastavit útočníka dřív, než dosáhne svého cíle, jehož následkem může způsobit hromadné ztráty na životech, poškození infrastruktury apod. Většinou jsou těmito cíli místa s velkým výskytem osob a místa s vysokou atraktivitou pro útočníka. Atraktivitu daného místa mohou zvyšovat kritéria, jako například přítomnost policie, otevřenost pro veřejnost, kvalita bezpečnostního personálu, přítomnost médií atd. [1]

Možností detekce podezřelého chování je mnoho – od nejjednodušších, které spočívají v pozorování osob, (rozčleněných podle typologií a vzorci chování) až po sofistikovanější, (využívajících scénářů útoku, výstupů analýz uskutečněných útoků až po implementování speciálních technologií pro detekci podezřelých osob). Všechny ale závisí na systematickém vyhodnocování toho, co se vymyká/nezapadá do určitého prostředí, s následným zkoumáním míry reálné hrozby.

## ZPŮSOB DETEKCE

Detekce podezřelého chování je jedním z nástrojů používaných při profilové bezpečnostní metodě – profilace, která je jednou z bezpečnostních metod používaných pro včasnou identifikaci rizikových osob u tzv. proaktivních bezpečnostních přístupů.

Cílem profilace je zaměřit bezpečnostní opatření na osoby ohodnocené jako rizikové. Detekují se zejména nestandardní fyziologické projevy a chování posuzovaných osob. K vypozorování pomáhá vyprovokování stresové reakce osoby, znalost kontextu, dokonalá znalost normálních projevů apod. Tyto projevy jsou analyzovány a na základě závěrů z analýzy je stanoven další postup bezpečnostního systému dle potenciálního ohrožení chráněných aktiv. [2]

K exaktnímu měření míry reakce člověka na vnější podněty se využívají fyziologické funkce a jejich biosignály. Tyto signály jsou proměnné v čase dle míry působení vnějšího podnětu a citlivosti daného jedince na daný podnět. Každý jedinec reaguje na daný podnět různě. Biosignály se mohou rozdělit do několika typů dle původu/vzniku:

- **Elektrické biosignály** – generují nervové a svalové buňky jako výsledek elektrochemických procesů. Při působení stimulu přesahující prahovou hodnotu buňky je generován akční potenciál (tok iontů), který lze změřit například mikroelektrodami. Potenciál je předáván okolními buňkami a umožňuje vytvářet elektrické pole v tkáni, které je měřitelné na povrchu těla.

- **Impedanční biosignály** – lze měřit aplikacemi elektrického proudu o nízkých hodnotách proudů (mikro až miliampéry do lidského těla. Z vypočítaného odporu lze poté určit nervovou a endokrinní[1] aktivitu, objem krve, či skladbu tkání.

- **Magnetické biosignály** – jsou generovány orgány, jako například mozkem či srdcem a vypovídají o aktivitě těchto tkání. Přesné měření generovaných magnetických polí je v současnosti velmi obtížné vzhledem k nízkým hodnotám ve srovnání s geomagnetickým polem Země.

- **Chemické biosignály** – jsou reprezentovány stanovením koncentrací iontů v buňkách prostřednictvím speciálních elektrod, stanovením parciálních tlaků plynů a měřením hodnoty pH. Získané hodnoty vypovídají o stavu zkoumané tkáně.

- **Mechanické biosignály** – jsou odvozeny z mechanického pohybu nebo průtoku. Prostřednictvím mechanických mikrosnímků lze změřit například tlak krve. Optickými biosignály se rozumí změna optických vlastností organismu. Například okysličení krve lze měřit na základě intenzity odraženého světla (dle vlnových délek) od tkáně nebo užívání abiotických tekutin (barvicí tekutiny) při získávání informací o plodu. [3]

- **Tepelné biosignály** – vypovídají o stavu fyzikálních a biochemických procesů v organismu, jejich složení v těle je různé. Měření je možno provádět kontaktním

[1] Endokrinní = týkající se žláz s vnitřní sekrecí, mající schopnost vnitřní sekrece [4]

způsobem klasickými teploměry, anebo bezkontaktně termokamerou/bezkontaktním teploměrem.

- **Akustické biosignály** – jsou generovány například průtokem krve srdečními chlopněmi a cévami, průtokem vzduchu dýchacími cestami, zažívacím ústrojím, klouby atd. Měření těchto signálů probíhá prostřednictvím mikrofonů a vypovídá o funkci zkoumaných orgánů.

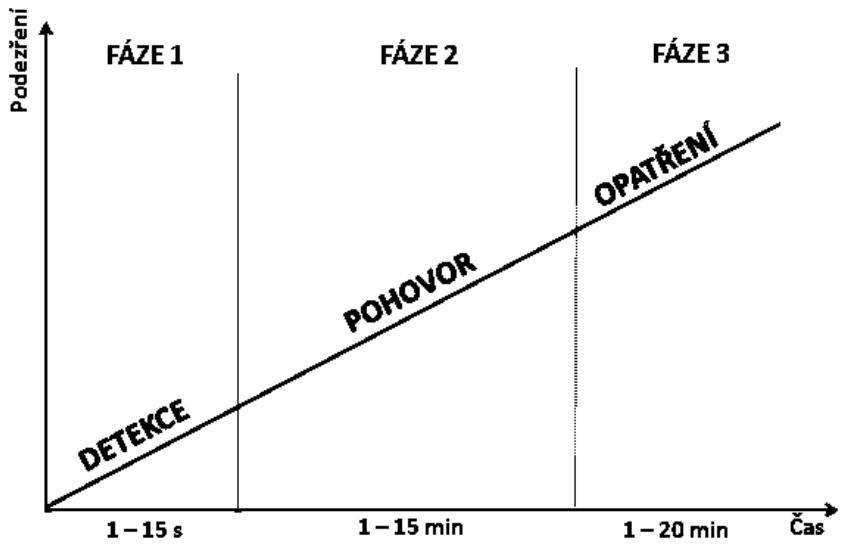
- **Radiologické biosignály** – lze využít pro získání informací o vnitřních anatomických strukturách. Vznikají reakcí ionizujícího záření s buňkami organismu.

- **Ultrazvukové biosignály** – vznikají interakcí ultrazvuku s buňkami a umožňují získání informací o velikosti objektu a charakteru pohybu. Měření probíhá piezoelektrickými senzory. [2] [3]

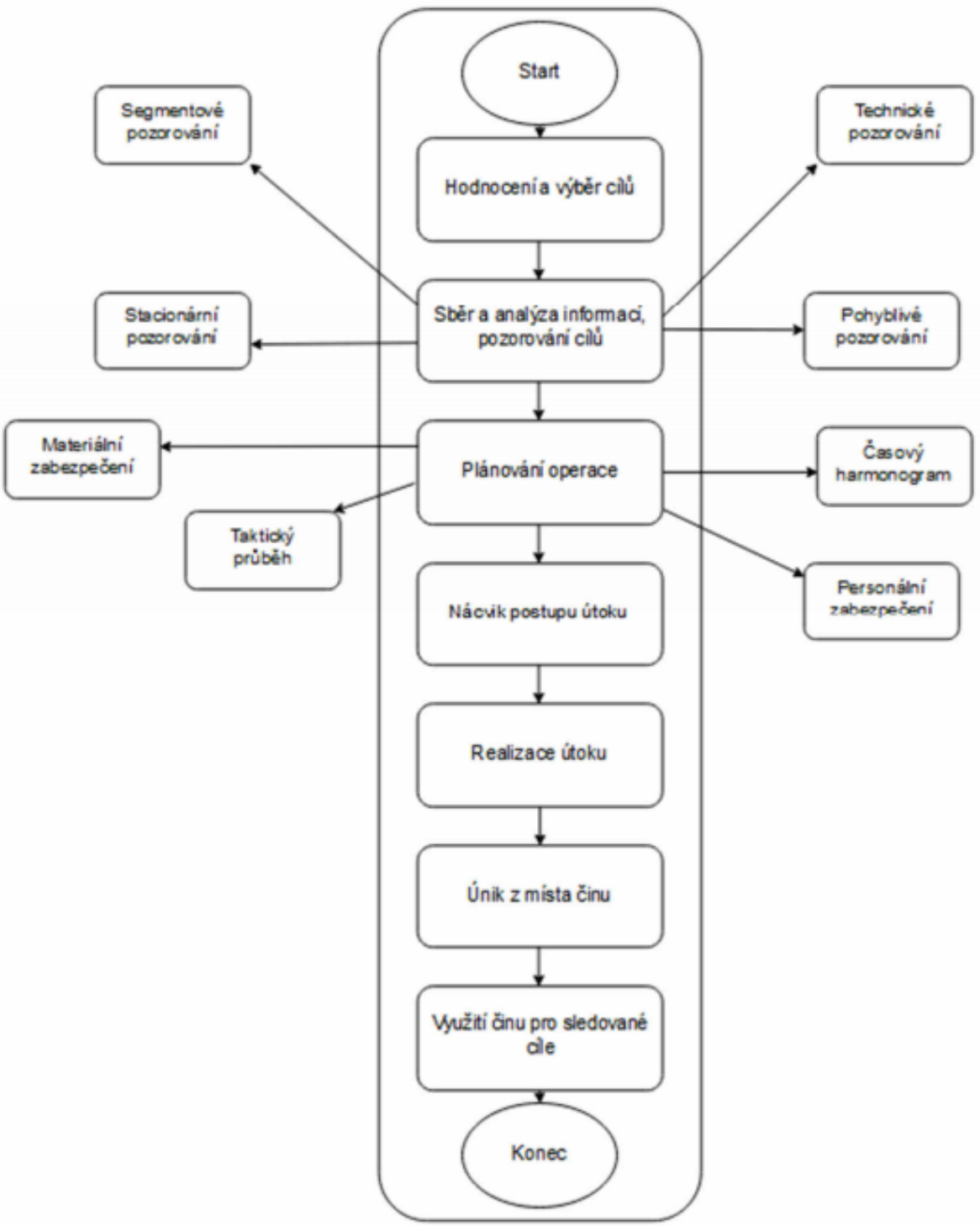
## JEDNÁNÍ PACHATELE

Teroristickému útoku předchází dlouhý proces plánování a příprav. Právě z tohoto důvodu je nutné se zaměřit na podezřelé chování a zavčas pachatele zastavit ve fázi připravování. Typickými znaky podezřelého chování mohou být například focení, natáčení, opakovaný výskyt osoby v referenčním objektu, pohyb neobvyklým tempem anebo po neobvyklé trase, maskování identity apod.

Po zaznamenání podezřelé osoby v daném objektu, je nutné ověření těchto informací/skutečností pomocí pohovoru s danou osobou. Zatímco detekce podezřelého chování se pohybuje v rámci sekund, následné prověření odhaleného trvá v řádech minut. K vedení profesionálního pohovoru existují přesné scénáře pro nejefektivnější odhalení pachatele. Pokud je výsledek pohovoru negativní, může se přistoupit k náležitým krokům či obranné reakci. [5]




Obr. 1: Jednotlivé fáze detekce podezřelého chování [7]




Obr. 2: Fáze útoku [5]

Každý teroristický útok organizované skupiny nebo útočníka prochází vývojem, který zahrnuje jako jeden z prvních kroků fázi zhodnocení a výběr cíle, na který má být spáchán atak ze stránky atraktivity a dosažitelnosti.

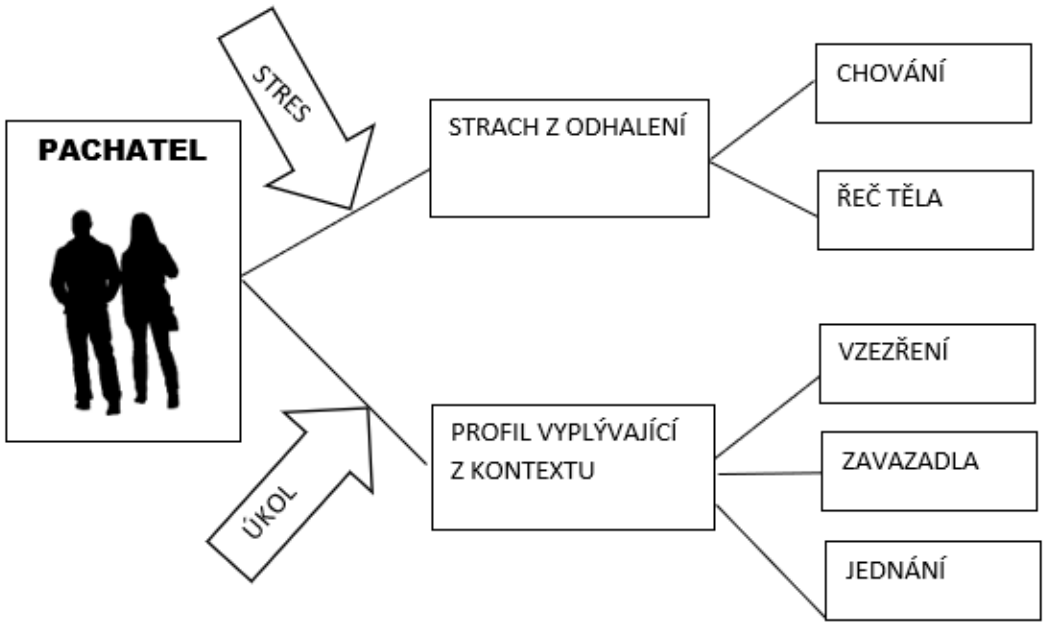
Pro zvolené cíle pachatel provede sběr informací. V dnešní době lze mnoho informací získat pomocí internetu, ale často se také přiklání k fázi sběru informací pozorováním. Typy pozorování lze z hlediska použitých metod a prostředků rozdělit do jednotlivých typů na stacionární, pohyblivé, technické a segmentové.

Po odpozorování a vyhodnocení potřebných informací nastává krok plánování útoku po stránce taktické, materiální časové. Velmi důležitým krokem je nácvik útoku, díky kterému se ověří funkčnost celého plánu. Realizace plánu vyvrcholí útokem, po kterém nastává nejkomplikovanější část útoku, kterou je opuštění místa činu.

Pro vizualizaci jsou jednotlivé fáze útoku popsány na obrázku č. 2., ve kterých působí dva typy pachatelů – útočníci a sledovatelé. Toto rozdělení pachatelů pomáhá v pokročilých fázích detekce podezřelého chování speciálním složkám. Útočníci se od sledovatelů liší typickými znaky podezřelého chování.

Pro sledovatele je typický opakovaný výskyt, natáčení, příznaky nadměrného stresu, neadekvátní oblečení, vyzvídání u personálu, maskování identity, pohyb po neobvyklé trase v neobvyklém tempu apod.

U útočníka je typickým podezřelým chováním odkládání neznámého předmětu, přibližování se ke skupině osob a čekání poblíž objektu se zbraní, je mimořádně nervózní se zjevně skrytým předmětem, má tunelové vidění či bezdůvodně mumlá. [5] [6] [7]




Obr. 3: Detekce podezřelého chování [6]

## TECHNOLOGIE PRO DETEKCI PODEZŘELÉHO CHOVÁNÍ

Boj proti terorismu je velmi rychle se rozvíjející odvětví, kde je zapotřebí velká představivost, efektivní procesy s neustále se zdokonalujícími opatřeními. Nejvíce technologií pro detekci podezřelého chování je využíváno na letištích, kde se vlivem událostí z minulosti klade velký důraz na včasné odhalení potenciální hrozby. Využití moderní technologie naleznou ale i v soukromých sektorech pojišťoven, bank, kasin a všude tam, kde je zapotřebí odhalení neobvyklého chování.

Většina uvedených technologií sestává ze sledovacích prvků a senzorů, které posílají naměřená data do centrální jednotky, kde dochází k jejich zpracování, případně jsou zpracovány přímo v daném systému a přenáší se pouze výsledky. Některé systémy nabízí uživatelské prostředí, odkud lze data sledovat, analyzovat a dále zpracovávat. [3] [7]

- Systém FAST

Future Attribute Screening Technology je vyvíjen americkým Ministerstvem vnitřní bezpečnosti pro zjišťování nepřátelských úmyslů u zkoumaných osob. Vychází z vědecké teorie „malintent[2]“, která se zabývá odhalováním nekalých a špatných úmyslů u sledované osoby.

Systém se specifikuje na sledování fyziologických a neverbálních projevů lidského těla (srdeční tep, frekvence dýchání, mimika ve tváři, pohyby těla apod.). Systém může obsahovat také senzory pro analýzu pohybu osoby, oční skener a senzor feromonů. Celá analýza trvá několik minut, během které skenovaná osoba není schopna rozpoznat proces snímání.

- Systém WeCU

Jedná se o izraelskou technologii, vyvinutou izraelskou společností pro leteckou bezpečnost WeCU (We See You). Důvodem zrodu systému byly opakované teroristické útoky na židovské cíle. Systém byl původně vyvinut k identifikaci potenciálních sebevražedných atentátníků. Umožňuje detekci nebezpečných a rizikových osob na základě sledování a chování elektronických senzorů. Systém sleduje reakce na stimul, kterým může být detailní informace nebo krátké sdělení.

Technologie se zaměřuje na rychlý pohyb očí a zvýšenou tělesnou teplotu. Nejprve je osobě v infračerveném spektru změřena aktuální tělesná teplota, tep a frekvence nádechů. Následně je osoba vystavena slabým stimulům – například promítnutí fotografie, obrázek výbušniny, symbol teroristické organizace, věta typu „Děkujeme, že pomáháte zvyšovat bezpečnost.“ apod. Princip fungování je založen na faktu, že lidé reagují na jim známý vjem, pokud jej spatří na neobvyklém místě. Senzory v takovém případě vyhodnotí změnu v signálech.

- VibraImage

Technologie VibraImage je vyvíjena ruskou společnosti Elsys Corporation a zabývá se odhalováním lidských emocí výzkumem tzv. tremorů[3]. Mikrovibrace svalů jsou charakteristické pro hlasivky, obličejové svalstvo, končetiny a trup těla.

Pohyby jsou řízené fyziologií mozku v reakci na vnější podněty a nejdou potlačit ani ovlivnit. Pohyby, které technologie zachybuje, jsou označovány jako vestibulární emoční reflexy.

[2] Malinent= malicious intent = zákeřný záměr [4]

[3] Tremor = neúmyslný, rytmický svalový pohyb vyvolaný mozkem v reakci na vnější prostředí [4]

Obrazový materiál, který VibraImage vyhodnocuje v reálném čase, lze zachytit různými způsoby. Funguje také přes digitální, webovou nebo televizní kameru. Pomocí specifické analýzy lze odhadovat lidské pocity, jakými jsou úzkost, hněv, radost, agrese apod.

- Real Time Pulse Monitor (RTPM)

Jedná se o technologii pro měření srdeční frekvence v reálném čase vyvinutou japonskou společností Fujitsu. Metoda spočívá v detekci změn světlosti tváře, která závisí na průtoku krve přes cévy v obličeji. Měření vyhodnocuje pohlcování zeleného světla hemoglobinem, který je součástí krve. Systém pořídí krátkou videosekvenci daného subjektu, jejichž snímky rozdělí a vypočítá barevné složky (červené/zelené/modré). Poté systém odstraní irelevantní data pro výpočet ze všech tří barevných složek a extrahuje křivku zelené složky. Srdeční frekvence je z této křivky spočítána pomocí Furierovy řady a Eulerovy metody na základě lokálních minim a maxim. Proces probíhá zcela bezkontaktně a trvá v řádech sekund.

- Analýza hlasu

Technologie analýzy hlasu se zabývá například izraelská společnost Nemesysco, která analyzuje změna projevu hlasu člověka podle emočního vypětí a má za úkol detekovat v grafickém záznamu hlasu stres. Nezaobírá se analýzou obsahu řeči, ale prvků a abnormalit toku lidské řeči, které jsou charakteristické pro různé situace, proto není závislá na jazyku, kterým posuzovaná osoba hovoří.

Technologie funguje na principu přednastaveného setu vokálních parametrů definovaných výzkumem v korelaci s klíčovými lidskými emocemi v různých kombinacích, aby byla schopna odhalit podvodné úmysly v běžných situacích. Technologie přináší řadu nových prozatím neobjasněných fonetických parametrů vycházejících z vlastností lidského hlasu. Přináší tak možnost rychlého posouzení osoby na informacích, imigračních kontrolách, check-inech apod.

- Videoanalýza

IP kamery disponují digitálním obrazovým výstupem, který je možné prostřednictvím SW zpracovávat. Pokud sledovaný objekt překročí prahovou hodnotu, SW předá obsluze alarmový stav a ta má možnost provést další opatření.

Sofistikovanější integrované systémy umožňují automatizaci reakce na vyvolaný poplach například spuštěním mechanických zábranných prostředků, elektrické požární signalizace, signálu atd. Na podobném principu pracují některé RTG na letištní třídírně zavazadel. [2] [3] [7]

## ZÁVĚR

Hrozba teroristického útoku se dotýká všech aspektů našeho života. Proto se neustále klade důraz na zdokonalování a vyvíjení moderních technologií, které v tomto boji proti terorismu mají pomoci v odhalení, odrazení útočníka a ubránění se útoku.

Kvalitní zbraní proti terorismu tkví v prolnutí několika oblastí a vytvoření tak co nejkomplexnější technologie. Je nutno podotknout, že ani nejdokonalejší technologie pro detekci nemohou být spolehlivé, pokud není i kvalitně připravené prostředí pro jejich začlenění do stávajícího systému.

**ZDROJE**


*[1] ČAJKOVÁ, Nikola. Teachers and Students Security Possibilities Against Terrorist Attacks on the U5 Building at TBU in Zlin. Zlín, 2019. Diploma thesis. Thomas Bata University. Vedoucí práce Pekař Libor, doc. Ing. Ph.D.*

*[2] ŠČUREK, Radomír. Speciální bezpečnostní technologie na ochranu osob a majetku. Ostrava, 2014. Odborné texty. Vysoká škola báňská –Technická universita Ostrava. Vedoucí práce Doc. Mgr. Ing. Radomír Ščurek, Ph.D.*

*[3] ŠČUREK, Radomír. Biometrické technologie - technické prostředky bezpečnostních služeb [online]. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2015 [cit. 20-09-29]. ISBN 978-80-248-3786-4.*

*[4] ABZ.cz: slovník cizích slov [online]. Praha, 2020 [cit. 2020-10-10]. Dostupné z: https://slovnik-cizich-slov.abz.cz*

*[5] CHUMCAL, Tomáš. Zajištění bezpečnosti na letišti pomocí profilace a identifikace cestujících. FBI, 2012. Diploma thesis. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Doc. Ing. Mgr. Radomír Ščurek, Ph.D.*

*[6] BRZYBOHATÝ, Marian. Terorismus I. 1. Praha: Ministerstvo obrany České republiky, 1999. ISBN 80-902670-1-7.*

*[7] MARŠÁLEK, Daniel. Zvýšení bezpečnosti civilního letectví detekcí podezřelého chování cestujících. Ostrava, 2015. Disertační práce. Vysoká škola báňská - Technická univerzita Ostrava - Fakulta bezpečnostního inženýrství.*