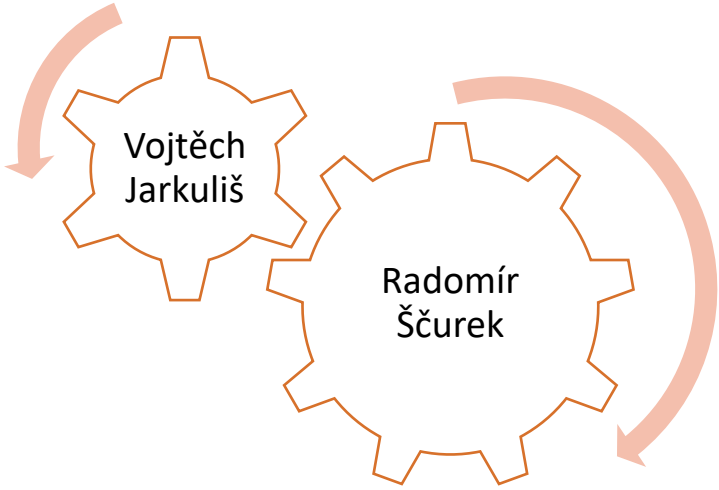
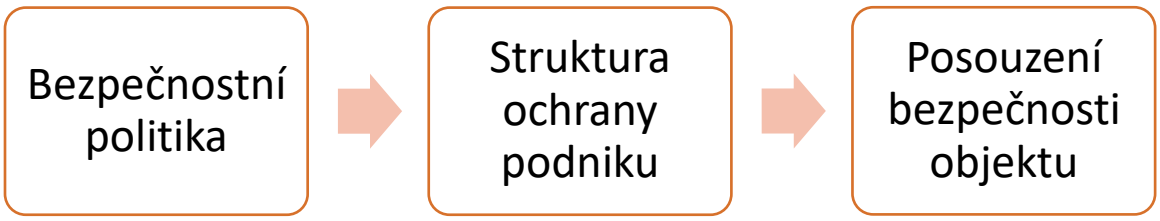
Studijní opora do předmětu:
Metodologie fyzické bezpečnosti podniku



Obsah

1. Vymezení bezpečnostní politiky podniku a řízení bezpečnosti organizace. Struktura ochrany podniku; metody posuzování bezpečnosti objektu. Segmenty fyzické ochrany podniku.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy týkající se bezpečnostní politiky podniku, s bezpečnostním management a samotným řízením bezpečnosti v podniku.

Cíl přednášky:

Student by měl po absolvování přednášky být schopen: rozčlenit fyzickou ochranu podniku a jednotlivé segmenty charakterizovat, vytvořit bezpečnostní politiku v obecném formátu, provést posouzení bezpečnosti objektu za využití kvantitativních a kvalitativních metod.

Literatura:

FRYŠAR, M. a kolektiv: Bezpečnost pro manažery, podnikatele a politiky, nakladatelství Public History ve spolupráci s Českou asociací bezpečnostních manažerů, Praha, 2006

UHLÁŘ, J.: Technická ochrana objektů 1.-3. díl, Policejní akademie ČR, Praha 2005

BRABEC, F., LÁTAL, I., MUSIL, R., PILNÝ, I., URBAN, M., VEJLUPEK, T.: Bezpečnost pro firmu, úřad, občana, nakladatelství Public History, Praha, 2001

Bezpečnostní politika
Souhrn organizačních a řídících opatření, norem standardů a pravidel, jejichž smyslem je ohodnotit informace o podnikatelských aktivitách a ostatní související fakta. Jedná se o ohrožení podniku, stanovení rizik a návrhy na ochranu podniku v rámci technologických, technických, organizačních a personálních opatřeních s důrazem na dodržování právních norem.

Je zde nutno odpovědět na tyto otázky:

- co má organizace v oblasti bezpečnosti činit, a z jakého důvodu
- jakých cílů v oblasti bezpečnosti chce dosáhnout
- jak budou řízeny jednotlivé podnikové činnosti a jaká opatření musí být provedena k dosažení požadovaných cílů.

Safety vs Security

Safety – selhání člověka	**Security – nebezpečný člověk**
BOZP	Ochrana osob
Požární ochrana	Ochrana majetku
Prevence závažných havárií	Ochrana informací
Technologická bezpečnost	

Fyzická ochrana (fyzická bezpečnost)
Soubor opatření k ochraně a rozvoji lidského systému.

Rozdělení

- **Fyzická ostraha**: prováděna vlastními silami, strážnými, SBS, případně policií
- **Režimová ochrana**: administrativně organizační opatření, která směřují k zajištění bezporuchového chodu celého systému
- **Klasická ochrana (MZS):** zabránění, ztížení narušení ochrany objektu
  - Perimetrická ochrana
  - Plášťová ochrana
  - Předmětová ochrana
  - Poloha (lokalita) objektu, situační ochrana (ochrana periférie)
- **Technická ochrana**: poplachové a zabezpečovací systémy (EZS), CCTV, systémy kontroly vstupu

Schéma bezpečnosti níže nám říká, že optimální bezpečnosti je dosaženo vyvážením všech složek bezpečnosti.

Koláč bezpečnosti ukazuje propojení fyzické ostrahy s technickou ochranou a režimovou ochranou, v případě absence jedné složky dochází k dysfunkci celého systému.

Pyramida bezpečnosti popisuje strukturu a jednotlivé segmenty ochrany podniku.

Riziko: kombinace pravděpodobnosti vzniku negativního jevu a jeho následku

Nebezpečí: stav při kterém vzniká nebo může vzniknout újma na chráněných zájmech

Ohrožení: soubor maximální dopadů v daném místě za specifikovaný časový interval s určitou pravděpodobností

Identifikace rizika: proces zjišťování toho, co může ohrozit chráněný zájem

Hodnocení rizika: komplexní proces určení míry rizika a stanovení opatření

Posouzení rizik

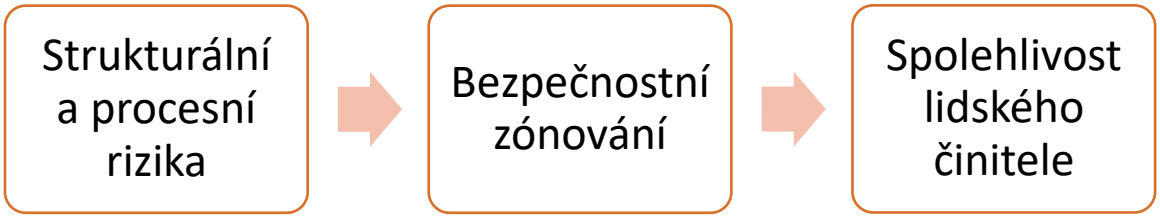
0. Rozdělení systémů na menší celky
1. Identifikace rizika
2. Modelování rizika
3. Analýza rizika
4. Opatření (Alara)

Rozdělení metod

Kvalitativní: expertní odhad, riziko vyjádřeno v rozsahu např. 1-10
Kvantitativní: matematický výpočet rizika z frekvence výskytu hrozby a jejího dopadu
Semikvantitativní: doplňují kvalitativní hodnocení bodovými hodnotami

2. Posuzování ochrany podniku z hledisek strukturálního a procesního. Zónování a metody kvantifikace selhání lidského činitele v ostraze podniku a zbytkové riziko.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti posuzování ochrany podniku z hlediska strukturálního a procesního, se zónováním a členěním částí objektů do jednotlivých segmentů a se základními metodami pro určení spolehlivosti lidského činitele při zajišťování fyzické ostrahy.

Cíl přednášky:

Student by měl po absolvování být schopen samostatně: definovat strukturální a procesní rizika a znát rozdíly mezi nimi, rozdělit středně velké objekty na jednotlivé zóny a v těchto zónách umět nadefinovat režimová a administrativní opatření, znát základní metody pro kvantifikaci selhání lidského činitele a určit míru možného zbytkového rizika.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Režimová a administrativní ochrana civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-882-3, vědecká monografie

DHILLON, Balbir. *Human Reliability and Error in Transportation Systems* [online]. Springer London, 2010 [cit. 2020-12-26]. ISBN 1849966516.

Procesní riziko: lidský faktor (zneužití zbraně, upadnutí na schodech)

Strukturální riziko: technické hledisko (prostříhání plotu, přelezení plotu, vniknutí na střechu)

Modelování rizika

- Ishikawův diagram: identifikace možných příčin problémů
- Strom poruch FTA: zpětný rozbor událostí (lampa nesvítí – selhání žárovky)
- Strom událostí ETA: průběh procesu od iniciační události – následují dvě možnosti příznivá a nepříznivá

Metodiky a metody pro řízení rizik

- **FMEA (**R=PxNxH)
- **FMECA (Failure Mode, Effects and Critically Analysis)**
- **Checklist**
- **SWOT**
- **WHATIF** (co se stane když)
- **HAZOP** (analýza nebezpečnosti a provozovatelnosti)
- **HVA**
- **HV index** (hodnocení dopadů havárie na životní prostředí)
- **CCA** (analýza přičin a dopadů)
- **RR** (relative ranking)
- **PHA** (předběžná analýza ohrožení)
- **HRA** (analýza lidské spolehlivosti)
- **CARVER**
- **Analýza souvztažnosti**
- **Forenzní audit**
- **Bezpečnostní audit**
- **Bezpečnostní prohlídka**
- **Winterlingova krizová matice**
- **HAZID** (Hazard Identification Study)

Software pro posuzování rizik

- **Aloha**
- **Effects**
- **Marplot**
- **TEREX**
- **Riskan**
- **NBC warning**

Kvantifikace selhání lidského činitele u fyzické ostrahy

Lidský faktor je nedílným prvkem fyzické ochrany, jehož spolehlivost se mimo jiné opírá o skutečnost, že člověk je zapojen do procesu bezpečnosti a často je klíčovým faktorem celkové spolehlivosti. Lidskou chybou rozumíme jednání nebo pokus o jednání, kdy dochází k překročení mezních hodnot parametrů daného systému. Lidské chyby lze kategorizovat následovně:

- Chyby, které jsou způsobeny chvilkovým výpadkem pozornosti - volba nesprávného postupu, kdy záměr byl správný.
- Chyby vzniklé nedostatečnými instrukcemi nebo proškolením - osoba neví, jak má postupovat, případně si myslí, že ví, co má dělat, ale učiní chybný krok.
- Chyby způsobené psychickeou nebo fyzické zdatnosti (důsledek nevhodného výběru pracovníka pro zastávání konkrétní pozice či činnosti).
- Chyby z nedostatku motivace nebo opatrného rozhodování při současném nedodržování směrnic - osoba špatně vyhodnotí situaci a následně volí postup řešení, který je v rozporu se směrnicí.
- Chyby manažerů vzniklé v důsledku například nedostatečně zajištěného školení pracovníků, nevyužití zkušeností z předchozích nehod.

Mezi nejčastěji používané metody kvantifikace selhání lidského činitele patří například metoda TESEO, metoda Shell, metoda ASEP, metoda HEART, metoda SLIM, metoda HCR korelací či databáze kvantitativních charakteristik lidských zásahů NUCLARR.

Metoda TESEO (Tecnica Empirica Stima Errori Operatori)

Je empirickou metodou pro odhad chyb operátorů, která byla vytvořena v roce 1980 autory G. C. Bello a C. Columbori. Tato screeningová metoda slouží ke kvantitativnímu hodnocení pravděpodobnosti selhání lidského činitele. Patří mezi nejjednodušší metody s nejmenšími kapacitními a materiálními zdroji. Odhalit spolehlivost lidského činitele lze pomocí aplikace pěti základních faktorů osobnosti. Míra pravděpodobnosti selhání operátora je vyjádřena jako součin všech těchto pěti faktorů, označených K1-K5.

- K1 = faktor typu činnosti (prováděná aktivita osoby), od činností jednoduchých ke složitějším
- K2 = faktor časový a stresový - vlivem aktuálních podmínek (normální nebo mimořádné)
- K3 = faktor osobních kvalit personálu - znalost, praxe a zkušenost
  K4 = faktor psychického stavu personálu
- K5 = faktor ergonomický - vytvoření pracovních podmínek

Pravděpodobnost lidské chyby samozřejmě závisí na všech shora uvedených faktorech, přičemž nejprve musí být určeny hodnoty pravděpodobnosti selhání lidského faktoru dle konkrétních situací. Při jednoduché rutinní činnosti, kratšímu trvání přechodné stresové situace společně s dostatečně vyškolenými pracovníky, kteří mají dostatečnou odbornost a praxi v konkrétních činnostech za předpokladu vynikajícího mikroklimatu a koordinovanosti s provozem, je riziko selhání lidského faktoru nízké a nehrozí pravděpodobnost vzniku havárie.

Model SHELL

Tento model se v současnosti využívá například v civilním letectví. Pomocí této metody lze znázornit model lidského činitele dle dílčích faktorů, které jsou vysvětleny následovně:

- S = software – postup
- H = hardware - stroj, nástroj
- E = environment - prostředí, ve kterém dochází k interakci S-H-L
- L = liveware - člověk, jedinec v centru zájmu
- L = liveware - lidé, se kterými je jedinec centra zájmu v nějakém vztahu

Pro lepší porozumění je níže popsána charakteristika rozhraní, přičemž centrem zájmu je L uprostřed, tedy jedinec:

- **L - H rozhraní** - zohledňuje vztah člověka a stroje
  L - S rozhraní - člověk ve vztahu k nefyzikálním aspektům systému, např. používaná symbolika, vzhled manuálů, počítačové programy
- **L - E rozhraní** - adaptace prostředí fyziologickým potřebám člověka (např. snižování hlučnosti v letectví)
  L - L rozhraní - jedná se o rozhraní mezi lidmi a fungování týmu jako celku, proto je kladen důraz na týmovou spolupráci, vůdcovství či mezilidské vztahy obecně

3. Kultura bezpečnosti ve fyzické ochraně, typologie firemní kultury, aplikovaná myšlenková mapa, grafické modelování nebezpečí a Paretův princip represe a prevence v ochraně podniku.

Základní pilíře:

Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti firemní kultury z bezpečnostního pohledu, ukázat mu příklad aplikace myšlenkové mapy, modelování nebezpečí ve fyzické bezpečnosti a Paretova principu pro efektivní management rizik a s represivními a preventivními opatřeními v ochraně podniku.

Cíl přednášky:

Student by měl po absolvování přednášky být schopen: definovat základní pojmy bezpečnostní kultury, aplikovat myšlenkovou mapu a několik základních metod pro modelování nebezpečí s následnou aplikací Paretova principu, znát principy represivních a preventivních opatření při ochraně podniku.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Technologie fyzické ochrany civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-862-5, vědecká monografie

BHUSHAM, N. I., KANWAL, R. Strategic Decision Making: Applying the Analytic Heirarchy Process. Londýn: Springer – Verlag, 2004. 200 s. ISBN 1-8523375-6-7

Kultura bezpečnosti ve fyzické ochraně

Kultura bezpečnosti je podstatnou součástí podnikové kultury. Je spojena s významem bezpečnosti na pracovištích. V návaznosti si musíme uvědomit, že pracovníci využívají různé, technologie jejichž složitost postupně roste. Někdy jen nepatrná chyba může způsobit závažný následek. V rámci pracoviště se dále mohou vyskytovat nadlimitní hodnoty např. hluku, prachu, které představují pro jedince možnost vzniku zdravotních potíží, popř. onemocnění. Rizikové aspekty se také týkají interpersonálních vztahů na pracovišti. Nakonec to jsou tedy charakteristiky daného jedince, jeho schopnosti, dovednosti, které se podílejí na úrovni bezpečnosti práce.

Kultura bezpečnosti musí prostupovat všechny úrovně organizace. Jde o to, do jaké míry jednotlivci:

- cítí svou osobní odpovědnost za bezpečnost,
- jednají s ohledem na zachovávání, zvyšování a sdělování starosti o bezpečnost,
- se snaží aktivně učit, přizpůsobovat se a upravovat své chování s ohledem na předchozí zkušenosti,
- jsou odměňováni s ohledem na výše uvedené aspekty.

Základním předpokladem je zde jasné vymezení, definování toho, co je pro danou organizaci z hlediska bezpečnosti přijatelné.

1. Mezinárodní komise pro atomovou energii definuje kulturu bezpečnosti jako **souhrn charakteristik a postojů u organizace i jednotlivců, které jako převažující prioritu dávají pozornost problematice bezpečnosti jaderných elektráren podle jejího významu**. Tato definice zdůrazňuje tři důležité body:

- Prvním bodem je důležitost kultury bezpečnosti jako podněcovatele postojů.
- Druhým bodem je zapojení celé organizace na mnoha úrovních i jejích jednotlivých příslušníků.
- Třetím je důležitost bezpečnosti jako převažující priority. Ačkoli je tato definice široce přijímána, říká málo o vzájemných vztazích, které jsou organizaci vlastní.

1. Merrit a Helmreich definují kulturu bezpečnosti jako **skupinu jednotlivců, vedených ve svém chování svým společným přesvědčením o důležitosti bezpečnosti a svým sdíleným pochopením, že každý člen ochotně podpoří skupinové normy a ostatní členy v dosažení konečného cíle**.

Jejich definice přidává další dva důležité body: účast každého člena a to, že se všichni účastní ochotně na základě společné víry v bezpečnost, spíše než na základě pouhého naplňování předpisů a norem.

- Zhuravlyov považuje kulturu bezpečnosti za „mentalitu“ nebo „stav mysli“ organizace nebo jednotlivce při činnosti v organizaci. Představuje kulturu bezpečnosti jako sdílený vzorec chování a jednání, který, jak věří, ovlivňuje veškerou činnost a interakce. Jeho definice popisuje všudypřítomnost kultury bezpečnosti jako způsob, kterým lidé myslí a pracují.
- Wert definuje kulturu bezpečnosti jako **pracovní prostředí, kde etika bezpečnosti prostupuje celou organizaci a chování lidí se soustřeďuje na prevenci úrazů pomocí kritického sebehodnocení, na proaktivní identifikaci managementu a technických problémů a vhodného, včasného a účinného řešení problémů ještě předtím, než se stanou kritickými**. Tato definice obsahuje „management“ jako klíčový faktor při prohlubování kultury bezpečnosti

a zdůrazňuje důležitost proaktivních opatření a trvalého zlepšování.

- Gellerův koncept „totální kultury bezpečnosti“ popisuje kulturu bezpečnosti jako aktivní péči každého jednotlivce o zdraví a bezpečnost druhých (Geller, 2000). Stejně jako v TQM - Total Quality Management, soustřeďuje se Geller ve své Totální kultuře bezpečnosti – Total Safety Culture na procesní management.
- British Health and Safety Commission (Britská komise pro BOZP) definuje kulturu bezpečnosti jako „produkt skupinových i individuálních hodnot, postojů, způsobilostí a vzorců chování, které určují angažovanost, styl a odbornost programů organizace v oblasti BOZP“. Tato definice je významná, protože zdůrazňuje důležitost angažovanosti – která vzniká z vzájemných vztahů a z odbornosti, jež vzniká ze školení a odborné praxe, z provozní zkušenosti.

Kultura bezpečnosti je nedílnou součástí celkové podnikové kultury, a tak do ní vstupují prakticky všechny aspekty ostatních složek kultury a je jimi výrazně a neopominutelně formována. Nelze proto uvažovat o zlepšování bezpečnostní kultury, aniž by zároveň neprobíhaly adekvátní změny podnikové kultury vůbec.

Kultura bezpečnosti se stává dominantní složkou organizační kultury podniku, což zejména platí pro zvýšeně rizikové provozy. Její funkcí je:

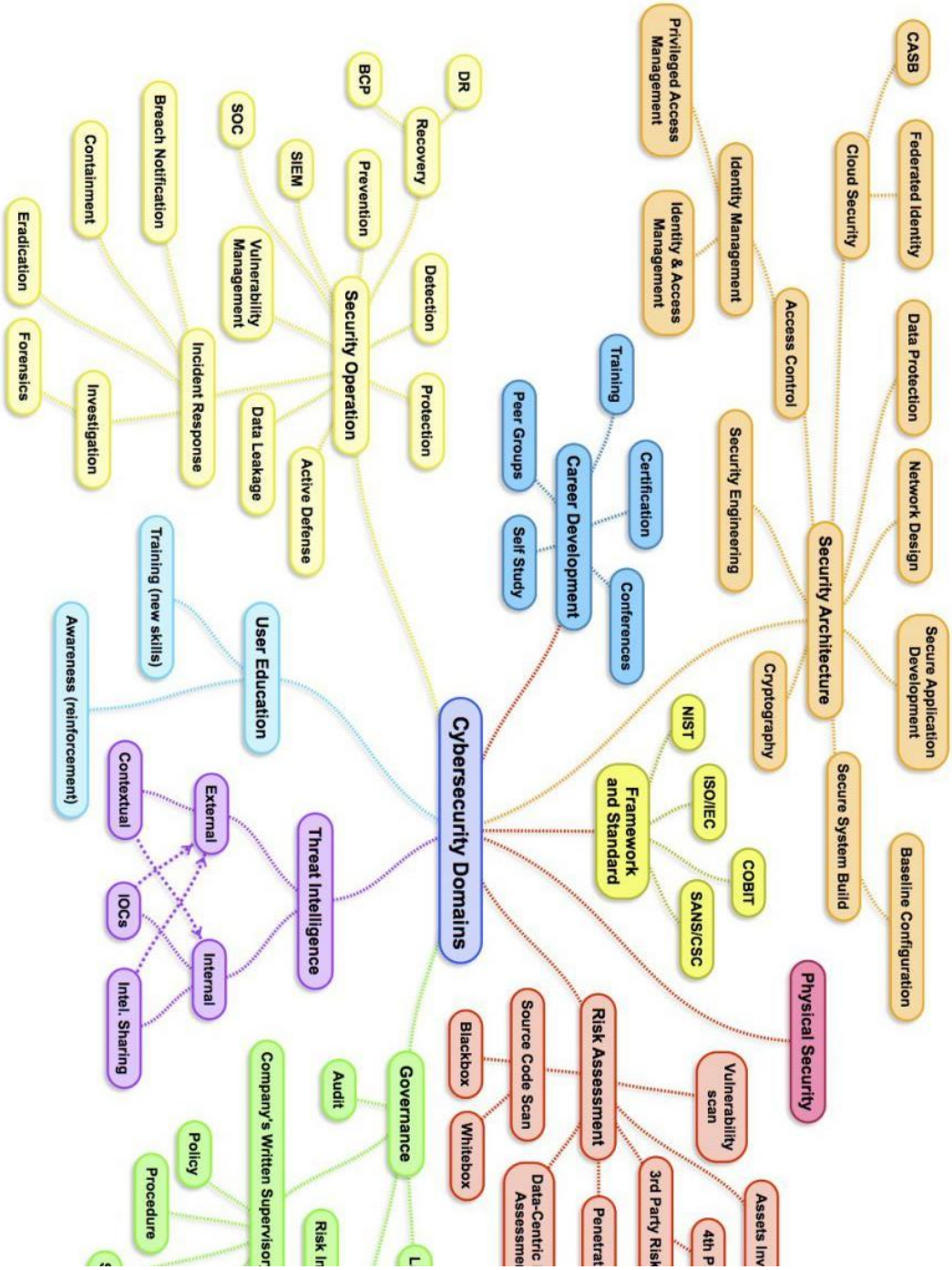
- redukce konfliktů uvnitř organizace, dostatečně silná podniková kultura podporuje soudržnost, konzistentnost vnímání problémů,
- zabezpečení kontinuity, usnadnění koordinace a kontroly, shodné vnímání hodnot a norem chování zjišťuje žádoucí chování a disciplínu,
- redukce nejistoty, vliv na pracovní morálku a emocionální pohodu – soulad mezi vnitřními normami pracovníka a organizační kulturou,
- motivace, pocit smysluplnosti práce, dává pracovníkovi pocit, že je důležitou součástí podniku,
- konkurenční výhoda – pokud je organizační kultura silná.

Smyslem formování kultury bezpečnosti je v konečném výsledku **dosahování co nejvyšší možné spolehlivosti lidského činitele** čili kvality pracovní síly zejména z hlediska spolehlivostních ukazatelů.

Kultura bezpečnosti práce v organizacích se odráží v míře pracovní úrazovosti a poškození zdraví zaměstnanců na pracovištích. Častou příčinou pracovních úrazů je selhání lidského činitele, které je právě úzce spojeno se zavedenou kulturou bezpečnosti a ochrany zdraví. Budeme-li v organizacích zlepšovat kulturu bezpečnosti práce, docílíme tím proaktivního přístupu v prevenci pracovních úrazů a poškození zdraví.

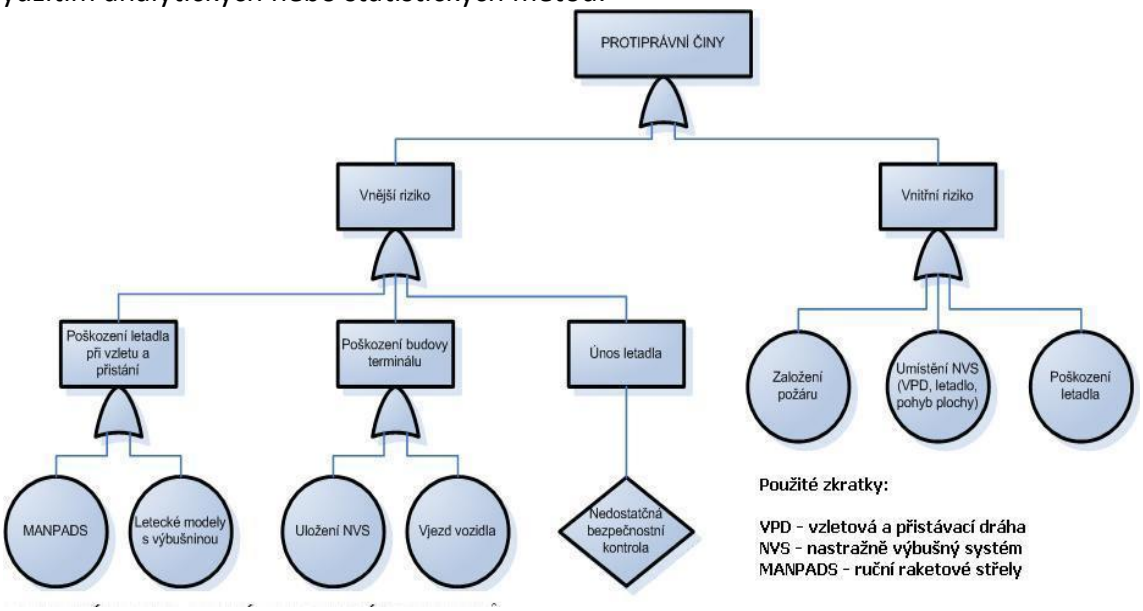
Myšlenková mapa

Je grafické uspořádání klíčových slov, doplněné obrázky vyznačující vzájemné vztahy a souvislosti. Může být využívána například k učení, plánování nebo řešení problémů. Do středu mapy zakreslíme klíčový objekt, jedná se o centrum naší pozornosti – jádro myšlenkové mapy, téma, nad kterým se chceme zamyslet nebo ho řešit. První myšlenku, která nás napadne, zaznamenáme nad pravý horní okraj jádra a tuto myšlenku rozvíjíme a heslovitě zaznamenáváme v daném ramenu, až do vyčerpání této myšlenky, přičemž jednotlivá hesla propojíme linkou. Další myšlenku zaznamenáme opět u jádra, pod první již vyjádřenou myšlenku. Začínáme hlavními tématy, jež s hlavním objektem přímo souvisí, a z nich pokračujeme dále vzdálenějšími motivy. Větve mají svá klíčová slova, popřípadě ilustrace. Jednotlivé klíčové pojmy jsou asociačními podněty, které by nám měly umožnit vybavit si celkovou informaci. V koncepci myšlenkových map je jasně patrná metoda řetězení.



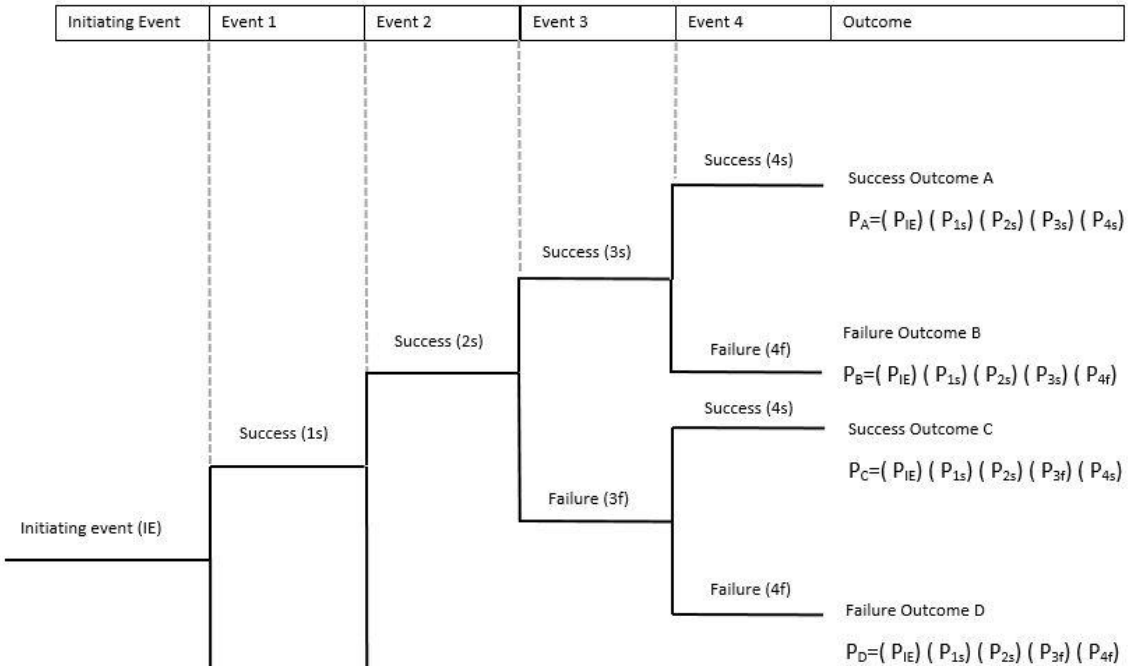
Fault Tree Analysis - FTA

Analýza stromem poruch je postup založený na systematickém zpětném rozboru událostí za využití řetězce příčin, které mohou vést k vybrané vrcholové události. Metoda FTA je graficko-analytická popř. graficko statistická metoda modelování rizik. Názorné zobrazení stromu poruch představuje rozvětvený graf s dohodnutou symbolikou a popisem. Hlavním cílem analýzy metodou stromu poruch je posoudit pravděpodobnost vrcholové události s využitím analytických nebo statistických metod.



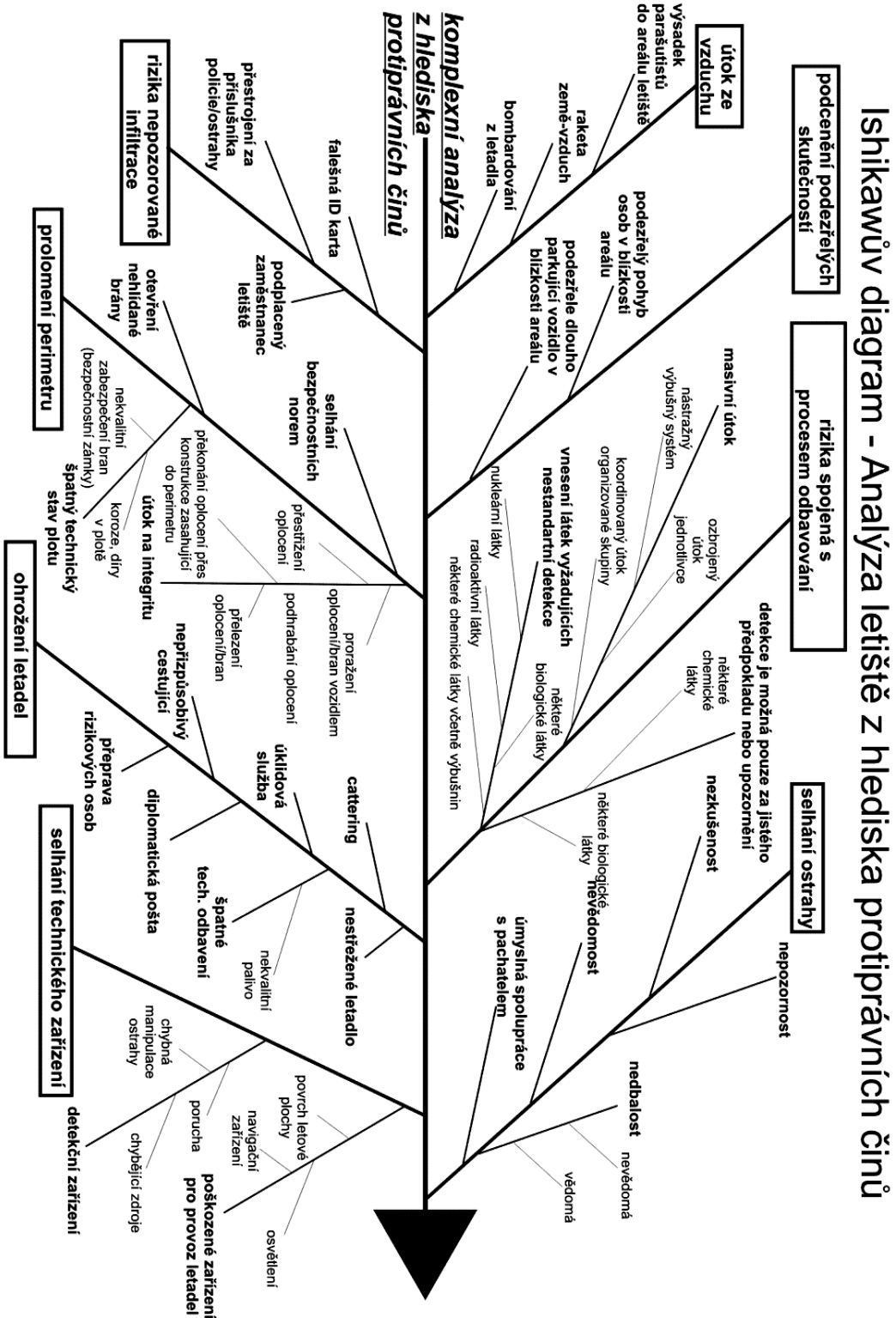
Event Tree Analysis - ETA

Analýza stromem událostí je postup, který sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Metoda ETA je graficko statistická metoda modelování rizika. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu.



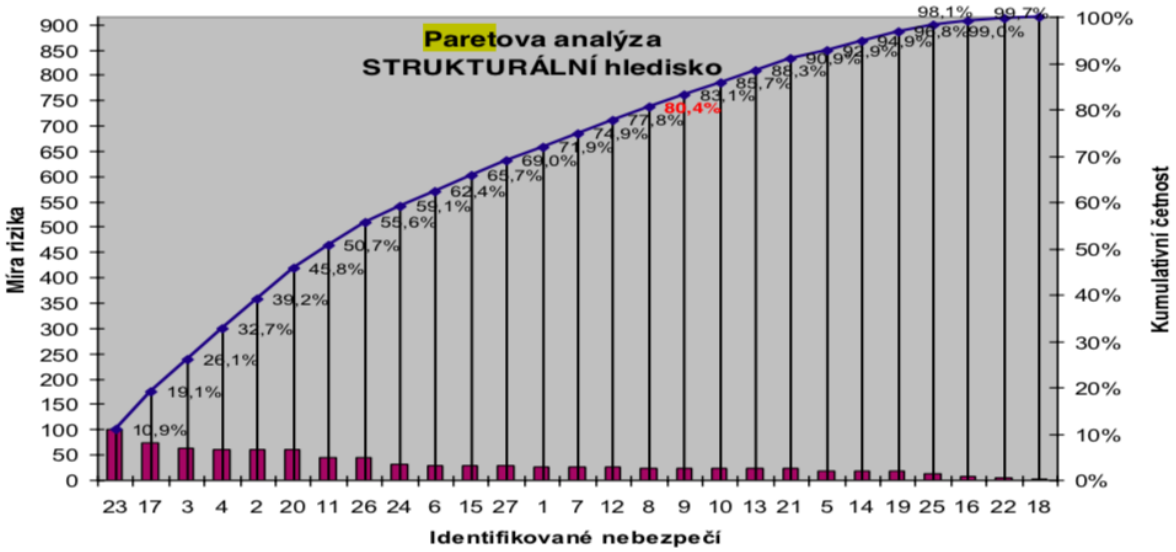
Ishikawův diagram

Tato technika pomáhá modelovat a strukturovat proces nebo identifikovat možné příčiny problému. Účelem je stanovení nejpravděpodobnější příčiny problému, který řešíme. V diagramu jsou formou grafického znázornění analyzovány zásadní faktory (příčiny), které způsobují řešený problém (následek). Každý zásadní faktor se dále analyzuje a hledají se dílčí příčiny.



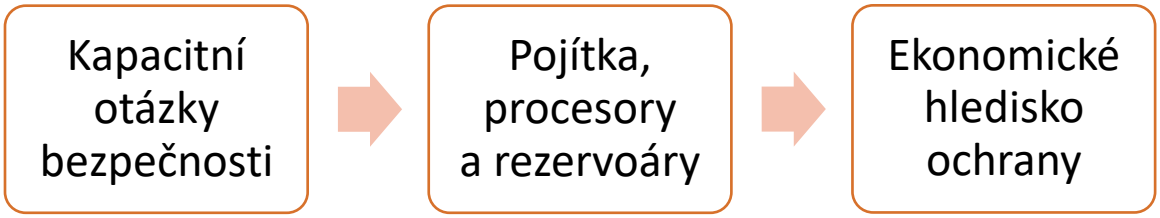
Paretův princip

Paretův princip, Paretovo pravidlo nebo též pravidlo 80/20 bylo formulováno na základě pozorování italského ekonoma Vilfreda Pareta. Podle Pareta pramení 80 % důsledků z 20 % příčin. Například 80 % zisku pochází jen z 20 % produktů. Paretovo pravidlo ve vztahu k fyzické bezpečnosti využíváme při aplikaci bezpečnostních opatření plynoucích z posouzení rizik na 20 % nejzávažnějších rizik s ohledem na ekonomickou stránku realizace vybraných opatření.



4. Kapacitní otázky zajištění bezpečnosti v podniku. Statická a dynamická kapacita pojítek, procesorů a rezervoárů, kapacitní špičky, ekonomické hledisko kapacitních řešení.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti kapacitních otázek zajištění bezpečnosti v podniku, statickou a dynamickou kapacitou pojítek, procesorů a rezervoárů a ekonomickým hlediskem kapacitních řešení.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen: vysvětlit rozdíl mezi kapacitními a projekčními otázkami bezpečnosti, definovat rozdíl mezi statickou a dynamickou kapacitou a umět vhodně naplánovat kapacitní systém, tak aby docházelo, k co nejmenší kumulaci osob v místech s největším rizikem vzniku protiprávního jednání a to s ohledem na ekonomickou stránku případných opatření.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Režimová a administrativní ochrana civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-882-3, vědecká monografie

KAZDA, Antonín a Robert E. CAVES. *Airport design and operation*. Third edition. Bingley, UK: Emerald, 2015. ISBN 1784418706id.

Pojítka: místa, která umožňují pohyb (pojízdné schody, chodníky, výtahy, schodiště.

Procesory: místa, kde jsou umístěny kontrolní body např. recepce.

Rezervoáry: čekárny, návštěvní místnosti a místa, kde se hromadí lidé.

Statická kapacita
Statická kapacita vyjadřuje počet osob nacházejících se v určité části budovy (nebo celku) v daném okamžiku. Stanovení hodnoty statické kapacity souvisí se znalostí celkového užitného prostoru a kvality poskytovaných služeb. Vztah má tedy následující podobu

$$Statická\ kapacita = \frac{užitný\ prostor\ (m2)}{standardní\ prostor/počet\ osob}$$

Vzhledem k tomu, že užitný prostor je většinou neměnný, statickaou kapacitu lze upravovat pouze změnou standardního prostoru.

Dynamická kapacita
Udává množství osob procházejících prostorem/objektem v daném časovém okamžiku, tímto časovým okamžikem je hodnota závislá na provádění operací. Dynamická kapacita obslužných zařízení udává rychlost obsloužení za jednotku času. Výpočet statické a dynamické kapacity bývá aplikován na kritická místa, pro něž je typická častá kumulace většího množství osob na malém prostoru. Pomocí výpočtů statické a dynamické kapacity je možno navrhnout optimální řešení, vedoucí ke snížení výskytu rizika napadení objektu. Čím větší je kapacita budovy (objektu), tím je vyšší riziko pravděpodobného útoku. Vyšší koncentrace osob ohrozí více lidí, útočník se může skrýt v davu s využitím nepozornosti bezpečnostních pracovníků, kterým tak snadno může uniknout.

Dynamická kapacita = Individuální obslužná rychlost * Množství obslužných zařízení

Významný prvkem využitelným při páchání protiprávních činů je z pohledu pachatele kapacita subsystémů např. u letišteních terminálů. Dle této kapacity lze vytipovat kritická místa s nejvyšší kumulací osob. Při posuzování kapacity terminálu letiště používáme parametry statické, dynamické a ustálené kapacity. U schodů, pásů, stanovišť a přepážek dochází ke zpomalení procesu při špičce, a to zvyšuje pravděpodobnost páchání protiprávních činů, protože obsluha nemá čas konat svou práci v dostatečné kvalitě. Řešit to lze zvýšením počtu obslužných zařízení, zaměstnanců ostrahy. Je potřeba se věnovat také parkovištím, kde je na malém prostoru velká kumulace osob a automobily mohou přispět při možném použití NVS k velkému výbuchu.

Čím větší je kapacita budovy (letiště), tím větší je riziko teroristického útoku. Větší počet osob zaujme více média, ohrozí více lidí, včetně vyšší pravděpodobnosti skrytí se v davu, nebo využití nepozornosti kontroly bezpečnostních pracovníků.

Ekonomické hledisko kapacitních řešení

Můžeme ho demonstrovat na příkladu civilního letiště, které funguje jako obchodní společnost, firma, která provozuje dlouhodobě svou činnost za účelem zisku. Příjmy letiště lze rozdělit na příjmy z leteckých a neleteckých činností. Větší aktivity letiště sebou přinášejí také zvýšené nároky na jeho bezpečnost. Z důvodu sezónnosti letecké dopravy představují neletecké činnosti prostředky k celoročnímu pokrytí provozu letiště a podílejí se rovněž na pokrytí nákladů na bezpečnostní opatření. Mnohá letiště na základě tržního principu investují do bezpečnostních opatření jen to, co ukládá zákon a preventivní zajištění bezpečnosti nad rámec zákonem stanovené povinnosti není pro ně nutností.

Vybírání poplatků patří k ziskům z leteckých činností. Jedním z vybíraných poplatků jsou například přistávací poplatky vypočítávané z maximální vzletové hmotnosti letadla v tunách násobené stanovenou sazbou pro letiště v měně dané země, nebo parkovací poplatky. Letiště také vybírají poplatky za každého odbaveného cestujícího. Tento poplatek se rovná počtu cestujících dané letecké společnosti a časovému úseku násobeno stanovenou sazbou pro letiště v měně dané země. Poplatky se vybírají i za služby při odbavení cestujících, zavazadel, pošty a nákladu. Technické odbavení letadla je předmětem smlouvy o pozemní obsluze, kdy hlavní podmínky odbavení a bližší specifikování služeb je upřesněno ve smlouvě, jež umožňuje kontrolu plnění nasmlouvaných služeb.

Připlácí se jen za specifické služby, např. požární asistence při plnění paliva, přetah letadla, nebo odmražení letadla v zimním období. K dalším zdrojům příjmů letiště patří příjmy z neleteckých činností, jako např.:

- pronájem budov, hangárů, skladů, ploch, opravárenských prostor,
- pronájem telekomunikačních služeb a informačního servisu,
- provozování parkovišť a garáží,
- pronájem a půjčování automobilů,
- pronájem a provozování ploch letiště pro maloobchodní činnosti,
- budování supermarketů a řetězců na letišti, provozování bezcelních obchodů a restaurací, kadeřnictví, jednacích salonků a služeb,
- příjmy z reklam,
- provoz cateringové společnosti,
- internetových a multimediálních kaváren, provoz heren a kasin,
- poplatky za provoz dopravy cestujících z městských center na letiště taxi společnostmi nebo hromadnou dopravou.

Za posuzování záměrů uživatelů a vydání případného zákazu realizace takového záměru na území letiště odpovídá letištní výbor pro bezpečnost.

Snaha o úspory v letecké dopravě částečně ovlivňuje také bezpečnost letecké dopravy. Například letecký předpis L 17 Bezpečnost, Ochrana mezinárodního civilního letectví před protiprávními činy, některá bezpečnostní opatření ukládá a jiná pouze doporučuje. S ohledem na nezávaznost letiště tato doporučení nenaplňují s odůvodněním, že plní vše, co zákon nařizuje, a doporučení nejsou závazná.

5. Koncepce prevence a metodika ochrany podniku jako měkkého cíle, komparace s tzv. tvrdými cíli, Crowd safety management (řízení bezpečnosti davů) a aplikace na vybrané objekty (letiště, škola).

Základní pilíře:

Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti prevence a metodiky ochrany podniku jako měkkého a tvrdého cíle, řízení bezpečnosti davů tzv. crowd safety management a následnou aplikací na vybrané objekty.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen: vysvětlit rozdíl mezi měkkými a tvrdými cíli a znát koncepci prevence a metodiky ochrany podniku, definovat základní principy řízení bezpečnosti davů a umět ho ve zjednodušené podobě aplikovat na vybrané objekty.

Literatura:

ČSN 73 44 00 Prevence kriminality - řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení

OTOOLE, William. *Crowd Management: Risk, security and health (Events, Management and Methods)* [online]. 2019 [cit. 2020-12-26]. ISBN 9781911396895.

Útočníci stále častěji zaměřují své útoky na nechráněná místa s větší koncentrací osob, bez ohledu na to, zda se jedná o nábožensky nebo politicky symbolická místa - tzv. „měkké cíle“. Ačkoli termín měkkých cílů (soft targets) není přesně definován, jedná se o místa s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům, která jsou pro tuto charakteristiku výběrem cíle ke spáchání útoků, kupříkladu teroristických. Oproti tomu tvrdé cíle (hard targets), jsou dobře chráněné a střežené objekty útoků, jde například o některé státní objekty, vojenské objekty, objekty bezpečnostních složek, ale i některé dobře chráněné či střežené nestátní či komerční objekty).

Rozdělení objektů na měkké a tvrdé cíle vychází z cílů útočníka, zaměřuje se na pravděpodobnost útoku. Přínosem takového přístupu je jistě skutečnost, že se zabývá ochranou subjektů, které by z hlediska tradičního pojetí nebyly do takovéto ochrany zahrnuty - například komerční objekty, soukromé osoby a jiné.

Do skupiny měkkých cílů patří mimo jiné například:

- školská zařízení, včetně studentských kolejí, menz, knihoven a studoven,
- obchodní centra, tržiště a obchodní komplexy,
- kina, divadla, zábavní centra,
- shromáždění, průvody, demonstrace,
- bary, kluby, diskotéky, restaurace a hotely,
- parky a náměstí, turistické památky a zajímavosti, muzea, galerie,
- sportovní haly a stadióny a v nich konané sportovní akce,
- vlaková a autobusová nádraží, letištní terminály,
- nemocnice, polikliniky a další zdravotnická zařízení,
- veřejná shromáždění, průvody, poutě,
- církevní památky a místa určená k uctívání a další.

Principy a fáze zabezpečení měkkých cílů

Při procesu vytváření bezpečnostního systému měkkého cíle je potřeba si v první fázi si ujasnit chráněné zájmy, tedy definovat, čeho si ceníme, o co nechceme přijít, co by nás poškodilo. Primárně se jedná o životy a zdraví osob před násilnými útoky, ale také o ochranu majetku, informací, hodnot či dobrého jména.

Druhá fáze procesu zahrnuje definování možného zdroje nebezpečí či hrozeb vůči chráněným zájmům. Při identifikaci je nutno se zaměřit na potenciální zdroje ohrožení za využití analýzy dosavadních útoků obdobného charakteru. Je potřeba zohlednit atraktivitu cíle z pohledu útočníka a reálné možnosti jeho zabezpečení. Bezpečnostní diagnostika ohrožení měkkého cíle vychází mimo jiné z vyhodnocení následujících faktorů:

- **Otevřenost pro veřejnost** - obecně platí, že čím je objekt otevřenější veřejnosti bez možnosti uzavřít perimetr a autorizovat vstupy, tím je atraktivita pro případného útočníka vyšší.
- **Vlastní bezpečnostní personál** - přítomnost bezpečnostních pracovníků z řad vlastního personálu či pořadatelské služby k plnění bezpečnostních úkolů opět atraktivitu cíle snižuje.

- **Množství a koncentrace osob** - pro měkký cíl je množství a koncentrace osob na určitém místě v určitém čase faktorem, který zásadně ovlivňuje zaměření bezpečnostního systému a proces přípravy jednotlivých bezpečnostních procedur.
- **Přítomnost policie** - pokud je v objektu trvale přítomna policie, působí jako výrazný odstrašující prvek a opět se jeho atraktivita pro případného útočníka snižuje, v tomto případ se však již nejedná o měkký cíl. Často je však policie přítomna pouze krátkodobě k zajištění veřejného pořádku pro konání konkrétní akce bez dostatečných zásahových dovedností.
- **Přítomnost médií** - pro útočníky je mediální přítomnost velmi přitažlivá, především v případě konání významných akcí s televizním přenosem v reálném čase.
- **Symboličnost -** zejména pokud jde o objekt, který je pro teroristy či jiné násilné skupiny symbolickým cílem (např. židovská, romská symbolika), ohroženost subjektu se významně zvyšuje. To vyžaduje zohlednění způsobů provedení útoků specifických násilných skupin a přizpůsobit svou bezpečnostní strategii i extrémním hrozbám.
- **Organizační struktura** - pro měkký cíl to znamená zpracovat bezpečnostní plán a řídit provádění bezpečnostních opatření ohroženého cíle. Více subjektů, které jsou v jedné ohrožené lokalitě (např. obchodní centra), vyžaduje koordinaci činností směřujících k zapojení všech a stanovení míry zodpovědnosti za bezpečnost daného prostoru, společně se sdílením případných nákladů.
- **Zdroje a prostředky na bezpečnost** - možnosti měkkých cílů přijmout vhodná opatření limituje rozpočet na bezpečnost a určení funkce bezpečnostního manažera, tedy osobu odpovědnou za bezpečnostní agendu organizace.
- **Schopnost identifikace vlastních rizikových situací** - faktor zkoumá, zda je subjekt schopen vyhodnotit rizikové aktivity a situace, zda je přítomen bezpečnostní manažer nebo jiný pracovník zodpovědný za bezpečnost a komunikaci s policií.

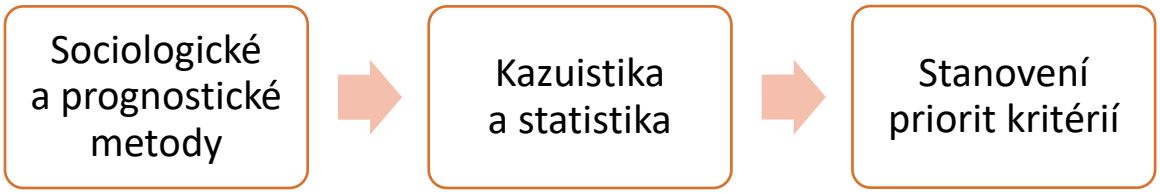
Komparace měkkých cílů s tvrdými cíly

Tvrdý cíl (anglicky hard target) je objekt s vysokým stupněm ochrany proti napadení a neoprávněnému vniknutí. Jedná se o dobře chráněné a střežené objekty, jako jsou například důležité státní objekty, vojenské objekty, objekty dalších bezpečnostních složek, ale i některé nestátní a komerční objekty. Oproti tomu měkké cíle jsou snadno dostupná místa s nízkou úrovní zabezpečení a ideálně velkou kumulací osob.

Crowd Safety Management neboli řízení bezpečnosti davů, jedná se o souhrný pojem, pod kterým si můžeme představit opratření a proaktivní kroky, které činíme, jako prevenci před potenciálními problémy. Jedná se tedy o souhrn opatření, kterými zamezíme vzniku negativních jevů při formování davů. Dalším pojmem, který se vztahuje k problematice řízení davů je **Crowd Control** neboli kontrola nad davem, když se začnou projevovat negativní jevy a je nutný zákrok policie popřípadě jiných bezpečnostních složek, aby se zabránilo dalším škodám a nebezpečí.

6. Sociologické a prognostické metody využívané ve fyzické bezpečnosti, kazuistika a statistika periferie podniku. Techniky stanovení priorit kritérií při minimalizaci rizika fyzické bezpečnosti.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti sociologických a prognostických metod využívaných ve fyzické bezpečnosti, s kazuistikami a statistikou periferie podniku, s technikami stanovení priorit kritérií pro minimalizaci rizik ve fyzické bezpečnosti.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen: rozlišit a definovat sociologické a prognostické metody, obecně se orientovat v kazuistikách a statistice periferie podniku, aplikovat elementární techniky pro stanovení priorit kritérií pro minimalizaci rizik ve fyzické bezpečnosti.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Režimová a administrativní ochrana civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-882-3, vědecká monografie

ŠČUREK,R., MARŠÁLEK, D.: Technologie fyzické ochrany civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-862-5, vědecká monografie

Sociologické metody

Statistická metoda: vychází z předpokladu, že všechno, co existuje, existuje v nějakém množství. Tuto metodu volíme při extenzivních šetřeních velkých populací. Pracujeme s vybraným vzorkem populace. Sociolog by měl garantovat, že zjištěné údaje jsou reprezentativní, že je lze na danou populaci zobecnit. Touto metodou můžeme sesbírat mnoho dat od mnoha respondentů, bohužel ale složité sociální problémy musíme zjednodušit pro potřeby statistického zpracování.

Monografická metoda: užíváme ji tam, kde máme zájem o hlubší analýzu problémů určitého menšího seskupení (škola, obec, sídliště apod.) Jde o výzkum jevu na jednom či pouze několika případech. Takový případ je zkoumán do hloubky a velmi podrobně. Použitím monografické metody a užitím příslušných technik jdeme sice do hloubky problému, ale naše závěry pak nemůžeme zobecňovat. Např. poznatky o životě jihomoravské vesnice nelze mechanicky aplikovat na život vesnice severočeské.

Experimentální metoda: jde o srovnávání dvou typů skupin (experimentální a kontrolní) v uměle navozené situaci. Jedna skupina je vystavena vlivu nějaké proměnné, druhá není. Rozdíl ve výsledcích u obou skupin se pokládá za vliv experimentální proměnné. Platný experiment lze provozovat jen v laboratorních podmínkách, proto se experiment v sociologických výzkumem moc nepoužívá.

Historická metoda: jde o zachycení procesu vývoje. Zkoumají se příčiny, podmínky a předpoklady, za kterých určitý jev vznikl, měnil se a vyvíjel, sledují se další vývojové tendence (např. vývoj rodiny jako společenské instituce, vývoj profesní struktury apod.)

Sociometrická metoda (sociometrie): je vhodná pro studium malých skupin a vztahů mezi jednotlivci. Skupiny charakterizujeme na základě zjištění sympatií a antipatií mezi jejími členy (podle ochoty či neochoty každého jedince s ostatními konkrétními jedinci sdílet nějakou určitou činnost). Tato metoda umožňuje měření a vyjadřování kvality a kvantity lidských (interpersonálních) vztahů. Sociometrie používá mnoho technik, např. sociometrický test (všichni účastníci testu si volí své partnery pro určité situace či společné činnosti), test rolí, sociodrama apod. Různé jsou i způsoby záznamu výsledků, často se používá tzv. sociogram (kruhový, terčový, individuální) či sociometrická matice. Vypočítávají se také tzv. sociometrické indexy (indexy, které měří status jednotlivých členů i indexy celé skupiny – index soudržnosti, index spojitosti, index skupinové integrace apod).

Sociologické techniky: řízený rozhovor, přímé pozorování, metoda sběru dat (analýza dokumentů), dotazník.

Kazuistika

Kazuistika nebo též případová studie patří mezi výzkumné metody a zabývá se popisem jednotlivých případů, např. vznikem, průběhem a vyléčením duševní choroby apod. Stejně jako jedince se může kazuistika týkat i skupiny lidí či instituce. Slouží jako pomoc a srovnání pro podobné situace. Jedná se o způsob práce s jednotlivým případem, kdy si přehledně (podle daného schématu) uspořádáme všechna fakta, která jsou nám o případu známa, a následně je analyzujeme. Díky metodě případových studií lze postihnout některé souvislosti, které nejsou na první pohled zjevné, a tím nám umožňuje pochopit celý případ do hloubky. Následně je pak zvolen adekvátní přístup k řešení celého případu.

Prognostické metody v bezpečnostní praxi

Bezpečnostní futurologie – předmět, který se zabývá budoucností vývoje bezpečnostní situace v regionech, oborech, odvětvích, objektech sociálních skupin atd. zpravidla vědeckým způsobem. Nesnaží se předvídat určitou konkrétní budoucí situaci, ale spíše se snaží podle dnešního trendu (vědecké analýzy) předvídat možná vývojová ohrožení i příležitosti.

Předpověď

- Vědecký základ = prognóza
- Libovolný, nevědecký základ = jasnovidectví, věštění, různá náboženská proroctví, pranostiky, životní moudra

Prognóza – vědecky zdůvodněné tvrzení o dosud neznámých, avšak relativně možných nebo skutečných faktech, lze dělit podle druhu závěru prognostického úsudku:

- podle předmětné oblasti – přírodní, společenské
- podle časového období – krátkodobé, dlouhodobé
- podle účelu, který se jejich vytvářením sleduje – strategické, perspektivní

Prognóza x hypotéza – jestliže tvrzení zaujímá v logickém úsudku místo závěru, jde o prognózu. Jestliže je naopak tvrzení součástí úsudku a může-li sloužit k odvozování jiných tvrzení o již zmíněných faktech, ovlivňuje- li tedy vysvětlení těchto (faktů), jde o hypotézu.

Intuice - „policejní čich“ - schopnost bezpečnostního pracovníka včas rozpoznat, vyhledat a analyzovat určitý jev, událost, skutek, které mají vliv na bezpečnostní situaci. Intuice hraje výraznou roli při odhalování pachatelů, hledání ztracených předmětů, předvídání určitých událostí, jevů.

- Talent, nadání – schopnost člověka chápaná jako možnost, potenciál, vloha, pro dosahování mimořádných výkonů.

Indicie – příznak, náznak, známka budící podezření, nepřímý důkaz (otisk prstů na vražedné zbrani dokazuje jen to, že ona osoba měla někdy zbraň v ruce, nikoli však také to, že s ní vraždu spáchala)

- kladné – umožňující zjištění určité skutečnosti
- záporné – vylučuje existenci určité skutečnosti, z právního hlediska méně hodnotné, ale i stejně spolehlivé.

Úsudek – myšlenkový postup, jimž se dostáváme od jistých předpokladů k určitému závěru.

Bezpečnostní prognózy

Účel: poznávat, předem očekávat, předpovědět bezpečnostní situaci v určitém objektu, okresu, kraji, atd.

Základ: využití vlastních nebo cizích chyb, především chyb zločineckého prostředí, informačních technologií, statistik. Neexistuje jednotná metodika (ve státním ani soukromém bezpečnostním sektoru). Bezpečnostní prognóza je složitější ještě v tom, že veškeré vstupní podkladové materiály mají omezenou platnost a mohou být i součástí utajovaných skutečností podle zákona.

Faktor času

- Krátkodobá prognóza – omezena na 1 rok, např.: okamžité a efektivní opatření
- Střednědobá prognóza – 3 – 5 let, např.: plánovací dokument pro zavedení bezpečnostního systému v určitém podniku
- Dlouhodobá prognóza – 5 - 10 let, státní administrativa (Nato, Interpol, BIS, MV, MO), např.: zakládání podniku komerční bezpečnosti. Základem je analýza (systémová, operativní, operativně technická). Analýza musí být všestranná (nesmí se týkat pouze jedné stránky jevu, ale musí ho analyzovat po všech jeho stránkách)

Faktor prostoru

Tím přesnější čím je užší objekt prognózy (bezpečnostní situace v továrně x bezpečnostní situace v Evropě)

Metodologie prognózování – způsob formování prognóz (statistická, analytická, historická)

- Empirický postup - metody založené na pozorování, měření
- Teoretické metody - založeny na ideovém zpracování údajů
- Metody založené na modelování a analogii - proces tvorby účelově zjednodušených zobrazení objektivní reality (zpravodajské služby – model agenturního aparátu, kriminální služba – model přepravy drog, v PKB – model fyzické ostrahy objektu)

Metoda prognózování – způsob, jak dosáhnout teoretického či praktického cíle při vypracování prognózy

- Universální metody (brainstorming, expertní panel, participativní metody, index stavu budoucnosti)
- Strukturální metody (systémová perspektiva, morfologická analýza a strom významnosti, kormidlo budoucnosti, analýza křížového účinku, textová analýza technologické prozíravosti, rozhodující technologie)
- Procesuální metody (analýza vlivů trendů, analýza megatrendů, Delphiho metoda, simulace a hry, scénáře, modeling rozhodování, vědecko - technologické cestovní mapy)

Universální metody

- Brainstorming - Vznikla jako protest proti dlouhým a neplodným poradám zpravidla ovlivněných vedoucím pracovníkem. Nástroj zbavení trémy, strachu z kritiky.
    - Účastnící řešení nemusí být jen odborníci v daném oboru, ale i lidé různé kvalifikace, která je v nějakém vztahu k řešenému problému (výrobce, spotřebitel, dopravce).

  - Počet účastníku: 5-12, délka trvání: 3 hodiny
  - Vyloučit zainteresované osoby na některém způsobu řešení, odstranění překážek v myšlení, názory zaznamenávány bez autorství
  - Cíl: stanovit úkol a vymyslet co nejvíce způsobů
- Metoda SYNECTICS
- Expertní panel - „parta chlapů kolem stolu“, 10 - 20 lidí, „porota znalců“, 3-18 měsíců vytváří řešení problému. Přínos v budoucnu: průmysl komerční bezpečnosti (PKB) a policie, policie a vojsko -> národní bezpečnostní strategie a koncepce (boj proti drogám)
- Participativní metody - metody sjednocování názorů v jednom oboru nebo v jedné komunitě lidí (Zefektivnění a usnadnění procesu politického rozhodování)
  - Výzkumy veřejného mínění
- SOFI – index stavu budoucnosti – zhoršování nebo zlepšování stavu budoucnosti
  - Kritéria: počet ovlivňovaných lidí, doba trvání vlivů, zda jsou změny vratné či nevratné

<u>Strukturální metody</u>

- Metoda perspektivy – řešení situací s velkými změnami (vražda na vesnici jistě vzbudí obrovský poplach, strach a paniku, zatímco ve městě půjde jen o „sdělení v novinách“)
  - Formulace potíží – hrozby a příležitosti, kterým organizace čelí, budoucí výsledky (důsledky), které nastanou, jestli nedojde ke změně
  - Plánování cílů – kreativní myšlení, 2 omezení (technické možnosti, operační proveditelnost) -> optimální řešení -> plánování prostředků (kdo by se měl podílet) plánování zdrojů (vstupy zaměstnanců, příslušenství, vybavení)
  - Realizace a kontrola
- Morfologická analýza a strom významnosti - definovány potřeby a cíle -> okolnosti, opatření a technologie k jejich dosažení
- Kormidlo budoucnost – název události se napíše doprostřed, přikreslení malých paprsků = dopady, důsledky. Další sekundární dopady vytvářejí druhý prstenec kormidla, pokračuje se až do doby, dokud nejsou vyjasněny všechny zobrazené dopady a důsledky (krádež automobilu v supermarketu – pokračuje se až k vyřešení problému = zadržení pachatele)
- Analýza křížového účinku – výpočet pravděpodobnosti výskytu určité události na základě známých pravděpodobností ostatních uvažovaných událostí a jejích vzájemných vztahů
- Metody krizových technologií – pro identifikaci nejvýznamnějších technologií použitých v určitém oboru v budoucnosti 10-15 let
  - 1. krok - výběr expertů
  - 2. krok - sestavení počátečního seznamu technologií
  - 3. krok - redukce seznamu (nebezpečí lobbingu)

<u>Procesuální metody</u>

- Sbližování trendů v časovém cyklu – základ: sledovaný proces za stejných podmínek se stejnými výsledky jak v minulosti, tak v budoucnosti
- Delphi metoda – dotazníkové šetření (dvě kola)
- Analýza vlivů směru vývoje – očekává určitý směr vývoje události, které mohou mít vliv na celkový vývoj bezpečnostní situace, předpoklad, že síly, které působily v minulosti, budou působit nadále

- Vědecko – technologické automapy – plánování a zkoumání vědecko technologického vývoje, mapy:
    - Produktové – cesta k požadovanému produktu
    - Nově vznikajících technologií – vznik a vývoj technologií
    - Problémové orientace

Techniky stanovení priorit kritérií

Metoda párového srovnávání (Fullerova metoda)

Tato metoda bývá nazývána Fullerovou metodou proto, že při její aplikaci sestavujeme váhy pomocí tzv. Fullerova trojúhelníku. Princip párového srovnávání je takový, že vždy porovnáváme dvě kritéria a z každé takové dvojice kritérií vybereme to důležitější. Srovnáváme-li každá dvě kritéria z celkového počtu k kritérií, vybíráme všechny kombinace dvou prvků z k. Pro větší přehlednost při srovnávání sestavujeme tzv. Fullerův trojúhelník. Trojúhelník má vždy k-1 dvojřádků. V prvním řádku jsou všechny kombinace pro porovnání s prvním kritériem, v druhém kombinace pro porovnání s druhým kritériem, kromě té, která je v předchozím řádku, v každém dalším řádku jsou kombinace pro porovnání s dalším kritériem, které nejsou v předchozích řádcích. Každý řádek má tedy o 1 člen méně, než řádek předchozí.

Kritérium	A	B	C	D	E	Součet
A	X	B	C	C	E	1
B		X	B	B	E	4
C			X	C	C	5
D				X	D	2
E					X	3

Kvantitativní párové srovnávání (Saatyho metoda)

Tato metoda je obdobou metody párového porovnání s rozdílem, že je navíc určena také hodnota důležitosti jednotlivých kritérií, která se určuje přiřazením počtu bodů (viz tabulka níže).

Počet bodů	Deskriptor
1	Kritéria jsou rovnocenná
3	První kritérium je slabě preferováno před druhým
5	První kritérium je silně preferováno před druhým
7	První kritérium je velmi silně preferováno před druhým
9	První kritérium je absolutně preferováno před druhým

1. Stanovení Saatyho matice
   a. S_{ii} = 1, prvky na hlavní diagonále jsou jedničky;
   b. $S_{ij} \in < 0, 9 >$, když i je preferováno před j, v opačném případě se zapíše převrácená hodnota
   c. $S_{ji} = \frac{1}{S_{ij}}$
2. Stanovení geometrického průměru i-tého řádku

$G_i = (\prod_{i=1}^{n} S_{ij})^{\frac{1}{n}}$

3. Stanovení normované váhy i-tého kritéria

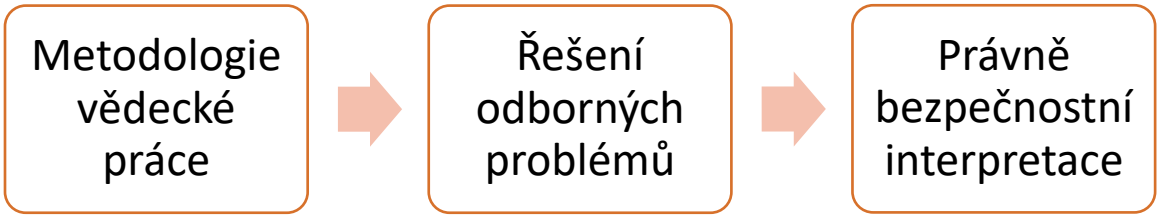
$V_i = \frac{G_i}{\sum_{i=1}^{n} G_i}$

Kritérium	K1	K2	K3	K4	Geometrický průměr	Normovaná váha
K1	1	5	1/3	1/5	0,76	0,14
K2	1/5	1	1/5	1/5	0,30	0,06
K3	3	5	1	1/3	1,50	**0,27**
K4	5	5	3	1	2,94	**0,53**
Součet					5,5	1

Další metody – bodovací metoda a metoda pořadí

7. Metodologie vědecké práce a řešení odborných problémů ve fyzické bezpečnosti obecně. Použití jazykového výkladu v právně bezpečnostní interpretaci.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti metodologie vědecké práce a řešení odborných předmětů ve fyzické bezpečnosti a právně bezpečnostní interpretace.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen: samostatně aplikovat vybrané metody vědecké práce, řešit odborné problémy a orientovat se v právně bezpečnostní interpretaci.

Literatura:

Vědecké metody ve společenských vědách (pro doktorandy)

ŠČUREK,R., MARŠÁLEK, D.: Technologie fyzické ochrany civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-862-5, vědecká monografie

Metody řešení odborných problémů a vědecké práce obecně

Výběr metod je tvůrčí práce. Každému zpracování odborné práce odpovídají nějaké metody, které jsou použitelné pro danou práci, jak ve fázi analytické (při získávání a zpracování faktů), tak ve fázi syntetické, hodnotící nebo shrnující. Jedná se o metody obvykle zpracovávané ve vědecké práci.

Hypotéza
Specifikuje výzkumný problém. Je možnou odpovědí na výzkumnou otázku a je formulována na základě dosavadních poznatků a teorií. Vyjadřuje vztahy, rozdíly nebo následky mezi proměnnými. Jedná se o tvrzení, které je vyjádřeno oznamovací větou v přítomném čase. Musí být falzifikovatelná (testovatelná), tzn. musí teoreticky existovat empirický postup, který může mít výsledek v rozporu s hypotézou. Elementární podmínkou je možnost měření proměnných použitých v hypotéze. Hypotézy s mnoha proměnnými jsou cirkulární, odkazují se na koncepty, které věda nezná, obsahují vágní a mnohovýznamové pojmy, jsou špatné hypotézy.

Hlavním účelem hypotézy je testování její pravdivosti, tj. konfrontace teorie z níž pochází s empirickými daty. Má nezanedbatelnou roli v experimentu. Konkrétnost hypotézy spočívá v uvádění předpokládaného výsledku.

Vlastnosti hypotéz: konkrétnost, smysluplnost (nepomáhají výzkumu), odůvodněnost (výzkum navazuje na jiné výzkumy či vlastní výzkumy – možný předpoklad výsledků).
Hlavní hypotéza – může obsahovat několik vedlejších
Nekonkrétní hypotézu – nelze ani potvrzovat ani odmítat
Nulová hypotéza – označována H0 – jedná se o hypotézu, kterou začínáme
Při rozhodování o přijetí hypotézy rozhodujeme na základě indukce.
Potvrzená hypotéza – musí dosáhnout argument alespoň 95% pravděpodobnosti výskytu. Výsledky se nedají odhlasovávat.
3 stupně statistiky – získání údajů, zpracování, vyhodnocení (rozhodnutí o významnosti)

Pozorování je základem každé práce, ve které jsou určité skutečnosti sledovány cílevědomě, plánovitě a systematicky. Výsledkem jsou skutečnosti a vysvětlení. Př. Porovnání pracovního dne, momentové pozorování atd. Jedním z druhů pozorování je měření → určení.
Teorie rozhodování se rozlišují příčiny, vyžadující nejprve zajištění a následně problémy u kterých je příčina známá, pokud není je třeba se jí zabývat. Problémy s jediným řešením či variantním.
Promyšlený způsob objektivně správný (postup, prostředek) či soustavu postupů umožňující nalezení či objasnění vědeckých poznatků a zákonitostí umožňující poznat daný objekt.
Metodologie – věda o metodách používaných v jednotlivých vědách.

Srovnávání (komparace)
Zjištění shodnosti či rozdílnosti stránek u dvou či více různých předmětů, jevů či úkazů. Srovnávat je možné stejné ukazatele i ve statistických souborech, lišících se věcně (dle skupin) prostorově (z hlediska umístění) časově. V případě užití ekonomických, finančních aj. rozborech používáme především tyto porovnávací formy: Plán (norma, standard) – tvorba daného plánu (normy, standardu)
Srovnání vývojové časové řady
Možnost užití srovnání je široké – jak při získávání poznatků a faktů, tak při zpracování. Jedná se o základní metodu hodnocení. Srovnání pojetím problémů, názorů a hypotéz

- Srovnání jako nástroj měření – zjišťování a objektivizace moc/málo, dobré/nedobré
- Tempo růstu dané ukazatelem
- Relativní srovnání (poměru), bezrozměrně

Analogie
Hledání obdoby, opírá se o metodu srovnávání. Myšlenkový postup na základě shody některých znaků usuzujeme shodu i dalších předmětů či jevů. Analogie poskytuje orientaci v těchto jevech. Každá analogie má své hranice, výsledky se mohou vlivem diferencovaných faktorů vzájemně kompenzovat.

Analýza a syntéza
Myšlenkové rozložení zkoumaného předmětu, jevu nebo situace či předmětů stávajících se předmětem dalšího zkoumání. Hlubší poznání – lepší a znalosti o jevu. Analýza předpokládá, že v určitém systému platí určité zákonitosti. Cílem je systém – jednotlivé rozhodovací prvky a jejich vzájemné vazby, poznat a odhalit zákonitosti fungování (chování) systému. Analýza a syntéza – nedílná součást jednoty, oba postupy se prolínají a doplňují. Přesněji by se mělo jednat o analyticko-syntetické poznávací postupy

Analýza – rozkládání: Nutné zkoumat základní vazby v jeho ekonomice, vytvářející učitý stupeň a kvalitu na vybavení práce technikou, ovlivnění produktu působícího na objem výroby a náklady. Dopracovávání se k základním momentům fungování.

Syntéza - skládání: *Myšlenkové sjednocení (spojení)* jednotlivých částí v celek. Při syntéze sledujeme vzájemné podstatné souvislosti mezi jednotlivými složkami jevu, a tím lépe a hlouběji poznáváme jev jako celek. Syntéza pomáhá odhalovat vnitřní zákonitosti fungování a vývoje jevu.

Analýza – získávání a zpracovávání faktů

- *Klasifikační analýzy*
- *Vztahové* – zkoumá závislost mezi jevy
- *Kauzální* – vyhledává a zkoumá příčiny jevů, nezkoumá systém, jen vnější vliv činitelů – užívání rozkladu syntetického ukazatele, využití pyramidové soustavy ukazatelů
- *Systémové* – zkoumá složitější systémy, probíhá obvykle ve 3 etapách (definování, analýza vlastností systému, návrh na změnu)

Výskyt analýz ve dvou formách – *syntetická* (dle podobnosti, poznatky a fakta do 3 tříd a dalších logických tříd – získání přehledného materiálu) a *analytická* klasifikace (vychází z určitého celku, množiny – syntetickou klasifikaci – rozložení prvků na podmnožiny).

Abstrakce – oproštění od jednotlivého (zvláštního, konkrétního). Myšlenkové oddělení nepodstatných vlastností jevu od podstatných, na základě tohoto zjištění podstaty jevu.

Indukce – vyvozování obecného závěru na základě poznatků o jednotlivostech. Induktivní úsudky mohou dojít až k podstatě jevů, zákonitostem. Typickou indukcí je statistické zpracování a zhodnocení reprezentativních souborů údajů umožňující formulaci obecnějších závěrů.

Dedukce – postup od obecného ke zvláštnímu. Způsob myšlení – od obecnějších závěrů, tvrzení k méně obecným.

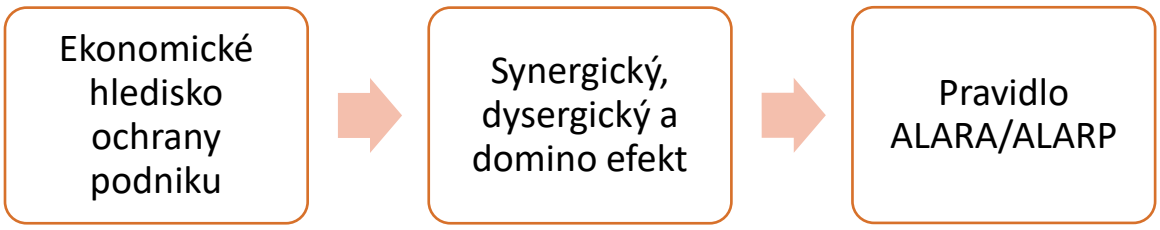
Analýza - logická metoda – použití při plnění cílů práce, při zjišťování současného stavu, při selektování potřebných údajů z velkého souboru informací potřebných na vytyčení charakter. vlastností, při zkoumání vyšetřovacích spisů

Syntéza – při vytváření manuálu procesu vyšetřování TČ, při aplikaci metod síťové analýzy procesu vyšetřování

Experiment – kvantitativní stránky určité vlastnosti, za účelem zvolení měřících jednotek. Je prováděno pozorování za kontrolovaných nebo řízených podmínek s cílem ověření pravdivosti určité hypotézy nebo teorie.

8. Ekonomické hledisko ochrany podniku; synergický, dysergický a domino efekt v bezpečnosti podniku, vliv právních předpisů na bezpečnostní ekonomiku, péče řádného hospodáře a porušování pravidel při správě majetku podniku, identifikace aktiv a pravidlo ALARP/ALARA v podniku.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy jako je: synergický, dysergický a domino efekt, vlivem právních předpisů na bezpečnostní ekonomiku a pravidlem ALARP/ALARA při stanovování opatření pro účely fyzické bezpečnosti podniku.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen definovat a na příkladu demonstrovat, co je to synergický, dysergický a domino efekt s popisem možných následků na stabilitu fyzické bezpečnosti v podniku, deskripce právních předpisů s vlivem na bezpečnost podniku a aplikovat pravidlo ALARP/ALARA, aby bylo zajištěno efektivní nakládání s finančními prostředky pro účely zajištění stanovené bezpečnostní úrovně podniku.

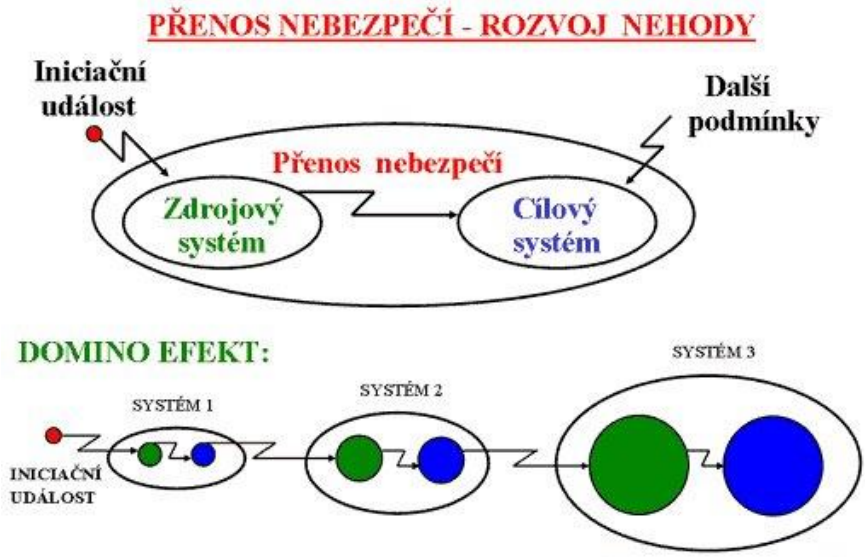
Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Technologie fyzické ochrany civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-862-5, vědecká monografie

ŠČUREK,R., MARŠÁLEK, D.: Režimová a administrativní ochrana civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-882-3, vědecká monografie

Synergický efekt
Výsledný účinek současně působících složek je větší než souhrn účinků jednotlivých složek. *(Symbolicky: 1+1>2).* Opačným jevem se projevuje dysergický efekt, kdy současným působením více složek dochází k menšímu efektu než by byla použita pouze jedna složka.

Domino efekt
Je definován v zákoně č. 224/2015 Sb., o prevenci závažných havárií jako možnost zvýšení pravděpodobnosti vzniku nebo následků závažné havárie v důsledku vzájemné blízkosti zařízení, objektů nebo skupiny objektů a umístění nebezpečných látek.



Péče řádného hospodáře
Pojem péče řádného hospodáře lze chápat tak, že řádný hospodář činí právní úkony týkající se obchodní společnosti odpovědně a svědomitě a stejným způsobem rovněž pečuje o její majetek, jako kdyby šlo o jeho vlastní majetek. Taková péče tedy nepochybně zahrnuje péči o majetek akciové společnosti nejen v tom smyslu, aby nevznikla škoda na majetku jeho úbytkem či znehodnocením, ale také, aby byl majetek společnosti zhodnocován a rozmnožován v maximální možné míře, jaká je momentálně dosažitelná. Problematiku péče řádného hospodáře upravuje občanský zákoník a zákon o obchodních korporacích. Ze zmíněných zákonů lze vyvodit několik znaků, kterými se posuzuje péče řádného hospodáře. První tři se nachází v občanském zákoníku a jsou jimi nezbytná loajalita, potřebné znalosti a pečlivost. Čtvrtý znak pak je uveden v zákonu o obchodních korporacích a je jím jednání jiné rozumně pečlivé osoby.

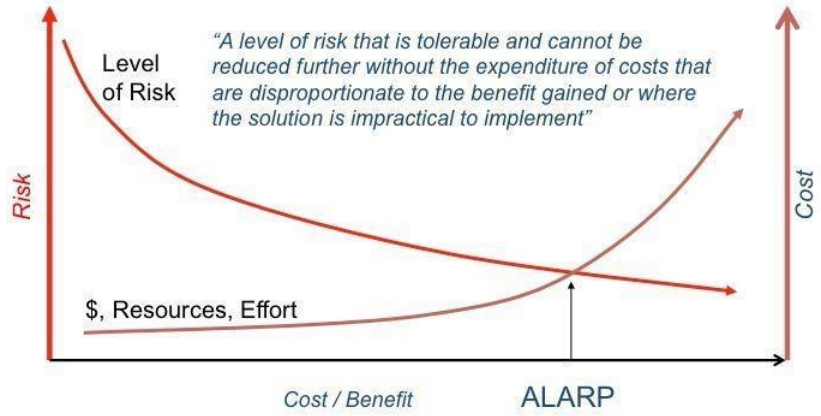
- **Loajalita:** V kontextu péče řádného hospodáře se nejedná o loajalitu ve vztahu k subjektu, ale ve vztahu k objektu, na němž je péče vykonávána. Jinak řečeno termín péče řádného hospodáře stanovuje kvalitu péče ke svěřené záležitosti, ale nevyplývá z ní kvalita jednání vůči osobě, která osobu povinnou daným jednáním pověřila.
- **Potřebné znalosti:** Co se týče potřebných znalostí, je potřeba zde rozlišit mezi odbornou péčí a péčí řádného hospodáře. Jednání s péčí řádného hospodáře neznamená, že pověřená osoba musí být schopna také odborné péče, ale musí být schopná vyhodnotit, kdy je odborná péče potřeba, tedy kdy je potřeba pro výkon činností zajistit kvalifikovanou osobu.

- **Pečlivost:** vyžaduje aktivní přístup ke svěřené záležitosti a rozumí se jí starostlivé a odpovědné jednání.
- **Jiná rozumně pečlivá osoba**: podle Mancelové (2015) se jinou rozumně pečlivou osobou v kontextu zákona myslí již řádný hospodář. Zůstává zde ale dostatek prostoru pro rozdílný výklad při soudních jednáních.

Porušování pravidel při správě majetku upravuje trestní zákoník

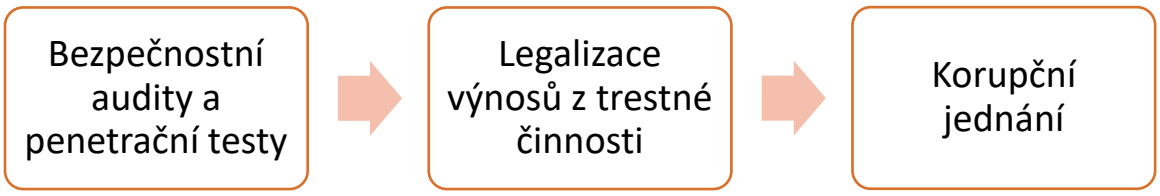
- **Porušení povinnosti při správě cizího majetku:** Kdo poruší podle zákona mu uloženou nebo smluvně převzatou povinnost opatrovat nebo spravovat cizí majetek, a tím jinému způsobí škodu nikoli malou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
- **Porušení povinnosti při správě cizího majetku z nedbalosti:** Kdo z hrubé nedbalosti poruší podle zákona mu uloženou nebo smluvně převzatou důležitou povinnost při opatrování nebo správě cizího majetku, a tím jinému způsobí značnou škodu, bude potrestán odnětím svobody až na šest měsíců nebo zákazem činnosti.

Ekonomické hledisko ochrany podniku a pravidlo ALARA/ALARP
(z anglického As Low as Reasonable Achievable/As Low as Reasonable Possible)
Riziko je nutné snižovat až na takovou úroveň, kdy se výdaje na snížení rizika stávají neúměrnými. Uvádí se 10 % hodnoty aktiv lze vyčlenit na zajištění bezpečnosti (v ojedinělých případech 15 %).



9. Podvodné jednání v podniku; audity, penetrační test a testy integrity v podniku, fenomén klientelismu, nepotismu, chráněnectví, korupce a legalizace výnosů z trestné činnosti a kazuistiky korupčního jednání, trestní odpovědnost, whistleblower.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti: podvodného jednání, penetračních testů, zaměstnávání příbuzných, korupce a legalizace výnosů z trestné činnosti, kazuistik korupčního jednání.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen definovat a rozpoznat podvodné jednání v podniku, provést bezpečnostní audit, penetrační test a test integrity, protiprávní jednání v oblasti legalizace výnosů z trestné činnosti a znát trestní odpovědnost za tyto činy a být schopen nastavit systém pro anonymní hlášení bezpečnostních incidentů v podniku.

Literatura:

BÉREŠ, Ján a Michaela KATOLICKÁ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* [online]. Wolters Kluwer, 2017 [cit. 2020-12-26].

DUNLAP, E. Scott. *Loss control auditing: a guide for conducting fire, safety, and security audits*. Boca Raton, FL: CRC Press, c2011. ISBN 9781439828861.

Nejčastější formy podvodného jednání

- Krádež majetku společnosti
- Střet zájmů
- Nezákonné výhody
- Korupce a úplatkářství
- Nepotismus
- Nedovolené užívání majetku společnosti

Penetrační testování

Tento proces zahrnuje podrobnou analýzu systému se zaměřením na případně bezpečnostní nedostatky vycházející z chybného nastavení systému nebo nedostatečných funkčních protiopatření. Analýza je prováděna z pohledu potenciálního útočníka a může vést k odhalení výše zmíněných nedostatků. Výsledky získané během analýzy jsou prezentovány vlastníkovi systému. Důkladné testy by měly k výsledkům přikládat také informace o reálných důsledcích jednotlivých nedostatků jak na systém samotný, tak na jeho vlastníka a měly by také doporučit možná protiopatření pro zmírnění rizika prolomení systému.

Testy integrity

Jsou v psychologii práce určeny k tomu, aby u zaměstnanců pomohly odhalit negativní aspekty jejich behaviorálních projevů – v návaznosti na kriminalitu, psychiatrickou léčbu nebo zneužívání drog a návykových látek. Zaměstnavatel si od detabuizace dané problematiky slibuje prevenci v rovině potencionálních problémů, způsobených na straně zaměstnanců, které se ale zásadně promítají do jeho vlastních ztrát. Důvodem jejich užití je tedy zejména ekonomické hledisko: společnosti chtějí ušetřit ekonomické ztráty na svojí straně v případě, kdy zvolí nevhodného kandidáta s nízkou integritou. Co se týká nákladů na tzv. opětovný nábor zaměstnanců (kdy je nutnost opakovaně obsadit stejnou pozici vhodnějším kandidátem), ty jsou až příliš vysoké a pro firmy kontraproduktivní.

Nepotismus

(z lat. nepos = synovec) označuje systém obsazování funkcí, v němž jsou preferováni příbuzní proti ostatním, nezřídka lépe kvalifikovaným kandidátům.

Legalizace výnosů z trestné činnosti

Proces legalizace výnosů z trestné činnosti lze rozdělit do tří fází.

1) Umístění – v této fázi dochází ke vstupu nelegálně získaných prostředků do finančního systému. Obvykle se tak děje rozdělením velkých částek na menší, méně podezřelé, jež jsou pak vloženy přímo na bankovní účet. Další cestou může být nákup řady nástrojů finančního trhu (šeky, peněžní poukázky), které se posléze shromáždí a uloží na jiném místě. Jakmile se peníze dostanou na finanční trh, nastává druhá fáze – rozvrstvení.

2) Rozvrstvení – představuje proces, v jehož rámci dochází k celé řadě převodů a přesunů finančních prostředků. Cílem je vzdálit je co nejvíce od jejich původu. Dochází tak buď k opakovanému nákupu a prodeji investičních nástrojů, nebo jen k jednoduché sérii převodů mezi několika účty a různými bankami.

3) Sjednocení – představuje poslední fázi na cestě ke zlegalizovaným prostředkům. Finanční prostředky se tak zpátky vracejí do legální sféry. Zpravidla jsou pak investovány do luxusních sídel a dalších nemovitostí nebo podnikání.

Praní špinavých peněz – zakrytí nezákonného původu výnosu
Praní špinavých peněz je ve světě přijatý termín pro legalizaci výnosů z trestné činnosti. Nejedná se ale o zcela přesné vyjádření, jelikož výnosem z trestné činnosti nemusí být jen peníze, ale třeba i cenné papíry, směnky nebo jakýkoliv majetek získaný trestnou činností. Jde o aktivitu, jejímž smyslem je legalizovat finanční prostředky získané nezákonným způsobem, tedy zisky z trestné činnosti, přičemž tato trestná činnost sama o sobě nemusí (ale také může) mít charakter ekonomické kriminality.

Praní peněz je vlastně poslední fází zahlazení stop nezákonného jednání, které současně umožní použít takto získané prostředky v legální ekonomice

a) Namáčení – shromáždění a rozmístění finančních prostředků.
b) Namydlení – zastření původu (nákup CP, nemovitostí, drahých kovů)
c) Ždímání – peníze se vrací ve formě legálního příjmu majitele.

Trestní odpovědnost – Trestní zákoník, část druhá, Hlava X, Díl 7, Organizovaná zločinecká skupina, § 361 Účast na organizované zločinecké skupině

(1) Kdo založí organizovanou zločineckou skupinu, kdo se činnosti organizované zločinecké skupiny účastní, nebo kdo organizovanou zločineckou skupinu podporuje, bude potrestán odnětím svobody na dvě léta až deset let nebo propadnutím majetku.

(2) Odnětím svobody na tři léta až dvanáct let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 ve vztahu k organizované zločinecké skupině určené nebo zaměřené k páchání vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(3) Odnětím svobody na pět až patnáct let nebo propadnutím majetku bude pachatel potrestán, je-li vedoucím činitelem nebo představitelem organizované zločinecké skupiny určené nebo zaměřené k páchání vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(4) Ustanovení § 107 a 108 se na pachatele činu uvedeného v odstavcích 1 až 3 neužijí.

Korupce
Je neformální vztah dvou subjektů jednajících v rozporu s dobrými mravy spočívající v nabídce, příslibu, realizování výhody v něčí prospěch nebo akceptování takového požadavku za vyžádanou, nabídnutou nebo slíbenou odměnu.

Obecně platná definice korupce, která vychází z níže uvedených atributů korupčního jednání platných pro všechny druhy korupce:

- vztah dvou subjektů – toho, kdo úplatek nabízí a toho, kdo jej přijímá,
- jde o směnný vztah, přinášející oběma stranám výhodu,
- souvislost s obstaráváním věcí obecného nebo institucionálního zájmu,

- korumpovaným je subjekt disponující určitým postavením, pravomocí,
- jde o jednání proti dobrým mravům.

Protiprávnost korupce - úplatkářství je v českém právním řádu upravena ve dvou základních rovinách:

- trestně právní jinak řečeno veřejně právní, kterou reprezentuje trestní zákoník,
- soukromoprávní, kterou reprezentuje obchodní zákoník.

Úplatkářství

Je jednou z forem korupce, která má na rozdíl od většiny ostatních forem korupce i rámec protiprávního jednání, naplňuje tedy znaky skutkové podstaty konkrétního trestného činu úplatkářství. Úplatkářství je užší vymezení korupčního jednání. Rozlišujeme úplatkářství aktivní a pasivní.

- Aktivní úplatkářství charakterizuje chování jednání osoby, která úplatek nabízí, slíbí nebo poskytne. Jde tedy o aktivní jednání osoby, která očekává za nabídnutý, přislíbený nebo poskytnutý úplatek nějakou konkrétní výhodu od protistrany, která je způsobilá očekávanou výhodu zajistit nebo alespoň přislíbit.
- Pasivní úplatkářství vyjadřuje jednání osoby, která je objektem uplácení to je osoby, která přijímá, žádá nebo si dá slíbit úplatek a jako protihodnotu poskytuje výhodu, obstarání věci obecného zájmu pro osobu, která poskytuje, nabízí nebo slíbí úplatek nebo jinou výhodu. V běžném slova smyslu lze korupci označit za jednání, kterým se na určitou osobu působí různými nenásilnými prostředky, aby osoba jednala buď proti dobrým mravům nebo proti svým úředním nebo morálním povinnostem.

Existují faktory, které korupčnímu chování přímo napomáhají a jejichž existence předznamenává možnost fungování korupčního prostředí. K těmto korupčním faktorům (kriminogenním faktorům) patří:

1. **Výše úplatku:** Nabízenému úplatku se špatně odolává. Základní otázka je, zda existuje hranice nabízeného úplatku, který je neodmítnutelný.
2. **Normativní systém:** Podstatně méně se bude dařit korupčnímu prostředí tam, kde působí oficiální systém norem, upravujících činnost veřejně činných úředníků, zejména pak veřejných činitelů. Součástí tohoto systému musí být i normy, které řeší případy korupce.
3. **Fungování administrativy:** Přemíra byrokracie, nejasnost fungování místní správy, státní správy, konfliktnost působení administrativy mezi sebou, neefektivnost a zdlouhavost vyřizování požadavků občanů je podhoubím korupce.
4. **Systém kontroly:** Nefungující nebo dokonce zkorumpovaný systém kontroly nevytváří dostatečnou hrozbu pro ty, kteří mají sklony k úplatku. Riziko odhalení korupčního jednání je nízké a vyplácí se.
5. **Korupční tradice**: Jsou země, kde korupce je považována za zcela normální, běžný jev, ba dokonce bez ní si běžné fungování společnosti nedokážou obyvatelé představit. Korupce je tak považována za normální, běžný způsob chování, je tolerována a úplatek se běžně očekává. Být zkorumpovaný se ve společnosti žádá.
6. **Sociální chaos:** Nastupuje zpravidla v těch společnostech, kde došlo k významným společenským změnám. Ten se projevuje nejen v každodenním životě, ale i v chodu institucí, státní správě a samosprávě.

7. **Kvalita státní správy:** Účinným protikorupčním jevem je silná, kvalifikovaná, výkonná a respektovaná výkonná moc, která má relativně dobře finančně ohodnocené úředníky.
8. **Klientelismus:** Jedná se o zvyk vyřizovat občanské záležitosti zákulisní cestou. Mimo pořadí, mimo pracovní dobu, prostřednictvím známých, na základě loajálnosti mezi úředníky, vzájemné úsluhy apod., to je silným kriminogenním faktorem korupce.
9. **Hodnotový žebříček:** Jedná se o osobní prospěch, osobní statky, bohatství, touhu rychle získat jmění apod.
10. **Chudoba:** Do jisté míry je protipólem kvalitní státní správy, například nízké platy státních úředníků, sociální nejistota, objektivně vysoké životní náklady vedou k bočním aktivitám kompenzovat chudobu.
11. **Korupční vzory:** Zde sehrává důležitou roli obecné povědomí a úzus, že úředníci jsou zkorumpovaní, čím silnější je takový úzus, tím náchylnější jsou ti, o kterých se hovoří, k úplatku.
12. **Vliv médií:** Míra objektivity a informační serióznosti sdělovacích prostředků má velký vliv na veřejné mínění a dokáže eliminovat nebo naopak rozpoutat korupční jednání.

Základní strategie boje proti korupci zahrnuje tři roviny:

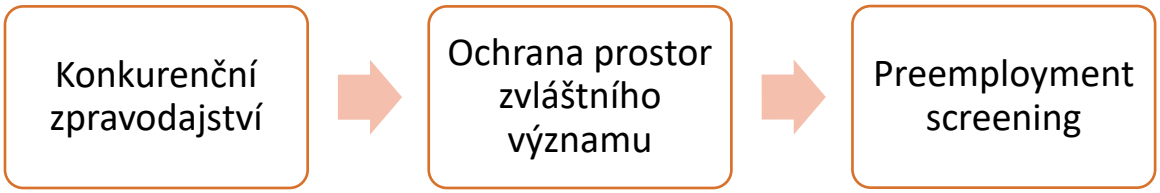
1. **Opatření na mezinárodní úrovni**
   - zprůhlednění podmínek přidělování mezinárodních dotací a jejich sledování k cílovému uživateli,
   - spolupráce s Evropskou unií proti zpronevěrám,
   - umožnění nezávislého auditu zahraničních partnerů.
2. **Opatření na vnitrostátní úrovni, zejména jde o vytváření**
   - nezávislých auditů,
   - kontrola finančních toků,
   - stanovení jasných pravidel pro poskytování dotací,
   - výchova politiků, funkcionářů, úředníků, občanů apod.
3. **Opatření ke snížení protikorupčních rizik u místní správy**
   - důkladnějším výběrem úředníků,
   - výcvikem, výchovou a kontrolou zaměstnanců.

Whistleblower (v angličtině doslova *ten, kdo hvízdá na policejní píšťalku)* je člověk, který veřejně vystoupí a upozorní na různá porušení (zákonů, nařízení, pravidel) nebo jiné nekalé praktiky jiného subjektu (osoby, firmy či korporace, státního orgánu).

Whistleblower může být jak například investigativní novinář, detektiv vyšetřující hospodářskou trestnou činnost, v několika výjimečných případech náhodný svědek, naopak asi ***nejčastěji zaměstnanec problémové firmy***. Podle jedné z definic je Whistleblowing uvážené a dobrovolné poskytnutí informací osobou, která má privilegovaný přístup k informacím a údajům o činnosti organizace, ve které působí nebo dříve působila. Toto poskytnutí informace se týká závažných protiprávních jednání nebo jiných nekalostí, které mohou ohrozit nebo poškodit veřejný zájem. Informace se týkají skutečností faktických nebo předpokládaných. Oznámení je zaznamenáno do veřejného záznamu mimo organizaci, která je předmětem oznámení, a je podáno takovému subjektu, který má pravomoc oznamovanou skutečnost vyšetřit a napravit. Osobě, která upozorní na nekalé jednání, se anglicky říká whistleblower.

10. Metodologie konkurenčního zpravodajství v podniku, mystery shopping, vetting, ochrana informací a prostor zvláštního významu podniku, personální preemployment screening, nástrahy.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy a definicemi z oblasti konkurenčního zpravodajství, mystery shoppingu, vettingu, ochrany informací a informační bezpečnosti a bezpečnostními prověrkami zaměstnanců.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen definovat konkurenční zpravodajství, pojmy jako mystery shopping, vetting, preemployement screening a aplikovat vybrané metody pro bezpečnostní prověřování zaměstnanců, potenciálních zaměstnanců, externích společností a dalších zainteresovaných stran s cílem minimalizovat vznik nežádoucích jevů, které by měly přímý nebo nepřímý dopad na fyzickou bezpečnost podniku.

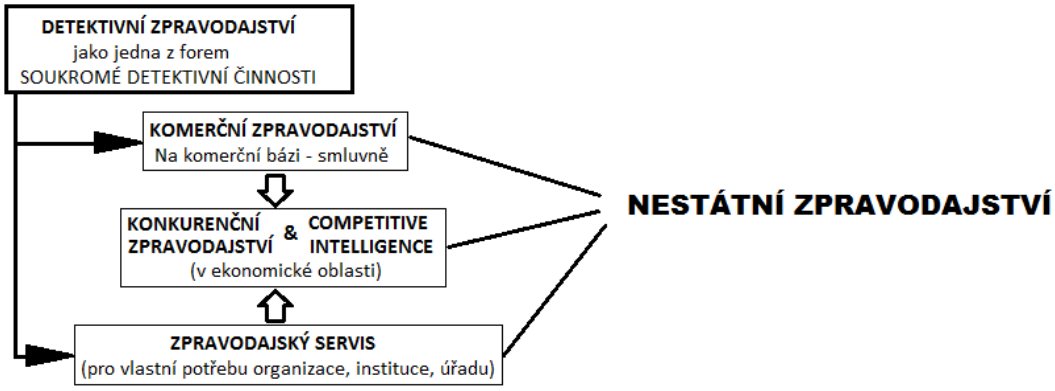
Literatura:

TYSON, Kirk W. M. *The complete guide to competitive intelligence*. 5th ed. Lisle, Ill.: Kirk Tyson International, c2010. ISBN 978-0966321951.

COLAPRETE, Frank A. *Pre-employment background investigations for public safety professionals*. Boca Raton, FL: CRC Press, c2012. ISBN 1439893853.

Zpravodajství představuje technologie (formy, metody a prostředky) a schopnost vyhledání, zpracování a distribuce znalostí a poznání. Souhrn relevantních informací k předmětnému problému představuje **znalost**. Souhrn znalostí v širších souvislostech představuje **poznání**. Úkolem zpravodajství je zpracovat data a informace do podoby relevantních informací ve vztahu k řešenému problému, tedy vytvořit znalost. Znalost pak dát do souvislosti a vytvořit poznání a toto ve „stravitelné“ (použitelné) podobě předat uživateli, který rozhoduje.

Nestátní zpravodajství
Realizace vědomého a systematického uplatňování zásad práce s informacemi a proces jejich přeměny ve znalost, a to mimo rámec státních orgánů a institucí. Napomáhá snížit nebo odstranit neurčitost v chování systému.



Subjekty nestátního zpravodajství
- OSVČ zabývající se komerčním zpravodajstvím
- Komerčně zpravodajské kanceláře
- Soukromé detektivní kanceláře
- Skryté subjekty komerčního zpravodajství (zpravodajské součásti PR agentur, reklamních agentur, komerční informační kanceláře)
- Subjekty nestátního zpravodajství tvořeného útvary vlastní organizace

Objekty nestátního zpravodajství
- Konkrétní fyzické osoby, politici a činitelé apod.
- Konkurenční podnikatelské subjekty
- Konkurenční politické strany, hnutí
- Organizace, instituce občanská sdružení
- Ekonomická sféra a situace
- Společenská sféra a situace
- Vědecko-technický výzkum
- Archivy, evidence, databáze

Roviny nestátního zpravodajství

1) Obranné
Jde o problematiku ochrany informací, dat, komunikačních a počitačových systémů v organizaci. Směřuje k ochraně aktiv chráněného subjektu (lidé, peníze, dobré jméno firmy, hmotný a nehmotný majetek firmy). Obranné zpravodajství zajišťuje personální bezpečnost, informační bezpečnost a ochranu před ofenzivním a vlivovým zpravodajstvím konkurence.

2) Ofenzivní
Zajišťuje informace potřebné pro rozhodovací procesy.

- V procesu třídění a analýzy z těchto informací vytřídit a zpracovat relevantní informace
- v procesu syntézy relevantní informace zpracovat na znalost o zadaném řešeném problému
- znalost zpracovat do formy přijatelné či požadované pro uživatele
- v předepsaném či požadovaném čase předat znalost v požadované době uživateli.

Externí komerční zpravodajství: zákazníci, dodavatelé, konkurenti, experti – databáze, média, internet, knihovny

Interní komerční zpravodajství: vlastní zaměstnanci - databáze

Technické prostředky zpravodajské činnosti:

- bezpečnostní (osobní zbraně, obušky)
- optické (dalekohledy, noktovizory)
- foto-video-audio (fotoaparáty, videokamery, audio záznamníky)
- vlivové = lobbing

Lobbing jde o prosazování zájmů (rozhodnutí) zpravodajskými postupy. Lobování je definováno jako nástroj vlivné zájmové skupiny, která prostřednictvím svých zaměstnanců či k této činnosti specializovaných lobbistů vytváří stálý nátlak na zákonodárce, ministry, členy byrokracie a výkonné moci za účelem ovlivnění jejich rozhodnutí ve vlastní prospěch.

Postupy: metody veřejné či cílené argumentace a věcného odborného přesvědčování, věcná argumentace

- asertivní přesvědčovací a argumentační metody
- demonstrativní metody (veletrhy, výstavy, reklama)
- metody cílené či veřejné dezinformace

Zpravodajská sociotechnika je psychologicko-pedagogicko – sociologická metoda – postup zpravodajských pracovníků, v našem případě nestátního (komerčního či konkurenčního zpravodajství), při získávání informací z primárních zdrojů (speciálních zdrojů detektivní a zpravodajské činnosti) speciálními zpravodajskými postupy. Je třeba si říci, že soukromý detektiv zabývající se nestátní či komerční zpravodajskou činností – komerční zpravodajský pracovník tím, že využívá sociotechnické metody, postupy a taktiky, „...využívá svou schopnost manipulace lidmi takovým způsobem, aby pomáhali v dosahování jeho vlastních cílů. Úspěch ve velké míře záleží na jeho znalostech.

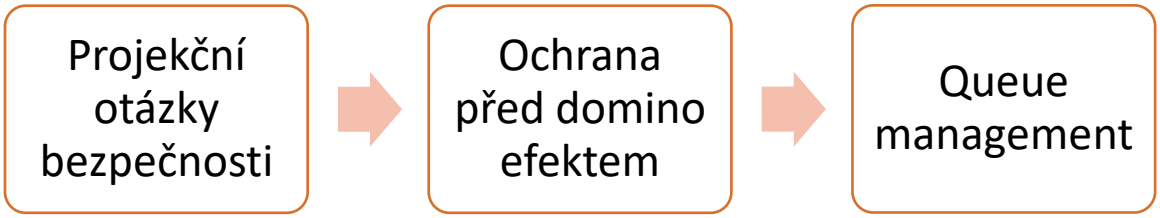
Sociotechnika již z definice zahrnuje jistý druh interakce mezi lidmi. Útočník bude na cestě k cíli velmi často využívat mnoho komunikačních metod a technologií. Při manipulaci obětí využívá psychologické postupy. Zejména v prvé řadě posoudí osobu (oběť) z hlediska jejích osobnostních rysů, zejména temperamentu. Máme-li poznat osobnost člověka (oběti) a manipulovat jím, je třeba poznat jeho podstrukturu motivační sféry. Podle toho pak také volí postupy a obsah motivace oběti s cílem jí ovlivnit. Motivací k ovlivnění může být kladná motivace i motivace formou vyvolání stresu či frustrace.

Mystery shopping je kvalitativní metoda výzkumu trhu, která měří maloobchodní kvalitu služeb nebo kdy se získávají informace o produktech a službách vlastní či konkurenční firmy. Mystery shopper je výzkumník, fiktivní nakupující, který vystupuje jako normální zákazník. Jeho úkolem je nákup výrobku, kladení otázek, registrace stížností nebo hraní určité role. Získává zpětnou vazbu o svých zkušenostech. Tato technika sběru dat eliminuje únik informací, na rozdíl od jiných výzkumných technik (např. dotazování, experiment). Záznamy se zpětnou vazbou vyplňuje výzkumník do dotazníku nebo může pořizovat audio a video nahrávky. Mystery shopping může být použit v každém odvětví. Nejčastěji se posuzují prodejny, kina, hotely, restaurace, zdravotnická zařízení apod. V oblasti hotelových služeb se používá i výraz mystery guest, například při ověřování klasifikace hotelu („hvězdičky“) některou z hotelových asociací.

Vetting je proces provádění ověření spolehlivosti u někoho předtím, než mu nabídnete zaměstnání, udělení ceny nebo prověření faktů před jakýmkoli rozhodnutím. Vetting můžeme doplnit pojmem **preemployement screening,** který je zaměřen výhradně na oblast nabírání nových zaměstnanců, oproti vettingu, kterým lze nazvat proces ověřování faktu i v jiných oblastech.

11. Projekční otázky zajištění bezpečnosti, předsunutá stanoviště ostrahy perimetru, labyrintové vstupy, ochrana před domino efektem u procesorů, pojítek a rezervoárů v podniku. Queue management - systém správy front a teorie fronty.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti projekčních otázek bezpečnosti, labyrintovými vstupy, ochranou před domino efektem u procesorů, pojítek a rezervoárů a řízením a správou front neboli tzv. queue management.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen deskripce projekčního hlediska bezpečnosti a popsání jeho základních částí jako jsou např.: předsunutá stanoviště, labyrintové vstupy, horizontální a vertikální dělení objektů, typy použitých stavebně konstrukčních materiálů a popsat systém správy front a ve zjednodušené formě ho také aplikovat ve vybraném objektu.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Režimová a administrativní ochrana civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-882-3, vědecká monografie

KAZDA, Antonín a Robert E. CAVES. *Airport design and operation*. Third edition. Bingley, UK: Emerald, 2015. ISBN 1784418706id.

Projekční otázky zajištění bezpečnosti

K páchání trestných činů lze zneužít projekční a kapacitní uspořádání budov (např. letiště). Jedná se například o umělé vyvolání nadměrné kumulace osob na jednom místě, což má za následek paniku a zmatek, kterou lze zneužít buď k neoprávněnému vniknutí, nebo realizaci protiprávního jednání.

Samotná kumulace osob a majetku může být možností, jak spáchat útok proti lidem například teroristickou organizací. Útočníci využívají velké kumulace osob na co nejmenším prostoru. Struktura objektů musí vycházet z počtu osob, které se v nich pohybují a dále musí být dimenzována část ploch, kde se osoby pohybují (např. tranzitní část haly letiště). Je potřeba zamezit páchání protiprávních činů a zabezpečit v případě letiště vstup a výstup lidí v hale.

Konstrukčně je to možné horizontálně v jedné úrovni a ve více úrovních – vertikálně. Projekční otázka bezpečnosti začíná již při samotném projektování objektu (plynulost pohybu). Bezpečnost budov a infrastruktury má především charakter architektonického řešení přístupových zón do jednotlivých částí objektů. Jedná se o rozdělení zón, kde mají přístup pouze zaměstnanci, proškolené a autorizované osoby. Tyto zóny musí být zabezpečeny vhodnými bezpečnostními a staveními prvky.

Stavebně – bezpečnostní prvky jsou například:

- přepážky
- dveře na kódy
- hlídané vjezdy
- závory
- brány.

Zaměstnancům jsou poté vystavovány identifikační karty podle úrovně přístupu do jednotlivých částí objektu. U letiště se používá rozdělení budovy na veřejný a neveřejný sektor, který se nazývá vyhrazený bezpečnostní prostor (Security restrict area – SRA). Veřejný prostor a neveřejný prostor musí být oddělen technickými zábranami, které jsou jasně označeny, udržovány v náležitém stavu a jejich konstrukce a rozměry zajišťují dostatečný stupeň ochrany před neoprávněným vniknutím do neveřejného prostoru. Průchody v těchto technických zábranách jsou střeženy, zamčeny nebo zajištěny systémem automatizované kontroly vstupu v kombinaci s nepravidelnou kontrolou hlídkami.

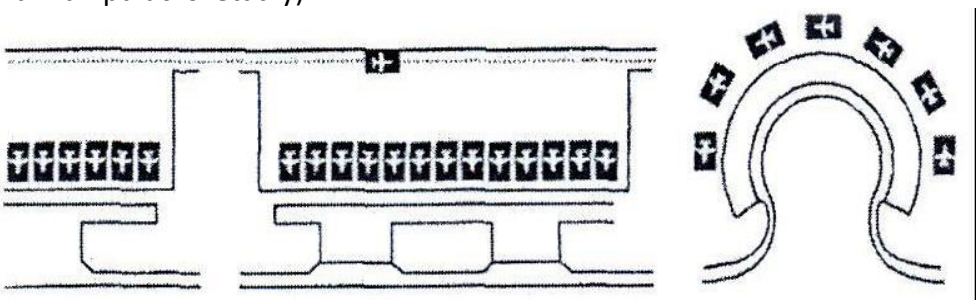
Prioritou je zabezpečení leteckých funkcí souvisejících se zabezpečením odbavovacího procesu a zabezpečení bezpečnosti proti protiprávním činům. Budova terminálu musí především zabezpečit bezkonfliktní pohyb proudů cestujících při příletu a odletu a z důvodu zajištění bezpečnosti tyto proudy oddělit. Oddělení proudů přilétávajících a odlétávajících je možné konstrukčně v jedné úrovni – horizontálně, nebo ve více úrovních – vertikálně.

Bezpečnostnímu systému malých letišť, vyhovuje jednoúrovňový systém. Pro velká letiště je vhodné vertikální oddělení cestujících ve dvou úrovních s použitím nástupních mostů a rukávů při nástupu do letadla. Ve světě jsou zaznamenány i trojúrovňové terminály, kdy je použit pro dopravu zavazadel samostatné patro, pod úrovní odbavovací plochy. Z bezpečnostního hlediska platí, že čím více proudů a úrovní, tím je větší riziko proniknutí neoprávněných osob

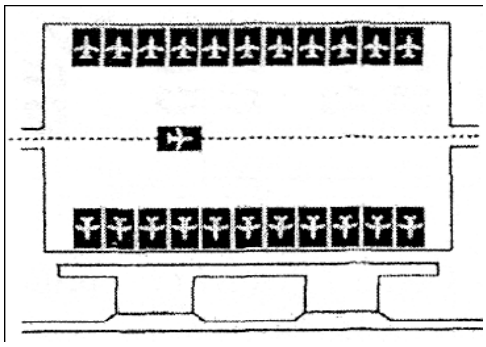
na plochu a do letadla, nebo naopak do země a v případě těchto více úrovní je nutné počítat se zvýšenými náklady na bezpečnostní opatření.

Při projektování odbavovacích hal je důležitá co nejkratší vzdálenost z odbavovací plochy na odletovou a příletovou dráhu (RWY), dále umožnění nezávislých pohybů letadel na sobě, dostatečný počet stojánků z hlediska špičkových hodin a slotů a splnění podmínek rychlého a plynulého nástupu a výstupu. Důležitý je prostor pro naložení a vyložení zavazadel a technické prostředky, či servis zajišťující odbavení letadla včetně minimalizace negativního vlivu na životní prostředí a možnosti dalšího rozšíření dráhy a odbavovacích ploch.

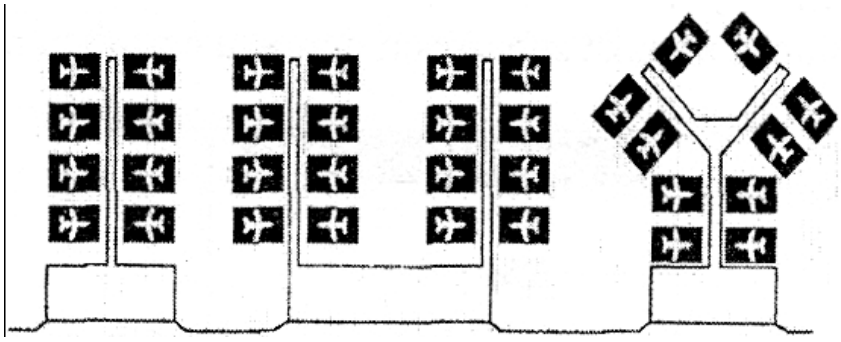
Rozvinuté uspořádání letadel (nejjednodušší uspořádání, nevýhodou je malá kapacita plochy na otáčení a manipulaci s letadly).



Uspořádání letadel na letišti systémem „otevřená plocha“ (vyloučen pohyb pěších cestujících, nutno využití autobusů, riziko křížení cest s vozidly zabezpečující technické odbavení u více letadel)



Ostrovní uspořádání letadel na letišti (výhodou je veliký prostor pro odbavení, nevýhodou komplikovaný systém oddělení přilétávajících a odlétávajících cestujících ve spojovacích tunelech)



Systém správy front

Systém správy fronty představuje sadu nástrojů a dílčích subsystémů, jež napomáhají k řízení toku zákazníků a čekací doby. Systém správy front zahrnuje také navyšování pozitivních zkušeností a zpětné vazby ze strany zákazníků. S řízením front je možné se setkat v řadě průmyslových odvětví, například v maloobchodu, školství, zdravotnictví, telekomunikacích či státní správě.

Typy front

- Fyzické fronty
- Virtuální fronty
- Mobilní fronty
- Strukturované fronty
- Nestrukturované fronty

Existuje řada technik využívaných pro měření a správu front při poskytování služby či zboží zákazníkům:

- Fyzické bariéry
- Přihlašovací a ohlašovací systémy správy front
- Systémy automatického měření front

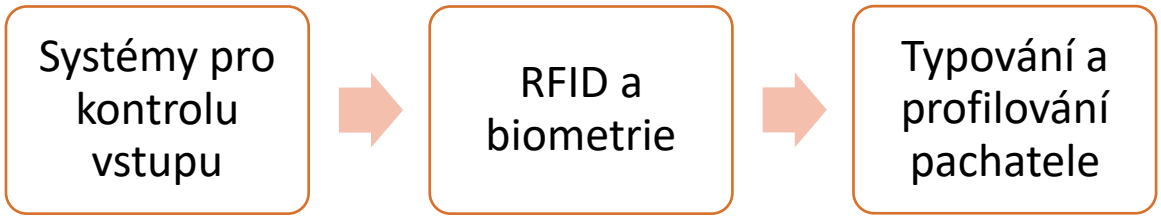
Teorie front

Teorie front (anglicky: *Queueing theory*) označuje soubor znalostí o očekávaném chování zákazníků ve frontách na základě explicitně stanovených předpokladů. Předpoklady jsou obvykle stanovovány pomocí různých matematických modelů, díky kterým je možné předvídat délky jednotlivých front, pravděpodobnou dobu čekání zákazníků a jejich chování ve frontě. Za přímý výstup teorie front je považováno měření účinnosti nebo provozní charakteristiky měřící výkon systému správy front.

V případě, že systém poskytovatele služeb či zboží splňuje podmínky základních modelů využívaných v teorii front, lze snadno využít vzorců, mezi které patří například Littleův zákon, ke stanovení předpokladů dlouhodobého jednání zákazníků v systému front. Jestliže tyto podmínky nejsou zcela splněny, nemusí být modely správy front plně odpovídající, tj. výsledky matematických výpočtů nemusí být pro konkrétní systém poskytovatele služeb či zboží přesné. Výstupy teorie front lze i přesto efektivně použít pro srovnání různých variant při optimalizaci v systému správy front. Z těchto a dalších důvodů je teorie front poskytovateli služeb či zboží považována za součást operačního řízení celého systému, protože výsledky procesu tvorby front a jejich šíření bývají stěžejní pro řadu obchodních rozhodnutí o přerozdělení zdrojů nutných k poskytování služeb či zboží.

12. Systémy kontroly vstupu do podniku, identifikace, autorizace a verifikace zaměstnanců a návštěvníků podniku, RFID, biometrika a biometrické technologie v bezpečnostní praxi podniku. Typování, dotazování, pozorování a profilování potencionálního pachatele v podniku.

Základní pilíře:



Anotace:

Přednáška seznamuje posluchače se základními pojmy z oblasti systému pro kontrolu vstupu do podniku, identifikace, autorizace a verifikace zaměstnanců a návštěvníků podniků, radiofrekvenční identifikací, biometrikou, typováním a profilováním potenciálního pachatele.

Cíl přednášky:

Student po absolvování přednášky by měl být schopen navrhnout funkční a efektivní systém kontroly vstupu do podniku za využití moderních technologií, jako jsou např.: biometrické čtečky, čtečky čipových karet a za využití dotazování, pozorování vytipovat a vyprofilovat potenciálního pachatele protiprávního jednání.

Literatura:

ŠČUREK,R., MARŠÁLEK, D.: Technologie fyzické ochrany civilního letiště. Akademické nakladatelství CERM, s.r.o., Brno, 2014, 978-80-7204-862-5, vědecká monografie

JAIN, Anil K., Patrick FLYNN a Arun A. ROSS. *Handbook of biometrics*. New York: Springer, c2008. ISBN 978-0-387-71040-2.

Rozpoznávání je proces, při němž dochází k rozpoznávání člověka na základě vhodné tělesné vlastnosti. Jedná se o druhotný termín, jenž nemusí znamenat nutně verifikaci nebo identifikaci.

Verifikace (ověřování) je proces, při němž dochází k ověření identity osoby systémem, jemuž je od začátku předložena ověřovaná identita. Při tomto procesu dochází k porovnání nasnímaného biometrického vzorku a referenční šablony. Verifikace je také nazývána porovnání 1 : 1 (při verifikaci může dojít k porovnávání 1 ku několika, jestliže je k identitě přirovnáno více šablon).

Identifikace je nazýván proces, při němž dojde k porovnání sejmutého biometrického vzorku se všemi referenčními šablonami v databázi. Identifikace se též označuje jako porovnání 1 : N nebo 1 ku mnoha. Tento proces je časově náročnější než verifikace a je závislý na velikosti databáze.

Autentizace při tomto procesu dochází k potvrzení hodnověrnosti identity dané osoby a přidělení statusu např. „oprávněný“ nebo „neoprávněný“, k němuž se pojí předem stanovená práva. Autentizace může probíhat jak při identifikaci, tak verifikaci.

Autentizace může probíhat na základě tří mechanismů k určení míry hodnověrnosti identity vstupujícího. Tyto mechanismy určují identitu tím:

- co člověk zná: heslo (levné, snadno realizovatelné, málo spolehlivé),
- co člověk vlastní: token,
    - paměťové – obsahují identifikační řetězec jednoznačně přiřazený konkrétní osobě (magnetické karty),
    - udržující heslo – pro vyslání identifikačního řetězce tokenem je potřeba zadat jednoduché heslo,
    - s logikou – token je schopen zpracovávat příkazy a reagovat na ně,
    - inteligentní – může komunikovat s uživatelem přes vlastní vstupní zařízení, může obsahovat časovou základnu atd.
- a čím člověk je: biometrie.

Velkou výhodou je, že ztráta tokenu je rychle zjistitelná a může být neprodleně zablokován. Může obsahovat více informací a může sloužit k prokázání do více systémů. Je obtížné ho padělat, a tím se zvyšuje bezpečnost. Nevýhodou je, že bezpečnost je závislá na složitosti tokenu a tudíž i na jeho ceně, navíc je token přenositelný. Bez tokenu se nelze autentizovat do systému, a jestliže je token poškozen nebo nefunkční, lze to jen velmi špatně zjistit.

Při biometrické autentizaci dochází k prokázání hodnověrnosti oprávněné osoby, že skutečně je tou oprávněnou osobou, v případě verifikace. Při identifikaci je hledaná osoba ztotožněna s identitou nebo neztotožněna se žádnou identitou v prohledávané množině identit. Zásadní rozdíl oproti předchozím způsobům autentizace spočívá ve faktu, že nelze při autentizaci jednoznačně odpovědět, zda předložená biometrická vlastnost skutečně patří oné osobě. Vždy tu bude nějaká nejistota, vyplývající z nemožnosti sejmout biometrický vzorek pokaždé naprosto shodě (uživatel neprovede snímání zcela shodně, dojde ke zkreslení signálu, podmínky snímání budou jiné atd.).

Na základě míry hodnověrnosti autentizace norma ČSN EN 50133-1 klasifikuje 4 třídy, které reprezentují **hodnověrnost**, že se skutečně jedná o osobu přijatou systémem. Při klasifikaci se bere v potaz riziko prozrazení oprávnění bez ztráty zachování možnosti vlastní autentizace:

- Třída identifikace 0 – žádná přímá identifikace – osoba se neprokazuje a je vpuštěna pouze na základě požadavku (tlačítko, senzor),
- Třída identifikace 1 – informace uložené v paměti (osobní identifikační čísla, čárové kódy, hesla), c) Třída identifikace 2 – identifikační prvek nebo biometrie (tokeny, fyzické klíče, otisky prstů),
- Třída identifikace 3 – identifikační prvek nebo biometrie spolu s informací uloženou v paměti (vícefaktorová autentizace).

Biometrii lze chápat jako: automatizované rozpoznávání lidských jedinců na základě jejich charakteristických anatomických a behaviorálních rysů. Rozhodnutí, zda daná vlastnost je vhodná pro automatizované zpracování závisí na splnění daných kritérií:

- **Univerzálnost:** každý člověk by danou charakteristiku měl mít. Toto kritérium nelze zaručit vždy a u všech. Mohou se najít případy, a většinou se najdou, kdy člověku není možno sejmout biometrický charakteristický rys, např. přijde o ruce nebo oči.
- **Jedinečnost:** vlastnost je unikátní pro každého člověka. Vlastnost má vysokou míru entropie a pravděpodobnost, že dvě osoby mají totožnou vlastnost, je minimální.
- **Stabilita:** vlastnost se časem nemění a zůstává zachována.
- **Získatelnost:** vlastnost je kvantitativně měřitelná.
- **Výkonnost:** zaručení vhodných pracovních a přírodních podmínek pro správný chod technologie a získání spolehlivých a přesných dat.
- **Přijatelnost:** ochota lidí akceptovat měření biometrické vlastnosti.
- **Odolnost: j**ak je vlastnost odolná proti falzifikaci.

Biometrický systém - automatizovaný systém schopný zachytit biometrická senzorová data uživatele, extrahovat data charakteristik z těchto zpracovaných získaných dat, porovnat zpracovaná data charakteristik s daty obsaženými v jedné nebo více biometrických šablonách, rozhodnout do jaké míry se shodují a indikovat, zda bylo nebo nebylo dosaženo identifikace nebo ověření identity.

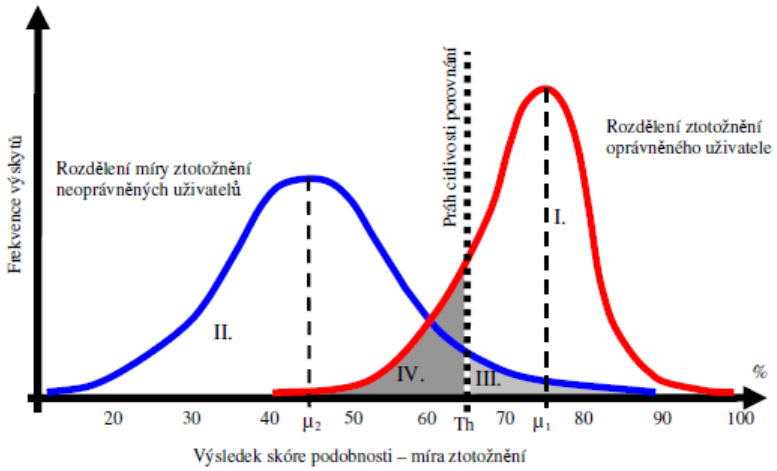
Rozhodnutí o identifikaci, verifikaci nebo autentizaci závisí na míře ztotožnění biometrického vzorku a šablony, která je vyjádřena porovnáním skórem podobnosti s prahovou hodnotou T.
Obě tyto hodnoty leží v intervalu <0;100>. Při porovnání dochází ke dvěma výsledkům:

a) jestliže $s \geq T$ je osoba přijmuta,
b) jestliže s < T je osoba zamítnuta.

Na základě těchto porovnání může u systému dojít ke čtyřem stavům:

1. správné přijetí – oprávněnou osobu přijme jako oprávněnou,
2. správné odmítnutí – neoprávněnou osobu zamítne jako neoprávněnou,
3. chybné přijetí – neoprávněnou osobu přijme jako oprávněnou (chyba II. typu),
4. chybné odmítnutí – oprávněnou osobu zamítne jako neoprávněnou (chybu I. typu).

3. a 4. stav jsou negativní a nežádoucí jevy, které slouží k hodnocení spolehlivosti a bezpečnosti biometrických systémů. Vyjadřují se jako míra chybného přijetí a míra chybného odmítnutí. Míry jsou velmi důležité k hodnocení výkonnosti systému a spolu s koeficientem vyrovnané chyby, dobou zápisu šablony a dobou ověření slouží jako ukazatelé při porovnávání jednotlivých systémů.



Míra chybného přijetí označována jako FAR (False Acceptance Rate) se *stanovuje jako podíl zaznamenaných transakcích provedených s nulovým úsilím útočníka, které byly chybně přijaty* 3. Je to vyjádření pravděpodobnosti, že systém dojde k chybnému závěru a neoprávněnou osobu přijme jako oprávněnou. FAR se stanoví:

$$FAR = \frac{N_{FA}}{N_{IIA}} \text{ nebo } FAR = \frac{N_{FA}}{N_{IVA}}$$

kde:
N_{FA} – počet chybných přijetí.
N_{IIA} – počet pokusů neoprávněných osob o identifikaci.
N_{IVA} – počet pokusů neoprávněných osob o verifikaci.

Hodnota FAR je důležitá z pohledu bezpečnosti, protože značí, s jakou pravděpodobností může dojít k bezpečnostnímu incidentu bez vynaložení prostředků útočníkem.

Míra chybného zamítnutí označovaná jako FRR (False Rejection Rate) *se stanovuje jako podíl zaznamenaných oprávněných transakcí, které byly chybně zamítnuty*. Vyjadřuje pravděpodobnost, že oprávněnou osobu systém zamítne jako neoprávněnou. Stanovuje se následovně podle:

$$FRR = \frac{N_{FR}}{N_{EIA}} \text{ nebo } FRR = \frac{N_{FRA}}{N_{EVA}}$$

kde:
N_{FR} – počet chybných přijetí.
N_{EIA} – počet pokusů neoprávněných osob o identifikaci.
N_{EVA} – počet pokusů neoprávněných osob o verifikaci.

FRR nemá tak velký vliv na bezpečnostní hledisko jako FAR, ale je uživatelsky nežádoucí. Dochází ke ztrátě důvěry v biometrický systém uživateli, kteří jsou donuceni podrobit se opětovnému snímání biometrické vlastnosti.

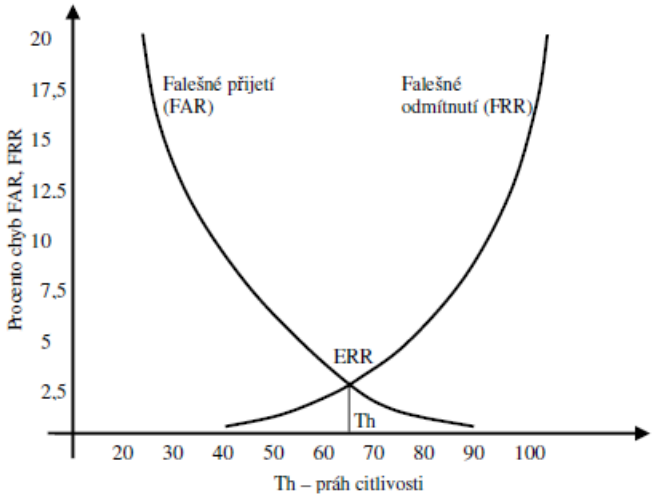
Míra selhání snímání je označována jako FTA (Failure To Acquire) jedná se o *podíl verifikačních či identifikačních pokusů, u kterých systém selže při snímání či lokalizaci vzorku s dostatečnou kvalitou* 5. Tato hodnota zahrnuje pokusy, při nichž nedošlo k autentizaci oprávněné osoby z důvodu, jestliže nemůže být sejmuta nebo dočasně předložena biometrická vlastnost (např. nemoc), jestliže algoritmem nebudou stanoveny biometrické charakteristiky ze vzorku, a jestliže biometrická charakteristika nedosahuje požadované kvality. Tato hodnota vypovídá o vhodnosti senzoru pro snímání dané biometrické vlastnosti.

Míra selhání registrace je označována jako FTE (Failure To Enroll) *je podíl populace, pro kterou systém selže při kompletaci procesu registrace* 6*.* V této hodnotě jsou zahrnuti lidé, kteří z důvodu nemožnosti předložení biometrické vlastnosti nebo ti, kteří nemají dostatečnou kvalitu vzorků při zápisu a nemohou být registrováni.

Míra chybné neshody označována jako FNMR (False Non-Match Rate) *je podíl vzorků získaných z pokusů oprávněných uživatelů, které jsou chybně deklarovány jako neshodné se šablonou stejné vlastnosti od stejného uživatele, poskytnuvšího vzorek.*

Míra chybné shody označována jako FMR (False Match Rate), je podíl vzorků získaných z pokusů neoprávněných uživatelů, které jsou chybně deklarovány jako shodné se šablonou jiné vlastnosti od jiného uživatele, poskytnuvšího vzorek. Tyto dvě hodnoty se podobají hodnotám FAR a FRR, ale nejsou do nich zahrnuty hodnoty vycházející z nemožnosti těch lidí, co se nemůžou zaregistrovat do systému (FTE), nebo těch, jejichž biometrická vlastnost nemohla být sejmuta (FTA). Hodnoty FTA a FTE ovlivňují jejich vypovídací hodnotu, kdy FTA zvyšuje hodnotu FRR a FAR snižuje a u FTE je to zcela naopak.

Míra vyrovnání chyb je označována jako EER (Equal Error Rate) a vyjadřuje hodnotu prahu citlivosti, při které bude míra chybné shody a neshody rovna, takže bude na základě chybného závěru chybně přijat a odmítnut stejný počet lidí. To umožňuje nastavení prahu citlivosti podle požadavků. Míra vyrovnání chyb slouží k porovnání jednotlivých systémů, kdy slouží jako ukazatel přesnosti. Porovnání samo o osobě však není jednoduchou záležitostí. Výrobci často demonstrují nejlepší dosažené výsledky, ale již neuvádějí jak k nim dospěli. To má za následek, že hodnota EER se pohybuje v dokumentaci kolem 1 % a ve skutečnosti to může být více než desetinásobek.



U multimodální autentizace dochází k tomu, že uživateli je sejmuto více biometrických vlastností. Při tomto způsobu se snižuje míra chybného přijetí a zvyšuje míra chybného odmítnutí, protože útočník musí mít všechna skóre podobnosti vyšší než práh citlivosti, dochází k velkému snížení FAR, což vyjadřuje:

$$FAR_C = FAR_1 \cdot FAR_2 \cdot .. \cdot FAR_N$$

kde:
FAR_C je celková míra chybného přijetí,
FAR_i je dílčí míra chybného přijetí, počet dílčích mír udává počet použitých čidel.

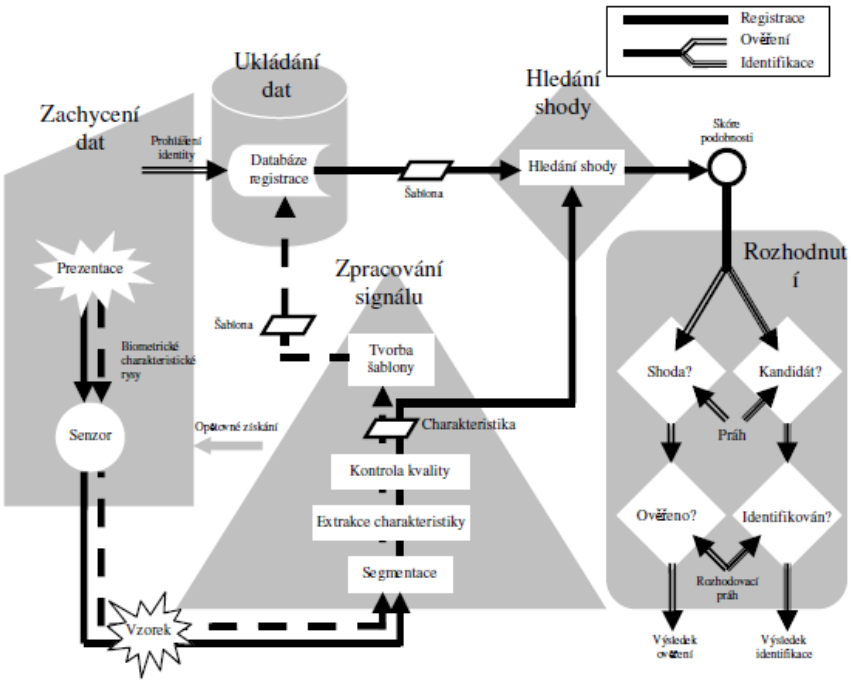
Nežádoucí je to však pro uživatele, protože stačí, aby jednou bylo skóre podobnosti menší než je práh citlivosti, a bude označen jako neoprávněný, čímž dochází ke zvýšení FRR vyjádřené vzorcem:

$$FRR_C = FRR_1 + FRR_2 + ... + FRR_N$$ FRR_C - je celková míra chybného odmítnutí,

kde:
FRR_i - je dílčí míra chybného odmítnutí, počet dílčích mír udává počet použitých čidel.

Jak vyplývá ze vzorců, výhodou multimodální autentizace je, že při zvýšení bezpečnosti přidáním biometrických senzorů dochází k mnohem rychlejšímu poklesu míry chybného přijetí než zvýšení míry chybného odmítnutí.

Obecný systém, který je zobrazen na obrázku 2, a je tvořen strukturou subsystémů, kdy každý subsystém plní určitou funkci:



Obrázek 2: Struktura obecného biometrického systému [6]

Zachycení dat: Senzor sejme předložený biometrický charakteristický rys a předává ho v podobě biometrického vzorku na výstup senzoru.

Komunikace: Tento subsystém přenáší biometrické vzorky, charakteristiky a šablony mezi ostatními subsystémy. Při těchto přenosech může dojít k znehodnocení v důsledku šumu, během procesu komprese či expanze nebo úmyslným zásahem, proto je potřeba chránit přenosové cesty a zaručit autenticitu, integritu a důvěrnost biometrických dat.

Zpracování signálu: Z biometrického vzorku se získávají matematickými postupy a algoritmy charakteristiky, ze kterých se tvoří referenční šablona. V tomto subsystému je zařazena kontrola kvality vzorku, která s určitou pravděpodobností zaručí, že charakteristiky jsou rozlišitelné a opakovatelné.

Ukládání dat: Získané šablony jsou prostřednictvím registrační databáze uchovány a opatřeny údaji registrovaného subjektu. Jako úložiště může sloužit token, čtecí zařízení nebo centrální databáze.

Přiřazování: Charakteristiky zde prochází procesem porovnávání s jednou nebo více šablonami. Výsledkem tohoto procesu je skóre podobnosti, které reflektuje míru shody porovnávané charakteristiky a šablony. Při procesu verifikace dochází k porovnání s jednou šablonou (může jich být i několik), a to vede ke skóre podobnosti. Při identifikaci je porovnávána charakteristika se všemi nebo jenom s určitou množinou šablon, čímž je vytvořen soubor skóre podobnosti.

Rozhodování: Rozhodování probíhá na základě skóre porovnání. Způsob rozhodnutí závisí na tom, zda jde o verifikaci nebo identifikaci. U verifikace dochází k prohlášení identity jako hodnověrné, jestliže skóre podobnosti přesáhne práh citlivosti. Při identifikaci, jestliže dojde k přesažení prahu citlivosti, je šablona přiřazena na seznam možných kandidátů, z něhož je identita osoby vybraná na základě nejvyšší hodnoty skóre podobnosti. Politika rozhodování může umožnit nebo vyžadovat více porovnání, než je rozhodnuto o verifikaci nebo identifikaci.

Rozpoznávání podle otisku prstů

Podstata této technologie spočívá v tom, že téměř všichni lidé mají na bříškách prstů obrazce tvořené papilárními liniemi (vyvýšené reliéfy kůže vysoké 0,1 až 0,4 mm, o šířce 0,2 až 0,5 mm). Obrazce jsou tvořeny základními markanty (krátká linie, začátek a konec, háček, můstek, křížení, zdvojení, posunutí, dvojitá vidlice, trojitá vidlice, tečka, očko, ostrůvek, ostrůvek s čárkou, uzavřená smyčka a speciální markanty), které dávají vysokou míru entropie a zaručují vysokou spolehlivost identifikace. Sejmutí biometrického vzorku je prováděno senzory, které pracují na různých fyzikálních principech. Senzory lze rozdělit podle toho, na jakém fyzikálním principu pracují:

Optický: Digitalizace otisků prstu u kontaktních optických senzorů je provedena prostřednictvím ozáření povrchu bříška prstu přiloženého k ochrannému sklu senzoru a snímání zpětného odrazu světla. Intenzita odraženého světla je závislá na tom, zda se odrazila od hřebenu linie nebo brázdy.

Kapacitní: Kapacitní senzor se skládá z pole miniaturních navzájem izolovaných vodivých ploch. Při přiložení prstu na vodivé pole dojde k propojení jednotlivých ploch papilárními liniemi a brázdy se chovají jako izolanty. Obrazec se vykreslí na základě napětí a úbytku kapacity.

Elektrooptický: Tyto senzory se skládají z několika vrstev. Dotyková první vrstva je polymer, který při dotyku lidské kůže emituje světlo, a to je následně zpracováno fotodiodami na elektrický signál, ze kterého je zpracován obraz papilárních linií.

Tlakový: Senzor je tvořen ze tří vrstev, kdy mezi dvě vodivé vrstvy, přičemž dotyková vrstva je elastická, je vložen nevodivý gel. Při přiložení prstu dochází k tlaku na elastickou vrstvu a nevodivý gel a dochází k propojení vodivých vrstev. V místě, kde jsou na bříšku papilární linie, dochází k většímu tlaku, než tam kde jsou brázdy, čímž dochází k digitalizaci otisku prstu. Tato technologie není citlivá na mokré nebo suché prostředí.

Termický: Pyroelektrická buňka senzoru snímá tepelné záření lidského těla při přejetí prstu přes senzor. Papilární linie vyzařují vyšší intenzitu tepelného záření oproti brázdám, čímž senzor může vykreslit papilární obrazec prstu. Tím že senzor snímá tepelné záření, dochází k vyloučení některých pokusů o autentizaci falzifikátem.

Ultrazvukový: Senzor se skládá z vysílače a přijímače, kdy obě části senzoru rotují kolem osy prstu. Vysílač vysílá krátké impulzy, které se odráží od prstu, kde se deformují v závislosti na tom, zda se odrazí od brázdy či linie. Impulzy pronikají až pod kůži, takže lehce mohou odhalit falzifikáty.

Velkou výhodou rozpoznávání podle otisku prstů je obrovský potencionál jejího využití, což se projevuje na implementaci do různorodých technologií (telefony, notebooky, pouzdra na pistoli ...), čemuž napomáhá možnost různého způsobu snímání. Určitou nevýhodou může u rozpoznávání podle otisku prstu být asociace na kriminální činnost. Mnohem podstatnější nevýhodou může být „jednoduchost" snímání některých senzorů (na vytvoření jednoduchého systému stačí kvalitní skener a počítač) a z toho vyplývající možnosti předložení falzifikátu otisku prstu (vytisknutý otisk na fólii).

Geometrie ruky

Pracuje na 3 dimensionálním snímání délky, šířky, tloušťky a povrchu ruky umístěné na podložce s pěti polohovými kolíky pomocí CCD kamery. Vybrané měřené parametry (lze provést až 90 měření) poté slouží autentizaci. Jelikož ale není geometrie ruky příliš unikátní biometrickou vlastností, je její aplikace v bezpečnostní sféře omezena právě stupněm bezpečnosti, kterého chceme dosáhnout.

Geometrie tváře

Jsou dva odlišné přístupy k rozpoznávání geometrie tváře:

- geometrický: rysy tváře,
- otometrický: vzhled obrazu tváře.

Tři nejlépe prozkoumané:

- **PCA:** tvář je rozložena na tzv. eigenfaces (matice jasových úrovní) a poté jde opět složit. Každá eigenface je reprezentována pouze číslem.
- **LDA:** třídí se pořízené obrazy a tvoří se skupiny. Cílem je maximalizace rozdílů jednotlivých skupin a minimalizace rozdílů v každé skupině.
- **EBGM:** bere v potaz okolní vlivy (osvětlení okolí, pozice hlavy nebo mimiku). Na obličeji jsou definovány uzlové body, které se propojí a tím se definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje. Samotné vyhodnocení poté probíhá na základě systému filtru uzlových bodů. Problém je přesnost lokalizace orientačních bodů na tváři.

Duhovka oka
Biometrický parametrem je vzorkování duhovky, které vzniká nezávisle (obě duhovky jednoho člověka nejsou totožné), při snímání duhovky je potřeba kvalitní digitální kamera a IR osvětlení. Porovnání mapy duhovky s tou referenční probíhá pomocí testu statistické nezávislosti, jestliže test selže je dotyčná osoba považována za oprávněnou, míra spolehlivosti vysoká.

Sítnice oka
Biometrický parametrem je obraz struktury cév na pozadí lidského oka v okolí slepé skvrny, k získání obrazu se využívá zdroj světla o nízké intenzitě, neskenovaný obraz je převeden do 40 bitového čísla. Vyžaduje nároky na uživatele: sundat brýle, dívat se do vymezeného prostoru, míra spolehlivosti: vysoká.

Akustická charakteristika hlasu
Pro ověření identity subjektu slouží předem uložené vzorky hlasu (klíčová věta). Výhoda ověření identity pomocí hlasu spočívá nejen ve specifiku lidského hlasu, ale také ve flexibilitě klíčových vět. V reálném prostředí je mnohem náročnější a zatím není systém, který by byl dostatečně přesný.

Struktura žil na zápěstí
Snímá hřbet ruky speciální kamerou v IR světle. Tak lze získat černobílý obraz stromové struktury žil, které tvoří zřetelný vzorec. Velkou výhodou je, že některé technologie vyžadují živou ruku, čímž je mnohem obtížnější falzifikace. Snímání probíhá tak, že zdroj prosvítí ruku a na základě různé absorpce záření krevních cév a ostatních tkání se vytvoří obraz pomocí snímací CCD kamery. Extrahováním se získávají body, úhly větvení a tloušťka cév. Prosvícením IR světlem se zvýrazní rozdíl řečiště a okolní kůže.

Behaviorální: měřenými parametry jsou parametry pocházející z chování měřené osoby.
Psaní na klávesnici
Obdoba dynamiky podpisu, sleduje dynamika úhozů na klávesnici. Parametrem je doba držení klávesy, prodleva mezi jednotlivými stisky kláves. Vytvoření šablony je časově náročnější. Velká pravděpodobnost „zaměnitelnosti“ a časová nestálost. Může sloužit jako další opatření proti neoprávněné autentizaci.

Dynamika podpisu
Využívá se jak dynamických, tak statických vlastností. Základními dynamickými parametry jsou rychlost, akcelerace, časování, tlak a směr tahu. Statický parametr je shodnost podpisů. Tyto parametry nelze z obrazu podpisu naučit. Lze je využít pouze pro verifikaci.

Dynamika chůze
Sledovaným parametrem při měření je styl chůze: pohyb po nohách nebo bipedální lokomoce. Porovnává křivky drah, které opisují určité body na lidském těle, tedy hlavně jeho těžiště. Jedinečnost křivky vychází z jedinečnost svalově kosterního systému a svým dynamickým stereotypem. Velkou výhodou je možná detekce maskovaných osob.

Typování a profilování potencionálního pachatele v bezpečnostní praxi letiště

Profilace: preventivní metoda, která umožňuje identifikovat nestandardní fyziologické projevy a chování u posuzovaných osob a na základě analýzy těchto odchylek identifikovat potenciální ohrožení chráněných aktiv. Slouží k selekci podezřelých osob z páchání TČ. Nastavení parametrů profilace se liší dle oblasti aplikace.
Pro uplatnění profilace je nezbytné znát profil běžného cestujícího, aby bylo možno hodnotit míru odchylek u nestandardních reakcí. Před profilací by se měly učinit následující kroky:

- analýza ohrožení: definice letů s největší potencionálním rizikem ze strany pachatelů,
- znalost profilu standardního cestujícího: profil cestujícího, který ji standardně využívá k přepravě,
- vizuální profil potenciálních pachatelů: na základě zkušeností, odborných publikací a dat z historie,
- znalost informací o každém cestujícím: dle cestovní dokumentace (rezervace, letenka, doklady, atd.)
- znalost postupu při pohovoru: získaní informací o cestujícím a jeho cestě, srovnání s údaji z cestovní dokumentace, ověření pravdivosti údajů, ověření reakcí na úmyslně aplikované podněty.

Pro určení profilu standardního cestujícího je potřeba znát odpovědi na následující otázky:

- o jaký druh letu se jedná,
- jaký druh cestujícího standardně využívá tento let,
- jak je běžný cestující tohoto letu oblečen,
- jak se běžně chová cestující daného letu,
- jaký je jeho běžný etnický původ,
- jaká zavazadla standardně používá,
- standardní trasa cesty cestujícího tohoto letu,
- jaký je nejčastěji udávaný účel cesty daného letu.

Míra reakce člověka na vnější podněty, lze využít tzv. fyziologické funkce a jejich biosignály. Biosignály jsou proměnné v čase dle míry působení vnějšího podnětu a citlivosti daného jedince na daný podnět (rozdílná reakce jedinců).

Biosignály je možno rozdělit na typy podle původu či vzniku: elektrické, impedanční, magnetické, akustické, chemické, mechanické, optické, tepelné, radiologické a ultrazvukové.

Metody profilace a typování
Real-Time Pulse Monitor: měření srdeční frekvence osob v reálném čase (detekce změn světlosti obličeje způsobených průtokem krve), rozpoznává pohyb obličeje či celého těla a tyto pohyby jsou na základě výpočtů eliminovány. Lze využít standardních digitální kamery.

Systém WeCU
Metoda je založena na hodnocení reakcí osob na specifické obrazové vjemy ve spojení s potenciální hrozbou. Systém dokáže snímat fyziologické signály lidského těla, jako teplotu těla, srdeční frekvenci a rychlé oční pohyby a vyhodnocovat jejich změny na základě vnějších podnětů. Detekce je časově nenáročná, postačuje přibližně dvacet až třicet sekund, a pro dotčenou osobu je tento proces nepozorovatelný.

Promítá infračervený podprahový obrazový vjem, který by rozpoznal pouze teroristu. Princip je založen na faktu, že lidé reagují na jim dobře známý obrazový vjem, pokud ho spatří na neobvyklém místě. Snímá se změna fyziologických parametrů způsobená vjemem.

Malintent
Umožňuje dálkovou detekci stavu mysli člověka a jeho případný nežádoucí úmysl. Je snímána: tělesná teplota, srdeční frekvence, frekvence dýchání, tělesný pach a nonverbální projevy. V rámci detekce by mělo dojít k rozeznání vystresovaného jedince od osoby s úmyslem páchání TČ.

Video analýza
Využívá se analytického softwaru pro zpracování a vyhodnocování kamerového záběru, jestliže dojde k pozitivní detekci, proběhne automatické uplatnění opatření nebo upozornění obsluhy. Lze využít následující funkce videoanalýzy:

- *zónování monitorovaného prostoru:* rozdělení obrazu kamerové jednotky na oblasti, při vstupu osoby do střežené zóny je vyvolán poplach,
- *vzdálený monitoring předmětů:* lze využít dvou možností, při první možnosti se střeží vybraný předmět umístěný v obrazu kamerové jednotky (při změně polohy předmětu dochází k vyhlášení poplachu), při druhé možnosti je detekce ponechaného předmětu v prostoru monitorovaného kamerového systému a umožňuje rozpoznat změnu obrazu vzhledem k původnímu a zároveň eliminovat dynamické vlivy (průchod osob se zavazadly,
- *počítání osob:* lze zajistit aplikací úsečky do zorného pole kamerové jednotky a pokud dojde k jejímu překročení, je to zaznamenáno, problémy nastávají při aplikaci na větší skupinu osob (nelze rozeznat veškeré pohybující se objekty),
- *Heat mapping:* grafické znázornění pohybu osob ve sledovaném prostoru a grafické odlišení prostoru scény dle hustoty pohybu, z pohledu bezpečnosti se uplatňuje analýza nestandardního pohybu jedince, včetně jeho trajektorie.

Analýza hlasu
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. Analýza může být provedena v reálném čase při hovoru nebo telefonátu.
Používaná analýza je tzv. LVA (vrstevná analýza hlasu), která je schopna zachytit emoční křivky v lidském hlasu, čímž lze analyzovat duševní stav a emoční rozpoložení posuzované osoby.
Identifikované jevy: různé typy stresu, nadšení, zamyšlení, zmatenost, kognitivní procesy, emocionální reakce, atd.

Metoda vedení pohovoru
Jsou kladeny nároky na osobu, která vede pohovor (faktor lidské chyby, který nelze vyloučit). Úspěšnost metody závisí na několika aspektech:

- správnost určení hrozby daného letu,
- znalost profilu standardního cestujícího daného letu a možného teroristy,
- precizní provedení kontroly cestovních dokladů cestujícího,
- pozorování cestujícího, zavazadel, spolucestujících,
- správná technika vedení pohovoru.

Otázky by měly být kladeny systematicky dle naučeného scénáře pro efektivní rozlišení nestandardní reakce. Otázky by měly vycházet z informací získaných z prvotního pozorování a kontroly cestovních dokladů. Využívají se čtyři základní typy otázek:

- **kontrolní:** cílené přivedení k lživé odpovědi, abychom mohli porovnat reakci při pravdivé a lživé výpovědi,
- **neutrální:** navrácení osoby do neutrálního fyziologického stavu, pokud předtím reagovala na jiný podnět (zvýraznění rozdílů mezi reakcemi na relevantní otázky),
- **relevantní:** cílem otázek je vyvolat fyziologickou reakci doprovázenou registrovatelným projevem (např. „Jste terorista?“),
- **symptomatické:** užívání otázek pro zjištění nepřirozených reakcí posuzované osoby (např. „Je něco v nepořádku?“).

Verbální projevy rozrušení osob (akustické):

- hluboce vzdychá, koktá, mluví váhavě, není schopen odpovědět, neodpoví na položenou otázku, neustále vás žádá o bližší vysvětlení otázek, odpoví na otázku otázkou, pomlaskává, přerývaný hlas, skřípe zuby,
- třese se mu hlas, váhá s odpovědí, zadrhává se v řeči, zívá (velmi důležitý znak), zopakuje otázku a opět požádá o zopakování.

Důležitým faktorem jsou projevy nonverbální komunikace:

- dává si nohy křížem a brzy se vrací do běžného postoje,
- dotýká se, uhlazuje nebo masíruje jakoukoli část těla,
- hraje si se šperky, má husí kůži, intenzivně se potí (pokud k tomu není příčina prostředí, oblečení nebo činnosti),
- ježí se mu chlupy na rukou nebo vlasy na zátylku,
- klopí zrak, kouše se do rtů, křiví ústa, mhouří se, mne si nos, nebo se jej dotýká,
- mne si ruce nebo prsty, mračí se, není schopen udržet pohled na jednom místě, neudrží chodidla v klidu,
- neudrží paže v klidu, neustále přenáší váhu z jedné nohy na druhou.

RFID

Neboli radiofrekvenční identifikace, jedná se o systém využívající el. magnetické vlny, který umí identifikovat objekt, aniž by byl přímo viditelný. Systém lze uplatnit například pro sledování pohybu zboží (logistika), při výrobním procesu, pro identifikaci zvířat s implementovaným RFID Tagem, pro bezhotovostní platby a v neposlední řadě také pro ochranu zboží v retailu a skladech. RFID technologie postupně nahrazuje technologii čárových kódů, kde je potřeba mít čárový kód umístěn na viditelném a přístupném místě, a poté je nutné ho fyzicky načíst, čímž je kód vystaven okolním vlivům, kde na druhou stranu RFID Tagy může být umístěn uvnitř zásilky, zboží.

Systém RFID

Má tři základní komponenty:

- Tag
- RFID čtečka
- Počítač pro zpracování informací

V Tagu je zaznamenaná informace o sledovaném předmětu. Tag se skládá z jednoúčelového zákaznického obvodu (ASIC) spojeného s anténou. RFID čtečka je zařízení sloužící k bezdrátové komunikaci s Tagem – identifikuje ho. Tag s čtečkou jsou schopny poloduplexní komunikace a umí směrovat rádiový signál.

Pro rozdělení systému RFID se nejčastěji využívá parametr kmitočtového pásma, může se jednat o systémy:

- LF (Low Frequency) 125 KHz – 148 KHz
- HF (High Frequency) 13,56 MHz
- UHF (Ultra High Frequency) 860 - 960 MHz
- MW (Microwave) 2,5 GHz a 5,8 GHz

LF využití například pro sledování pohybu zvířat a přístupové systémy. HF se využívá v knihovnách pro management knih. UHF najde uplatnění ke sledování zboží, předmětů v Supply Chain. Nevýhodou je použití rozdílných kmitočtů v jednotlivých částech světa. MW slouží nejčastěji k identifikaci vozidel pro systém elektronického mýtného. Vyšší frekvence zvyšuje přesnost a rychlost čtení tagů, ale zvyšuje také náchylnost na kovy a snižuje všesměrovost.

RFID Tag

Jedná se o čip, ve kterém je uložena informace o sledovaném předmětu. Tento čip potřebuje ke své funkci elektrickou energii. Na základě toho, jak tuto energii získává, tyto čipy dělíme na:

- Aktivní
- Pasivní
- Semi-aktivní
- Semi-pasivní

Aktivní čipy mají svůj vlastní zdroj napájení. Výhoda těchto čipů spočívá v možnosti integrace senzorických systémů pro měření teploty, vlhkosti, otřesů. Fungují na vyšší vzdálenosti, ale jejich cena je oproti ostatním kategoriím vyšší, životnost kratší a prostorově jsou větší.

Pasivní čipy nemají svůj vlastní zdroj napájení. Využívají elektromagnetického vlnění vysílaného RFID čtečkou. Aby byla zajištěna správná funkce systému je potřeba zajistit dostatečný výkon k aktivaci čipu, a následně musí být dostatečný výkon odražený čipem pro umožnění detekce čtečkou. Důležitými faktory pro tento typ čipů je vzdálenost čtečky a materiál, na kterém je čip umístěn.

Semi-aktivní čipy mají svůj vlastní zdroj napájení, ale který nevyužijí, dokud neproběhne aktivace čipu pomocí čtečky, tento zdroj poté využijí pro komunikaci se čtečkou. Jejich výhodou je možnost komunikace na větší vzdálenosti, delší životnost, na druhou stranu nevýhodou bývá dlouhá odezva. Semi-pasivní čipy využívají napájecí zdroj pro integrovaný obvod, ale ne pro komunikaci se čtečkou.

RFID Tagy lze dále rozdělit podle jejich vlastností do pěti tříd.

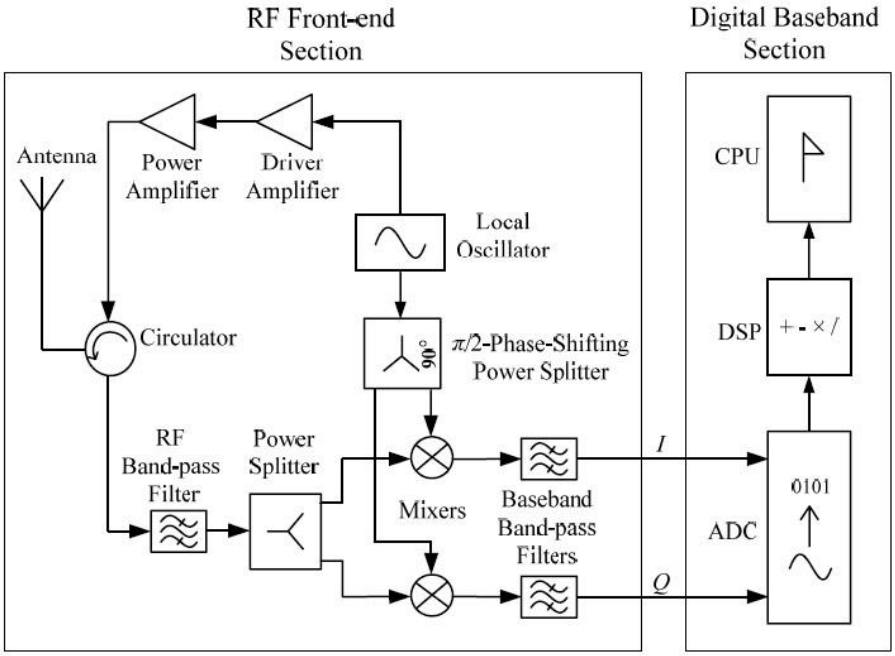
- Nepřepisovatelné
- Zapisovatelné pouze jednou
- Opakovatelně přepisovatelné

- Semi-pasivní s opakovatelným přepisováním
- Aktivní - schopné komunikovat s dalšími aktivními tagy

RFID čtečka

Komunikace mezi RFID čipy je zajištěna pomocí RFID čtečky, která vysílá, přijímá a vyhodnocuje elektromagnetické vlny. Funkci RFID čtečky lze vidět na schématu níže viz obrázek. Schéma se dělí na dvě části: blok vysokofrekvenční a číslicového zpracování.

Vysokofrekvenční část je vytvořena z přijímače, vysílače, oscilátoru, cirkulátoru a antény. Přijímač je tvořen z vysokofrekvenční pásmové propusti, děliče výkonu, bloku posouvajícího fázi, dvěma směšovači a dvěma pásmovými propustmi, které fungují v defaultním pásmu. Vysokofrekvenční pásmová propust zamezuje interferencím, které vznikají mimo pásma operační frekvence. Data modulovaná tagem jsou obnovována pomocí kvadraturního demodulátoru, který je tvořen děličem výkonu, blokem posouvajícím fázi a směšovačem. Pásmová propust naladěná na základní pásma má za úkol eliminovat nízkofrekvenční a vysokofrekvenční rušivý signál a šum. Pro dosažení požadované výkonové úrovně obsahuje vysílač zesilovače. Cirkulátor separuje přijímač od vysílače a je nutný za předpokladu, že využíváme jednu anténu pro vysílač i přijímač. Anténa vyzařuje energii vysílače do volného prostoru a zároveň přijímá signály „odražené“ od tagů a překážek nacházející se v daném prostoru. Blok číslicového zpracování se skládá z A/D převodníku (ADC), digitálního signálového procesoru (DSP) a centrálního procesoru (CP).



Kmitočet, na kterém čtečka funguje, není stálý, ale využívá frekvenčního posunu, jehož účelem je omezit rušení, které může nastat jako důsledek využívání kmitočtového pásma jinými zařízeními. Pro komunikaci mezi RFID čtečkou a tagem, musí kromě shodného kmitočtového pásma – frekvence, využívat i stejná modulační schémata, která jsou specifikovaná vybranými komunikačními protokoly.

Komunikaci čtečky a tagu může vyvolat samotná čtečka, která vyšle signál a tag odpovídá, nebo samotný tag vyšle signál, když je v přítomnosti elektromagnetického pole čtečky. Na základě typu čipu – pasivní/aktivní dojde k vyslání energie. Pasivní tag komunikuje se čtečkou, jakmile získá potřebnou energii. Aktivní tag vysílá pořád pokud má dostatek energie, ikdyž se nenachází v blízkosti čtečky, což usnadňuje odposlech komunikace mezi čtečkou a čipem. [8]