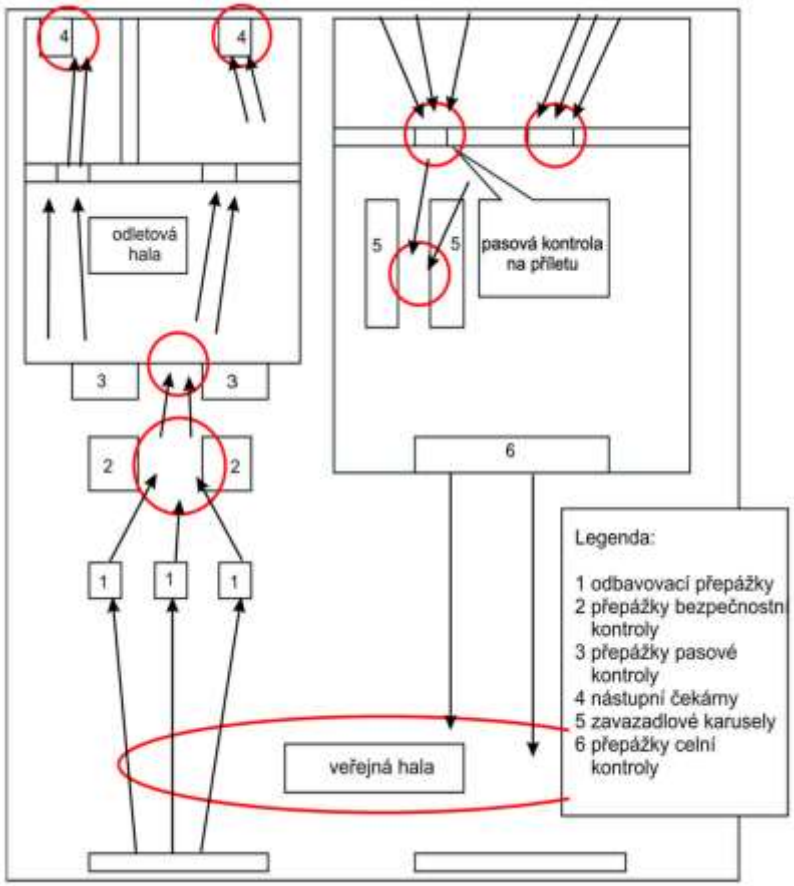
Vysoká škola báňská – Technická universita Ostrava
Fakulta bezpečnostního inženýrství
Katedra bezpečnostních služeb

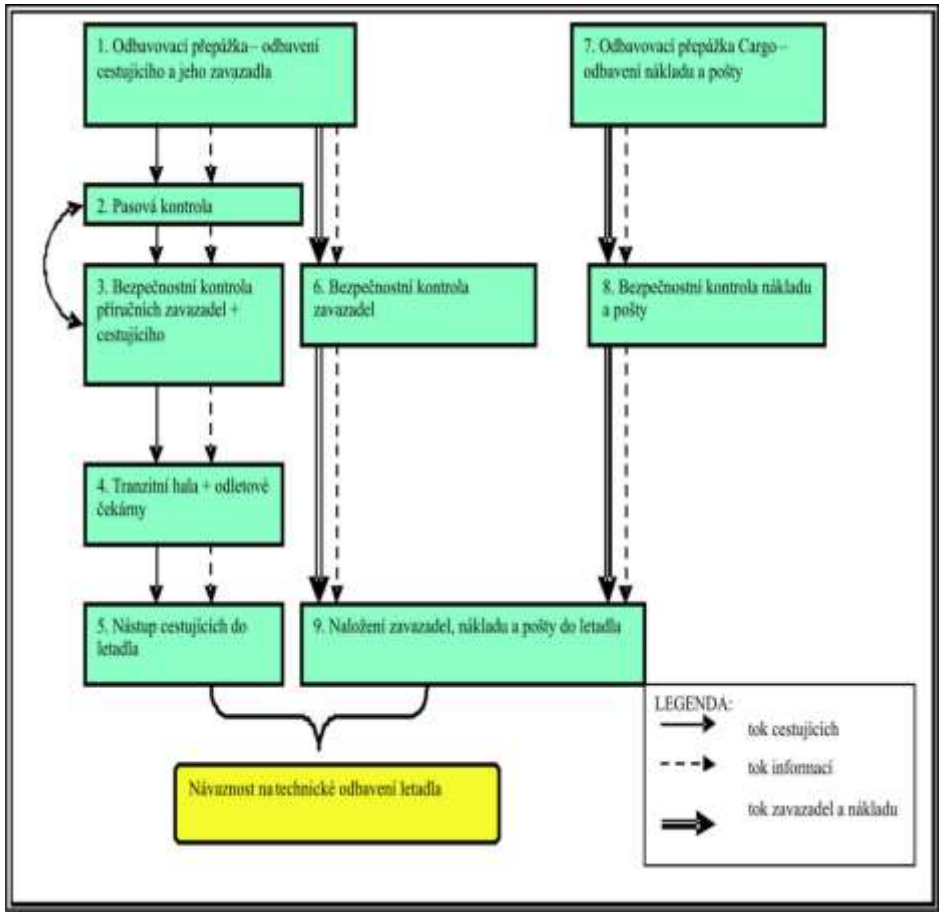
Speciální bezpečnostní technologie na ochranu osob a majetku

Odborné texty 2014

Doc. Mgr. Ing. Radomír Ščurek, Ph.D.

Kapacitní a projekční bezpečnost letiště





RaŠ

Bezpečnost letiště

- Ochrana objektu letiště je zajišťována vhodnou kombinací bezpečnostních opatření, která je možno rozdělit na ***fyzickou ostrahu, režimová opatření a technické bezpečnostní systémy*** (systém kontroly vstupu, poplachový zabezpečovací a tísňový systém, elektrická požární signalizace).
- Tato opatření zajišťují bezpečnost jednak preventivním působením, ale i represivně v případě potřeby reakce na konkrétní čin.
- Požadavkem na tato opatření je ale kromě zajištění vysoké bezpečnostní úrovně také co nejmenší míra omezení cestujících z důvodu potřeby rychlosti a plynulosti činnosti na letištích.

RaŠ

Bezpečnost letiště

- Fyzická ostraha objektu letiště je vykonávána jak policejním orgánem, tak pracovníky soukromých bezpečnostních služeb.
- Všechny tyto osoby by měly být důkladně proškoleny a seznámeny se standardními postupy řešení mimořádných událostí na letišti. Část bezpečnostního personálu by měla svou činnost vykonávat bez uniformy.
- Důležitá je nepřetržitá kontrola kritických prostor letiště (SRA – Security Restricted Area) a objektů definovaných analýzou rizik (přístupové body, koridory, odpadkové koše, atd.), které by měly být prověřovány bezpečnostními pracovníky v pravidelných časových intervalech.

Bezpečnost letiště

- Ochrana perimetru letiště je pro zajištění bezpečného provozu klíčová, protože brání nepovolaným osobám v přístupu do areálu letiště (tedy přístupu k letadlům).
- **Rizikové prostory letiště:**
  - koridory s velkým pohybem osob,
  - prostory, které nejsou monitorovány kamerovým systémem,
  - přistávací a vzletový prostor letadel,
  - kritická infrastruktura letiště (elektrická energie, klimatizace, IT infrastruktura, skladování paliva, atd.),
  - snadno přístupná místa v okolí letiště v blízkosti přistávajících a odlétajících letadel.

Bezpečnost letiště

- **Rizikové faktory:**
  - útoky na leteckou dopravu v minulosti,
  - přítomnost extrémistických skupin s cílem útoku na leteckou dopravu,
  - nepříznivá politická, ekonomická, či náboženská situace v zemi,
  - konání mezinárodní politické události v zemi.
- **Stavební členění letiště:**
  - veřejný prostor letiště,
  - neveřejný prostor letiště,
  - vyhrazené bezpečnostní prostory (SRA),
  - kritické části vyhrazených bezpečnostních prostorů (CSRA).

Bezpečnost letiště

- **Kontrola vstupu:**

1. Vstup do neveřejného prostoru letiště se omezí s cílem zabránit vstupu neoprávněných osob a vjezdu vozidel bez povolení k vjezdu do tohoto prostoru.
2. Vstup do vyhrazených bezpečnostních prostor je kontrolován s cílem zajistit, aby do těchto prostorů nevstoupily žádné neoprávněné osoby a nevjela žádná vozidla bez povolení k vjezdu.
3. Osobám a vozidlům může být udělen přístup do neveřejného prostoru letiště a do vyhrazených bezpečnostních prostorů pouze tehdy, pokud splňují požadované bezpečnostní podmínky.
4. Osoby, včetně členů posádky letadla, musí před vydáním identifikačního průkazu člena posádky letadla nebo letištního identifikačního průkazu opravňujících k přístupu bez doprovodu do vyhrazených bezpečnostních prostorů úspěšně absolvovat ověření spolehlivosti.

Bezpečnost letiště

- **Detekční kontrola osob jiných než cestujících a detekční kontrola vnášených předmětů:**

1. Osoby jiné než cestující se spolu s vnášenými předměty při vstupu do vyhrazených bezpečnostních prostor podrobují nepřetržité namátkové detekční kontrole s cílem zabránit vnesení zakázaných předmětů do těchto prostorů.
2. Všechny osoby jiné než cestující se spolu s vnášenými předměty při vstupu do kritických částí vyhrazených bezpečnostních prostor podrobují detekční kontrole s cílem zabránit vnesení zakázaných předmětů do těchto částí.

RaŠ

Bezpečnost letiště

- **Dozor, hlídky a jiné fyzické kontroly:**
- Na letištích a případně ve veřejně přístupných přilehlých prostorech se provádí dozor, hlídky a jiné fyzické kontroly s cílem **zjistit podezřelé chování osob**, nalézt slabiny, které by mohly být využity ke spáchání protiprávního činu, a osoby od páchání těchto činů odradit.

RaŠč

Součást bezpečnostní kontroly

Detekční prohlídka osob je započata průchozím detektorem kovů, která je doplněna namátkovou fyzickou prohlídkou nejméně u 10% z celkového počtu kontrolovaných osob. Tyto fyzické prohlídky jsou prováděny u všech osob, u nichž kontrola vyvolá poplašný signál

Právní předpisy z oblasti civilního letectví

Mezinárodní právní předpisy 1/6

- **Nařízení Evropského parlamentu a Rady (ES) č. 300/2008** ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002.
- Nařízení se skládá z dvaceti 4 článků a přílohy.
- V první části udává důvody standardizace bezpečnostních pravidel v rámci Evropské unie, cíle tohoto nařízení a oblast působnosti. Dále jsou uvedena bezpečnostní opatření. Články 10 až 14 popisují požadavek na zpracování bezpečnostních programů pro ochranu civilního letectví před protiprávními činy, které musí být vypracovány. Příloha specifikuje požadavky na zajištění bezpečnosti civilní letecké přepravy.

Mezinárodní právní předpisy 2/6

- **Nařízení komise (EU) č. 185/2010** ze dne 4. března 2010, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti.
- Nařízení se skládá ze 4 článků a 12 doplňků.
- Jednotlivé doplňky rozpracovávají specifikaci požadavků na zajištění bezpečnosti civilní letecké přepravy uvedených v příloze Nařízení Evropského parlamentu a Rady (ES) č. 300/2008.

Mezinárodní právní předpisy 3/6

- **Úmluva o mezinárodním civilním letectví**
  Úmluva o mezinárodním civilním letectví (tzv. Chicagská úmluva) byla sjednána v Chicagu v roce 1944. Prostřednictvím této úmluvy vznikla Mezinárodní organizace pro civilní letectví ICAO. Dokument obsahuje devadesát šest článků upravujících procesy v rámci mezinárodního civilního letectví.
- **Úmluva o potlačení protiprávního zmocnění se letadel**
  Takzvaná Haagská úmluva byla podepsána v roce 1970 v Haagu. Podle této úmluvy každá osoba, která na palubě během letu protiprávně za použití násilí nebo hrozby násilím nebo jakékoliv jiné formy zastrašování, se zmocní letadla nebo vykoná nad ním kontrolu nebo se pokusí o jakýkoliv takovýto čin nebo je spolupachatelem osoby, která páchá nebo se pokusí spáchat takovýto čin, spáchá trestný čin

Mezinárodní právní předpisy 4/6

- **Úmluva o potlačování protiprávních činů souvisejících s mezinárodním civilním letectvím** (Montrealská úmluva)
- Úmluva byla sjednána v roce 1971 v Montrealu a popisuje činy, které jsou spáchány proti bezpečnosti civilního letectví, jako trestné činy:
  - násilný čin proti letadlu za letu,
  - násilný čin proti letadlu za provozu nebo způsobení škody, která neumožňuje vzlétnutí,
  - umístění takového předmětu na palubu letadla, který ho může poškodit nebo zničit,
  - poškození zařízení letadla,
  - nepravdivá informace mající za následek ohrožení bezpečnosti provozu.
  - Montrealská úmluva byla dále doplněna Protokolem o boji s protiprávními činy násilí na letištích sloužících mezinárodnímu civilnímu letectví, který byl přijat v Montrealu v roce 1988

Mezinárodní právní předpisy 5/6

- **Letecký předpis L14 – Letiště**
- Předpis L14 upravuje požadavky na fyzické vlastnosti a překážkové plochy letišť, popis vybavení a poskytovaných technických služeb. Stanoví minimální provozní parametry letiště dle v současnosti provozovaných letadel, nebo letadel plánovaných provozovat. Opatření pro provoz letadel s vyššími nároky nejsou tímto předpisem stanovena a jejich posouzení je záležitostí každého letiště, případně příslušných orgánů. Cílem předpisu je zvýšit úroveň ochrany na letišti. Předpis se nezabývá usměrňování či omezování provozu letadel. Předpis dále neřeší postupy pro plánování letišť, vliv na životní prostředí, ekonomické aspekty provozování letiště a jiné netechnické souvislosti.

Mezinárodní právní předpisy 6/6

- **Letecký předpis L17 – Bezpečnost – Ochrana mezinárodního civilního letectví před protiprávními činy**
- Letecký předpis L17 se zabývá problematikou ochrany civilního letectví před protiprávními činy, kam náleží bezpečnost pasažérů, posádky letadel, pozemního leteckého personálu a ostatní veřejnosti a zároveň vytvořením takových podmínek, aby bylo možné reagovat v případě nárůstu bezpečnostní hrozby. Předpis dále popisuje bezpečnostní opatření, jejich kontrolu a řízení kvality. Opatření jsou rozdělena do kapitol dle dotčených subjektů. Závěrečná část se zabývá činnostmi při protiprávních činech, a to jak prevencí, tak i represí a způsoby reportingu a výměny informací.

Právní předpisy ČR 1/6

- **Zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání, ve znění pozdějších předpisů**
- Zákon upravuje podmínky ve věci civilního letectví (podmínky stavby a provozování letiště, letecké stavby, podmínky využívání leteckého prostoru a poskytování leteckých služeb, podmínky provozování leteckých činností, ochrana letectví, podmínky užívání sportovního létajícího zařízení, výkon státní správy) a implementuje do českého právního prostředí požadavky mezinárodních úmluv ve vztahu k civilnímu letectví. Zákon se v omezené míře vztahuje také na vojenské letectví.

Právní předpisy ČR 2/6

- **Zákon č. 101/2000 Sb., o ochraně osobních údajů** a o změně některých zákonů, ve znění pozdějších předpisů
- Účelem tohoto zákona je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí. Upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do cizích států. V souvislosti s typováním a profilací osob je nutné tento zákon aplikovat mimo jiné při využití kamerového systému se záznamovým zařízením.

Právní předpisy ČR 3/6

- **Vyhláška č. 410/2006 Sb., o ochraně civilního letectví před protiprávními činy** a o změně vyhlášky Ministerstva dopravy a spojů č. 108/1997 Sb., kterou se provádí zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání ve znění pozdějších předpisů.
- Vyhláška stanoví strukturu bezpečnostního programu, způsob provádění bezpečnostních kontrol, způsob získání a ověření odborné způsobilosti a další náležitosti ve vztahu k bezpečnosti civilního letectví.

Právní předpisy ČR 4/6

- **Národní bezpečnostní program ochrany civilního letectví České republiky před protiprávními činy**
- Národní bezpečnostní program ochrany civilního letectví České republiky před protiprávními činy byl schválen Bezpečnostní radou státu usnesením č. 15 ze dne 5. dubna 2008 a aktualizován na základě vnitrostátních právních předpisů, předpisů Evropských společenství a mezinárodních právních předpisů. Dokument se zabývá bezpečnostními programy letiště a leteckého dopravce a popisuje bezpečnostní opatření a postupy v civilní letecké přepravě. V závěrečné části pojednává o mimořádných událostech a krizových situacích

Právní předpisy ČR 5/6

- **Národní program bezpečnostního výcviku v civilním letectví České republiky**
- Národní program bezpečnostního výcviku v civilním letectví České republiky vychází z Národního bezpečnostního programu ochrany civilního letectví České republiky před protiprávními činy schváleného Bezpečnostní radou státu usnesením č. 15 ze dne 15. dubna 2008 a je zpracován v souladu s vnitrostátními právními předpisy, předpisy Evropských společenství a mezinárodními právními předpisy. Dokument popisuje metodiku náboru pracovníků civilního letectví, povinnosti subjektů a základní náležitosti bezpečnostních opatření, zásady bezpečnostního výcviku a typy odborné bezpečnostní přípravy

Právní předpisy ČR 6/6

- **Národní program řízení kvality bezpečnostních opatření k ochraně civilního letectví České republiky před protiprávními činy**
- Národní program řízení kvality bezpečnostních opatření vychází z Národního bezpečnostního programu ochrany civilního letectví České republiky před protiprávními činy schváleného Bezpečnostní radou státu usnesením č. 15 ze dne 15. dubna 2008 a je zpracován v souladu s vnitrostátními právními předpisy, předpisy Evropských společenství a mezinárodními právními předpisy. Dokument se zabývá metodikou kontrolní činnosti, kvalifikací a činnostmi auditorů, systémem řízení kvality a vyhodnocováním nedostatků a realizací nápravných opatření včetně jejich hodnocení

Systém předběžného hodnocení cestujících v letecké dopravě

(bezpečnost letecké dopravy je nejvíce exponovaný problém)

Profilace a Typping cestujících

Profilace

- Profilace je preventivní metoda v oblasti bezpečnosti, která umožňuje identifikovat nestandardní fyziologické projevy a chování u posuzovaných osob a na základě analýzy těchto odchylek identifikovat potenciální ohrožení chráněných aktiv.
- Úroveň profilování závisí na kvalitě informací potřebných pro vytvoření profilu.
- Primárním důvodem vytváření profilu je selekce podezřelých osob z páchání trestné činnosti. Profilování však nezaručuje přesnou identifikaci pachatele.
- Nastavení parametrů pro profilaci se liší dle oblasti aplikace. Úkolem profilace a typování podezřelých osob v prostředí civilního letectví je minimalizovat pravděpodobnost teroristického útoku či jiného protiprávního činu v souvislosti s bezpečností civilního letectví na co nejnižší možnou míru

RaŠč

Profilace 1/2

- Před aplikací profilace je potřeba znát profil běžného cestujícího, aby bylo možno hodnotit míru odchylek u nestandardních reakcí. Před realizací profilace by se měly učinit následující kroky:

1. Analýza ohrožení – definice letů s největším potenciálním rizikem ze strany pachatelů (teroristů).
2. Znalost profilu standardního cestujícího – profil cestujícího, který definovanou linku standardně využívá k přepravě.
3. Vizuální profil potenciálních pachatelů – na základě zkušeností, odborných publikací a dat z historie vytvořit profil vzhledu a chování potenciálního pachatele (teroristy).

Profilace 2/2

4. Znalost informací o každém cestujícím – dle cestovní dokumentace (rezervace, letenka, doklady, atd.) – důležité informace o cestujícím a charakteru jeho cesty.

5. Znalost postupu při pohovoru („questioning“) – získání informací o cestujícím a jeho cestě, srovnání s údaji z cestovní dokumentace, ověření pravdivosti údajů, ověření reakcí na úmyslně aplikované podněty.

Profil cestujícího

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

1. O jaký druh letu se jedná (obchodní, charterový, atd.)?
2. Jaký druh cestujícího standardně využívá tento let?
3. Jak je běžný cestující tohoto letu oblečen?
4. Jak se běžně chová cestující daného letu?
5. Jaký je jeho běžný etnický původ?
6. Jaká zavazadla standardně používá (typ, vzhled, počet)?
7. Standardní trasa cesty cestujícího tohoto letu?
8. Jaký je nejčastěji udávaný účel cesty daného letu?

RaŠč

Historie profilace

- Původ oboru profilování je přisuzován americké FBI (Federal Berau of Investigation).
- Profilování z pohledu kriminalistiky lze charakterizovat jako analýzu vzorců chování, charakteristik místa činu a vztahujících se trestných činů.
- Ve vědeckém prostředí existují dva rozdílné přístupy k profilaci pachatelů, a to jednak tzv. „Škola FBI" v USA, ale i takzvaná „Škola investigativní psychologie" ve Velké Británii.
- Oba přístupy se v metodách profilace odlišují

Profilování v pojetí FBI

- Profilování v pojetí FBI (deduktivní metoda) je definováno jako proces interpretace forenzních důkazů a důkladné studium jednotlivého pachatele, za účelem přesné rekonstrukce chování na místě činu.
- Tento proces ***silně závisí na možnostech rozpoznání vzorců chování hledaných pachatelů***.
- Způsob profilování vychází z obecných pravidel chování pachatele.
- Profilování v pojetí FBI rozděluje pachatele trestných činů na organizované a neorganizované.
- Poprvé bylo toto rozdělení užito pro pachatele vražd, později se začalo přenášet také na pachatele jiných typů trestných činů

Profilování v pojetí Liverpoolské školy

- Ve Velké Británii se profilováním pachatelů zabývá obor **investigativní psychologie** v Liverpoolu (Centre for Investigative Psychology).
- Cílem tohoto oboru je vytváření teorií pro policejní vyšetřování, které jsou zakotvovány do empirické a vědecké psychologie.
- Tento způsob se nezaobírá pouze výzkumem trestných činů, ale také rozhodováním policie během vyšetřování a řízením informací.
- Metodika profilování vychází z empirických výsledků výzkumů daného počtu pachatelů určitého trestného činu. Získané údaje umožňují vytvářet vzorce chování pachatelů určitých druhů trestných činů.

Historie profilování v ČR

- Počátky profilování pachatelů trestných činů v České republice sahají do 30. let 20. století. Poprvé bylo profilování zmíněno v knize Kriminální psychologie z roku 1930
- Velký rozvoj nastal v 80. letech, kdy se vyšetřovatelé a odborníci na trestnou činnost začali soustředit na dílčí aspekty kriminálního chování. V tomto období se tak objevilo velké množství publikací s tématem profilování.
- Na počátku 90.let byly sepsány publikace Kriminální agresor, či Psychologické profilování: mýtus a skutečnost, Velmi podrobný popis profilování pachatelů byl publikován v knize Vybrané kapitoly z kriminalistické psychologie

Psychologické aspekty kriminálního chování

- Je důležité uvědomit si variace mezi pachateli trestnými činy:
- dlouhodobě připravovaný trestný čin je odlišný od spontánního,
- motivy trestných činů jsou u různých pachatelů různé,
- organizovaná a neorganizovaná trestná činnost,
- pachatelé nejsou specializováni pouze na jeden typ trestné činnosti

Specifikace pachatele (multimediální pohled)

kriminální x nekriminální chování

TČ spáchán na osobě x na majetku

druh trestné činnosti (vloupání, atd.)

vzorec kriminálního chování

způsob páchání trestného činu s jeho specifickými znaky (modus operandi)

kriminální podpis

Specifikace pachatele (multimediální pohled) 1/2

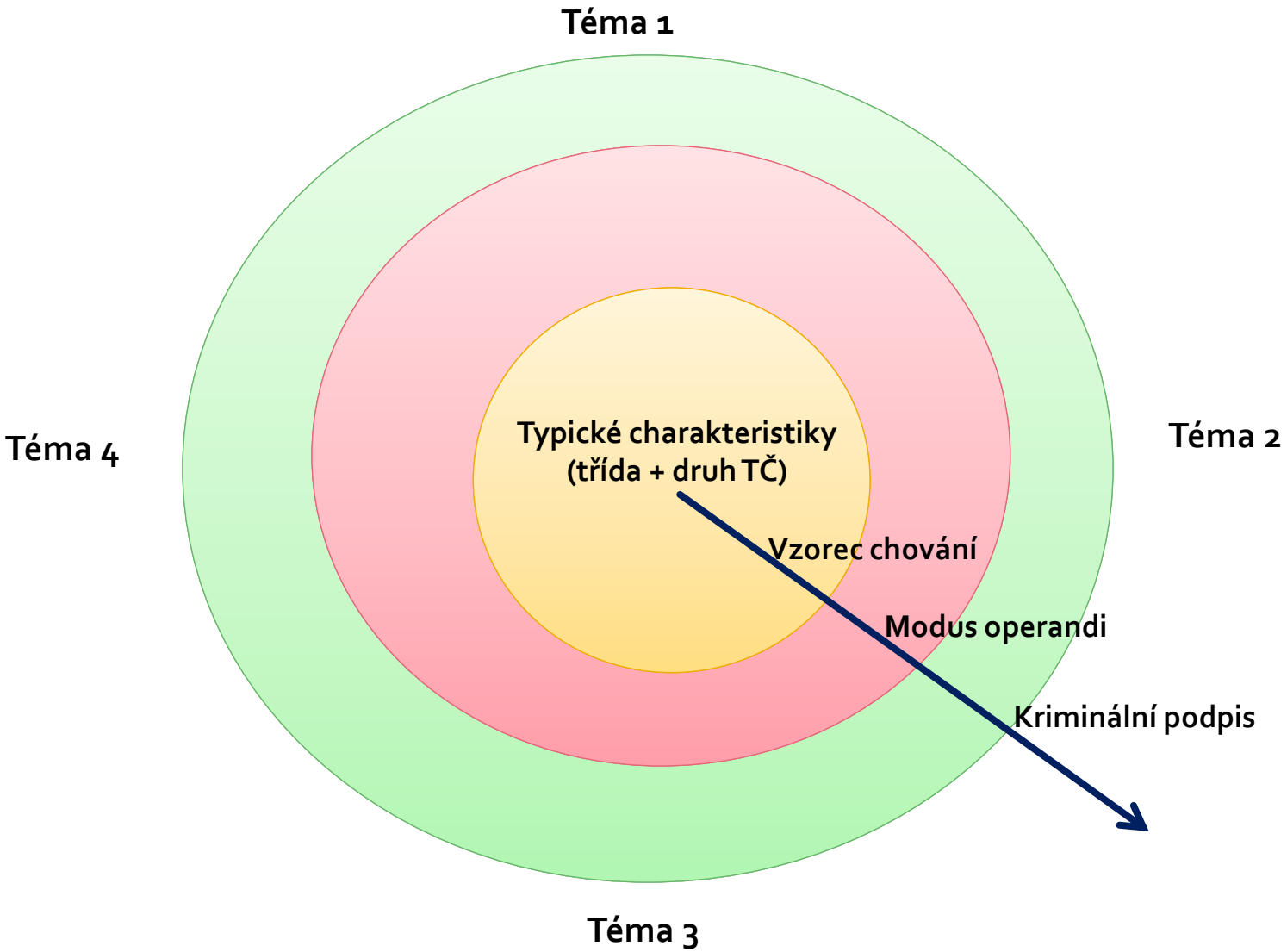
- Multidimenzionální přístup vychází ze dvou aspektů trestné činnosti:
  - **aspekt specifičnosti,**
  - **aspekt tematický.**
- **Aspekt specifičnosti** vychází z výše zmíněného postupu definice pachatele.
- Na počátku jsou typické společné znaky pro pachatele trestných činů, na kanci pak specifické znaky pro daného pachatele (kriminální podpis).
- **Aspekt tematický** vychází z jednotlivých kriminálních podpisů pachatelů trestných činů.

RaŠč

Specifikace pachatele (multimediální pohled) 2/2

- Propojením těchto dvou aspektů a přenesením do grafického znázornění získáme takzvaný radexový model, který poprvé popsal v roce 1954 Louis Gutman
- **Radexový model** je možno využít pro analýzu multidimenzionálního škálování (MDS)
- Jedná se o statistickou metodou pro získání tématu kriminálního chování, frekvence a vazby k dalším trestným činům, nebo pro analýzu SSA (Smallest Space Analysis – analýza nejmenšího prostoru)
- Model vyjadřuje vztahy mezi proměnnými vyjádřením v geometrickém prostoru

Radexový model



Sběr údajů o cestujícím leteckým dopravcem (v rámci služeb letiště)

- **Údaje PNR** (Passenger Name Record) – slouží k obchodním účelům. Jméno cestujícího, objednávka, zaplacení letenky, národnost, bydliště, místo pobytu v cizí zemi, profese apod.
- **Údaje API** (Advence Passenger Information) – údaje požadované imigračními úřady některých států. Stejné údaje jako PNR plus navác délka plánovaného pobytu, kontakty apod.
- Údaje o cestujícím spravovány v globálním distribučním systémů GDS – v USA se používá SABRE, GALILEO/APOLLO, v Evropě AMADEUS (např. ČSA)
- Při rezervaci letenky je vytvořen záznam o cestujícím a postupně jeho změny.


PLEASE WAIT TO BE SCANNED
SHOCK-BRACELETS ARE NOW MANDITORY
WE CARE ABOUT YOUR SAFETY

Děvět základních údajů o cestujícím

- Za účelem boje proti nedovolenému přistěhovalectví a zdokonalení hraniční kontroly
- Na základě směrnice Rady EU č. 82/2004 (v ČR uvedeno v z.č. 49/1997 Sb.)
- Letecká společnost je povinna o každém cestujícím tyto údaje:
  - jméno a příjmení,
  - datum narození,
  - číslo a typ použitého cestovního dokladu,
  - státní příslušnost,
  - údaj o hraničním přechodu na území členského státu EU,
  - kódové číslo letu,
  - čas odletu a příletu,
  - celkový počet osob přepravovaný daným letem,
  - počáteční místo nástupu na palubu letadla.
- Údaje využívány pro bezpečnostní účely, ale také k identifikaci obětí leteckých nehod

Bezpečnostní Kontrola v USA 1/3

Dvoustupňová kontrola:

- **prověření, zda se osoba nevyskytuje na seznamech NO FLY a SELECTEE** (seznamy osob podezřelých z terorizmu, které jsou poskytovány leteckým společnostem bezp.složkami USA).

V případě pozitivního nálezu jsou informovány bezp.úřady a osobě je zamítnuto letět, příp. je podrobena důkladnější kontrole.

- **Prověření těsně před odletem – opět podle výše uvedených seznamů na základě API údajů.**

V případě pozitivního nálezu informováno Středisko pro informace o teroristech – to vydá doporučení, zda osobu zatknout, vpustit/nevpustit do letadla, příp. zadržet. Let může být navíc odkloněn nebo vrácen zpět.

Bezpečnostní kontrola v USA 2/3

- **Systém CAPPS (Computer Assisted Passenger Pre-screening System** (počítačový systém předběžného hodnocení cestujících)

- Integrovaný bezpečnostní systém, který je napojen na odbavovací, bezpečnostní a vyhledávací systémy
- V provozu od 1997 v USA pod vedením FBI
- Pokud byl některý z cestujících vybrán jako potencionální bezpečnostní hrozba, byla jeho zavazadla podrobena důkladnější kontrole, ale cestující sám žádnou podrobnější prohlídkou neprocházel – zásadní slabina systému
- 11. září 2001 správně identifikoval většinu atentátníků jako potencionální hrozbu, ale protože jejich zavazadla prošla kontrolou bez problémů, byli všichni vpuštěni na palubu letadel
- V roce 2003 předložen nový systém CAPPS II

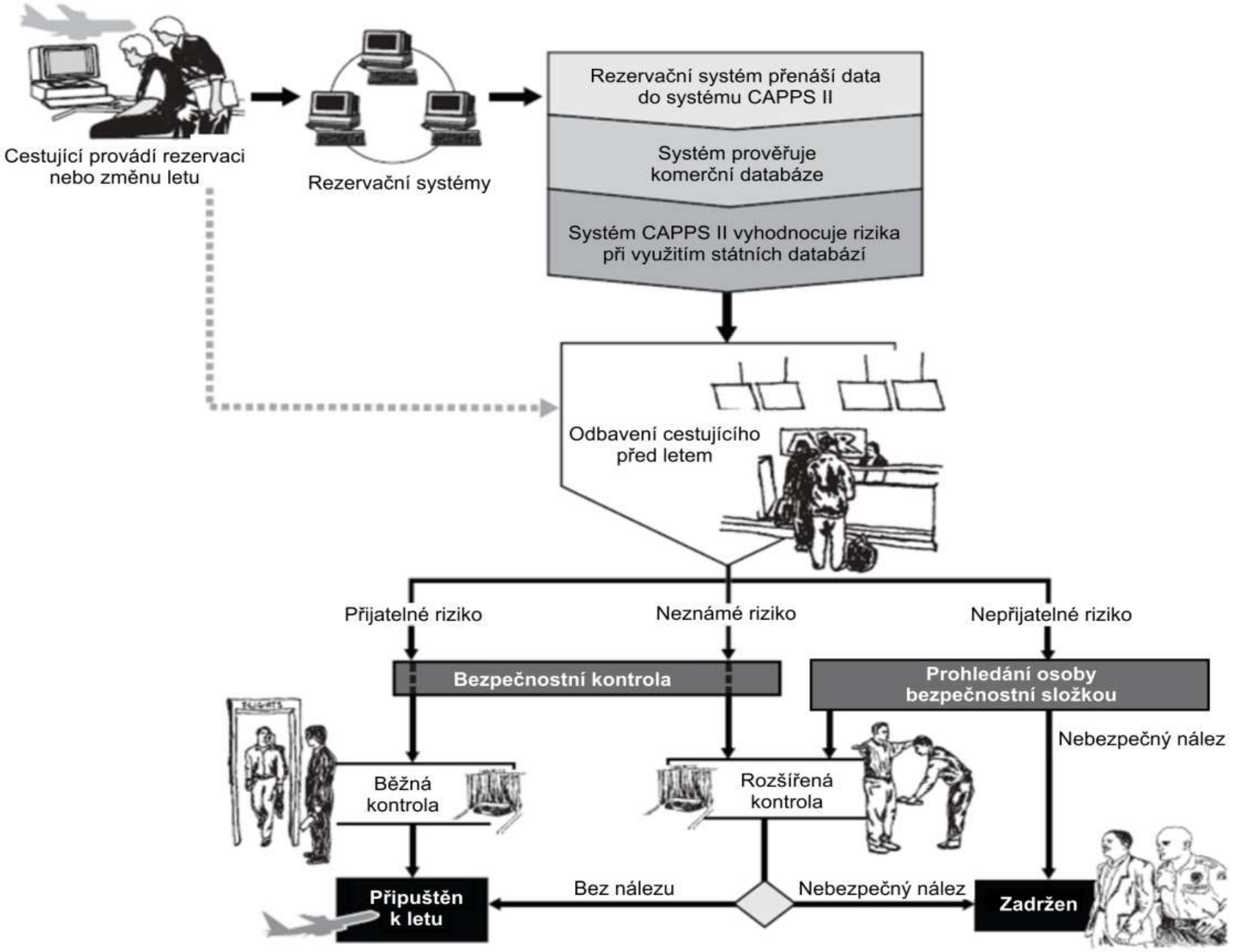
Bezpečnostní kontrola v USA 3/3

- **CAPPS II**

je postaven na analyzování dat na základě křížových dotazů.

- Data z PNR porovnávány s dalšími údaji uloženými ve státních a komerčních databázích.
- Ověřuje se totožnost, kriminální aktivity, možné vazby na teroristy
- Systém provede, na základě vstupních dat, výpočet "skóre rizika" a to uvede pomocí barevné škály na palubní vstupenku:
  - zelená (bez ohrožení) představuje žádnou další bezpečnostní kontrolu
  - žlutá (neznámé nebo možné ohrožení) znamená další screening
  - červená (vysoké riziko) neumožní držiteli palubní vstupenky nastoupit na palubu letadla a bude zadržen a předán příslušným orgánům.

V současné době přechází systém CAPPS II do programu Secure Flight (ve vývoji)

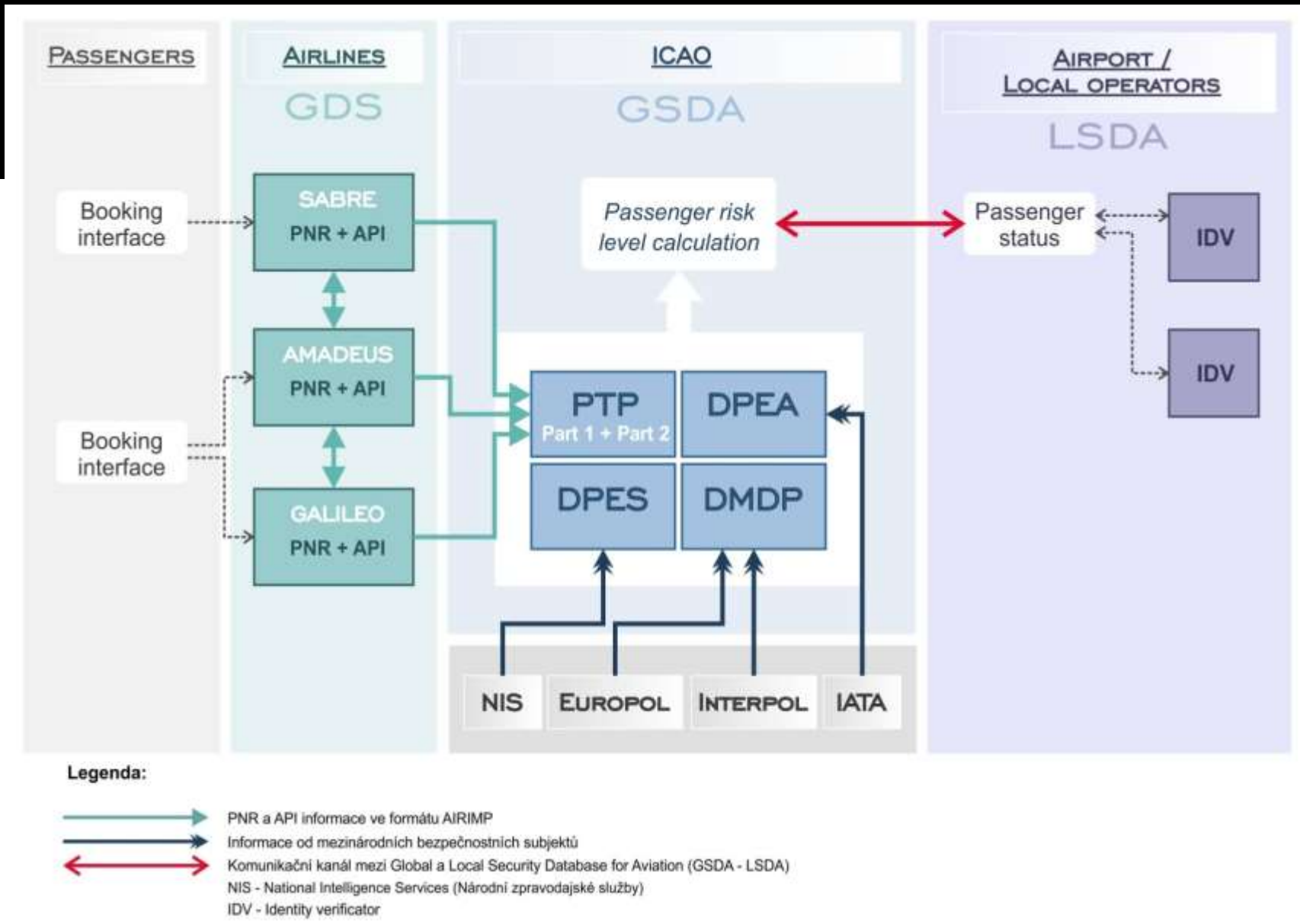

Cestující provádí rezervaci nebo změnu letu
Rezervační systémy
Rezervační systém přenáší data do systému CAPPS II
Systém prověřuje komerční databáze
Systém CAPPS II vyhodnocuje rizika při využitím státních databází
Odbavení cestujícího před letem
Přijatelné riziko
Neznámé riziko
Nepřijatelné riziko
Bezpečnostní kontrola
Prohledání osoby bezpečnostní složkou
Nebezpečný nález
Běžná kontrola
Rozšířená kontrola
Bez nálezu
Nebezpečný nález
Připuštěn k letu
Zadržen

Inovativní systém GSDA v letecké dopravě 1/2

- **GSDA dále obsahuje následující databáze:**
- **PTP (Passenger Travel Profile)** – profil cestujícího, který obsahuje informace o jeho letech, destinacích, příslušnosti k věrnostnímu programu dopravce, jeho aktuálních rezervacích, vízech, cestovatelských návycích (třída ve které nejraději cestuje, zda využívá zapsaná zavazadla, zda se někdy nedostavil k odletu apod.).
- **DPES (Database of Potentially Endangered Subjects)** – Databáze potenciálně ohrožených subjektů jako letiště, aerolinie a osoby. Jde o samostatnou databázi obsahující bezpečnostně relevantní informace o možných hrozbách.

Inovativní systém GSDA v letecké dopravě 2/2

- **DPEA (Database of People Excluded from Aviation)** – Databáze osob vyloučených z letecké dopravy představuje obdobu amerického seznamu osob, které jsou vykázány z letecké přepravy z důvodu spolupráce s teroristickými a extremistickými organizacemi, trestně stíhané osoby, osoby, které se dopustily násilí na palubě letadla, resp. v objektu spadajícím pod specifický paragraf trestního zákona apod.
- **DMDP (Database of Missing and Dangerous People)** – Databáze pohřešovaných a nebezpečných osob, která je aktualizována organizacemi INTERPOL a EUROPOL, tak aby byla včas identifikována osoba na útěku, osoba která byla unesena nebo je monitorována policií pro nezákonnou činnost.


PASSENGERS
AIRLINES
GDS
ICAO
GSDA
AIRPORT / LOCAL OPERATORS
LSDA
Booking interface
SABRE PNR + API
AMADEUS PNR + API
Booking interface
GALILEO PNR + API
Passenger risk level calculation
PTP Part 1 + Part 2
DPEA
DPES
DMDP
Passenger status
IDV
IDV
NIS
EUROPOL
INTERPOL
IATA
Legenda:
PNR a API informace ve formátu AIRIMP
Informace od mezinárodních bezpečnostních subjektů
Komunikační kanál mezi Global a Local Security Database for Aviation (GSDA - LSDA)
NIS - National Intelligence Services (Národní zpravodajské služby)
IDV - Identity verificator

Profilace cestujících

Profilace cestujících

- **Na letištích a v letadlech se sledují osoby podrobněji a důsledněji.**
- **Zaměřit se na podněty, které odhalí pachatele protiprávních činů předtím, než spáchají útok.**
- **Místo hledání špatných věcí – hledáme „špatné lidi".**
- Pozorný personál, podstata správné profilace.

Definice profilingu

- Technické profilování- provádí se pomocí technologií.
- Subjektivní profilování – prostřednictvím lidského rozhraní.

- *Používání specifických charakteristik, rasa, věk, vede k zobecňování osob, zda osoba může být zapojena do nezákonné činnosti.*
- *Posuzování chování osob a analýza psychologických vlastností, s cílem předpovědět nebo posoudit jejich schopnosti.*

Subjektivní profilování

- Subjektivní profilování další rozměr detekce v letecké dopravě, kterou se používá k identifikaci potenciálních pachatelů, nebo narušení letů.

- Profilování provádění běžným leteckým personálem – pracovníci na přepážkách, agenti v gatech, nakladači, pracovníci v třídírně zavazadel a letecký personál

Sleduje se absence normálních, nebo přítomnosti abnormálních vlastností.

Subjektivní profilování
Co je „normální“ ?

- Chování založeno na našich životních zkušenostech, zobrazení charakteristik, oblečení, národnosti, chování, s nimiž se můžeme osoby identifikovat.

- **Jak byste popsali následující cestující ?**

1. *Běžný obchodní cestující letící na pracovní cestu.*
2. *Běžný turista vracející se z Disneylandu.*

Subjektivní profilování
Co je „abnormální“ ?

- Abnormální neznamená neakceptovatelné, nebo špatné. Ani není spojeno žádným způsobem s pohlavím, rasou, barvou pleti nebo etnickým původem.
- Znamená, netypické pro danou situaci.
- Výskyt abnormálního se zaměřuje na to, co by nemělo být. Mnohokrát, je absence normálního doprovázeno přítomností abnormálního.

Netypické může být zcela odlišné od mentálního modelu osoby, kterou pozorujeme.

Subjektivní profilování

- Důležitou součástí profilace pachatelů je **metoda vedení pohovoru** (neboli „Questioning“) s již vytipovaným subjektem.
- Úspěšnost metody závisí především na osobě, která pohovor provádí.
- Vzhledem k velké závislosti pouze na lidském faktoru nelze vyloučit chyby této metody.
- Úspěšnost metody závisí na několika aspektech:
  1. Správnost určení hrozby daného letu.
  2. Znalost standardního cestujícího daného letu a profilu teroristy.
  3. Precizní provedení kontroly cestovních dokladů cestujícího.
  4. Pozorování cestujícího (chování, vzhled), zavazadel, spolucestujících.
  5. Správná technika vedení pohovoru

Subjektivní profilování

- Otázky by měly být kladeny systematicky, dle naučeného scénáře (nikoli nahodile), aby bylo možné co nejefektivněji rozlišit nestandardní reakce a měly by vycházet z informací získaných prvotním pozorováním a kontrolou cestovních dokladů.
- Pro ověření pravdivosti odpovědí, je možné otázky v jiné fázi rozhovoru znovu zopakovat a získané odpovědi porovnat.
- Využívají se čtyři základní typy otázek:

1. Kontrolní otázky
2. Neutrální otázky
3. Relevantní otázky
4. Symptomatické otázky

Subjektivní profilování

- **Kontrolní otázky** - jsou pokládány z důvodu ověření výpovědi metodou, kdy osobu přivedeme cíleně ke lživé odpovědi, abychom mohli porovnat reakci při pravdivé a lživé výpovědi (například otázka: „Lhal jste někdy partnerovi?“).
- **Neutrální otázky -** umožňují navrátit posuzovanou osobu do neutrálního fyziologického stavu, pokud předtím reagovala na jiný podnět.
- Tento postup je aplikován z důvodu potřeby zvýraznění rozdílů mezi reakcemi na relevantní otázky.
- Stejný typ otázky může vyvolávat u různých osob různé reakce, proto je zapotřebí ptát se systematicky.

Subjektivní profilování

- **Relevantní otázky -** jsou cíleny k jádru problému a jejich úkolem je vyvolat fyziologickou reakci doprovázenou registrovatelným projevem.
- U posuzované osoby mohou navíc vyvolat pocit podezření kontrolní osoby s možností zmaření plánů. Příkladem může být otázka: „Jste terorista?"

- **Symptomatické otázky -** se užívají pro zjištění nepřirozených reakcí posuzované osoby.
- Následná reakce se porovnává s reakcí na relevantní otázku. Příkladem otázky může být: *„Je něco v nepořádku?"*

Subjektivní profilování

- Porovnávají se nejen reakce na otázky, ale rovněž projevy nonverbální komunikace.
- Nejdůležitější jsou optické a akustické vjemy kontrolující osoby, proto musí posuzovanou osobu neustále sledovat a poslouchat obsah a formu odpovědí.
- Kontrolující osoba musí být připravena na tendence kontrolovaného odbočovat od tématu, přehnaně reagovat (přílišná přátelskost nebo naopak neochota ke spolupráci), zastírat úmysly, přehánět, předstírat rozhořčenost, bagatelizovat atd.
- Existuje výčet nonverbálních a verbálních projevů rozrušení osob, které mají pro kontrolující osobu důležitou vypovídající hodnotu

Subjektivní profilování
Stresové situace a jejich zdroje

- **Co sledovat:**

1. **Hlava (oči, ústa, rty, tváře, vlasy, krk)**
2. **Ruce a paže**
3. **Nohy a chodidla**
4. **Ostatní tělesné pohyby nebo náznaky, čeho si všímat**
5. **Nervózní chování**
6. **Další potenciální abnormální / nebezpečné chování, na které se zaměřit.**

Subjektivní profiling a sluchové projevy rozrušení

- Není schopen odpovědět
- Váhá s odpovědí
- Odpoví na otázku otázkou
- Zopakuje otázku a pak vás požádá, abyste zopakovali otázku
- Neustále vás žádá o bližší vysvětlení otázek
- Třese se mu hlas
- Koktá
- Přerývaný hlas
- Mluví váhavě
- Neodpoví na položenou otázku
- Pomlaskává
- Hluboce vzdychá
- Opakovaně si odkašlává
- Zívá (velmi důležitý znak)
- Skřípe zubama

Profiling a nonverbální projevy rozrušení

- Zčervenání v obličeji
- Zblednutí – výmluvnější
- Viditelně se třese
- Vyhýbá se pohledu z očí do očí
- Těká pohledem z místa na místo
- Přílišné mrkání
- Rozšířené zorničky
- Zavírá oči
- Zakrývá oči
- Mne si nos, nebo se jej dotýká
- Uhlazuje si nebo upravuje knírek
- Popotahuje ušní lalůčky
- Zakrývá si uši
- Popleskává si rukou o tváři
- Upravuje a uhlazuje si vlasy
- Zívání

•Olizuje a kouče si rty
•Zakrývá si ústa
•Opakovaně nebo příliš často polyká
•Pulzující krční tepna
•Intenzivně se potí
•Ruce neklidné
•Hraje si se šperky
•Mne si ruce nebo prsty
•Opakovaně se škrábe
•Popotahuje za oděv nebo část těla
•Sedí si na rukou nebo je jinak ukrývá
•ukazuje na něco jiného
•Neustále si čistí oblečení
•Neudrží paže v klidu
•Podupává si
•Ruce v oblasti rozkroku

Technologické profilování

Systems
- Queue management
- Behavioral identification
- Rapid risk assessment
- Screening methodologies

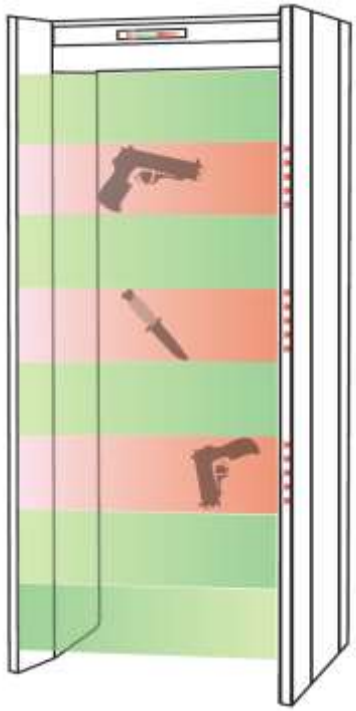
Operational Characteristics
- Discover screening methods for intent
- Avoids All Privacy Issues
- Simple to operate and use

Functions
- Attribute measurement
- Risk determination
- Behavior focused screening

Homeland Security

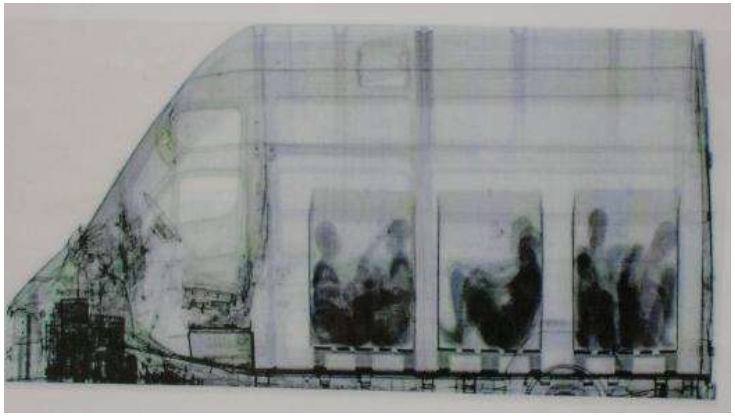
Technologický profiling

Detektory kovu a rentgeny



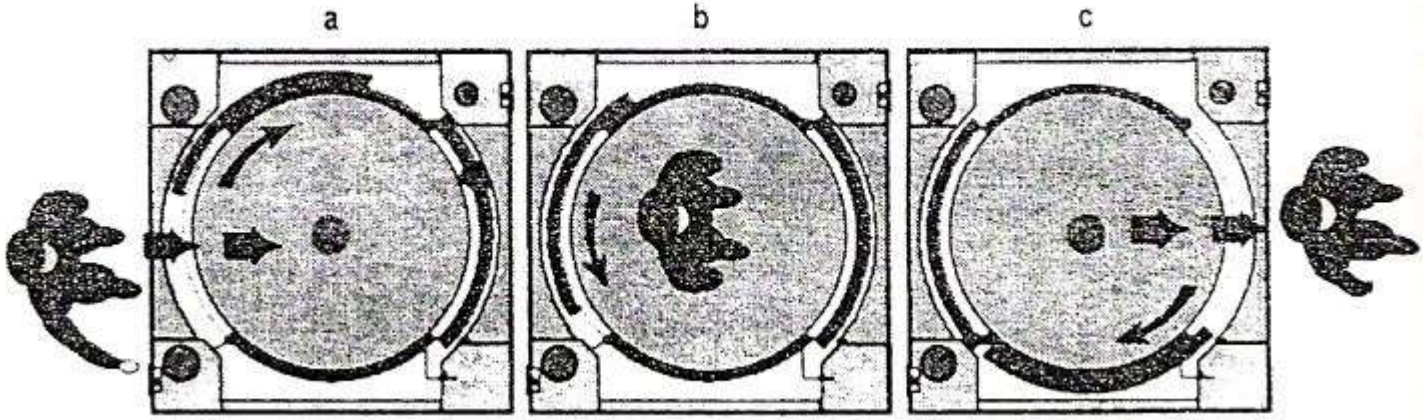
RaŠ

Technologické profilování
Detektory kovu a rentgeny

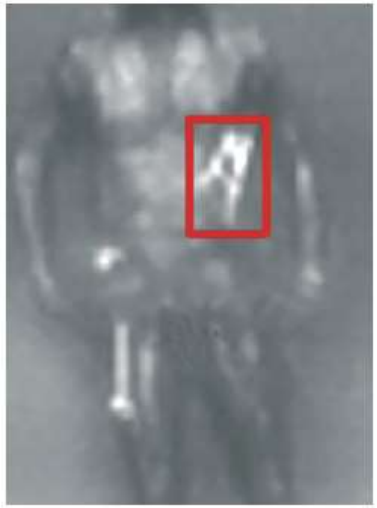


Technologické profilování
Detektory kovu a rentgeny

Otočné dveře uzavřou osobu po dobu skenování

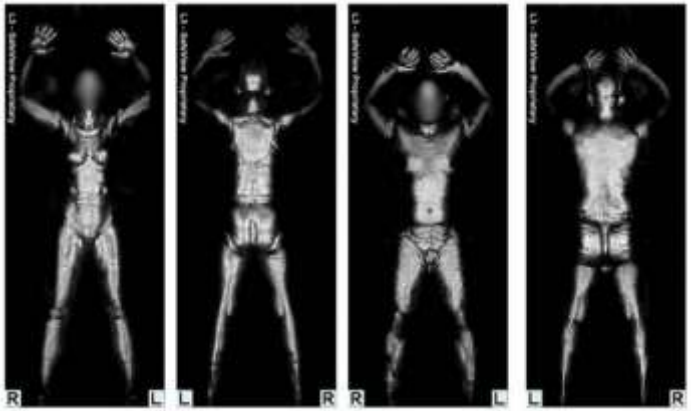


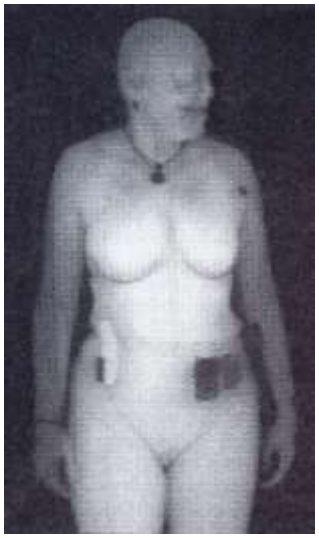
Technologické profilování - termokamery identifikující zvýšenou tělesnou teplotu



Technologické profilování Milivize

- každý člověk vyzařuje v oblasti mm vln (lambda 3 mm), vyzařování těla je stíněno předměty na těle, převodem záření na el. signál se dá získat obraz, kde jsou zobrazeny předměty, které stíní vyzařování, výhodou je, že systém detekuje i keramické (nekovové) zbraně .





RaŠč

Real-Time Pulse Monitor 1/3

- Společnost Fujitsu Laboratories vyvinula a v březnu roku 2013 publikovala technologii pro měření srdeční frekvence osob v reálném čase (Real-Time Pulse Monitor – RTPM).
- Systém je založen na detekci změn světlosti obličeje způsobených průtokem krve.
- Měření vyhodnocuje pohlcování zeleného světla hemoglobinem, který je součástí krve. Systém snímá videosekvenci daného subjektu a následně propočítává průměrné hodnoty barevných složek (RGB – červená/zelená/modrá) v oblasti obličeje pro každý snímek sekvence.

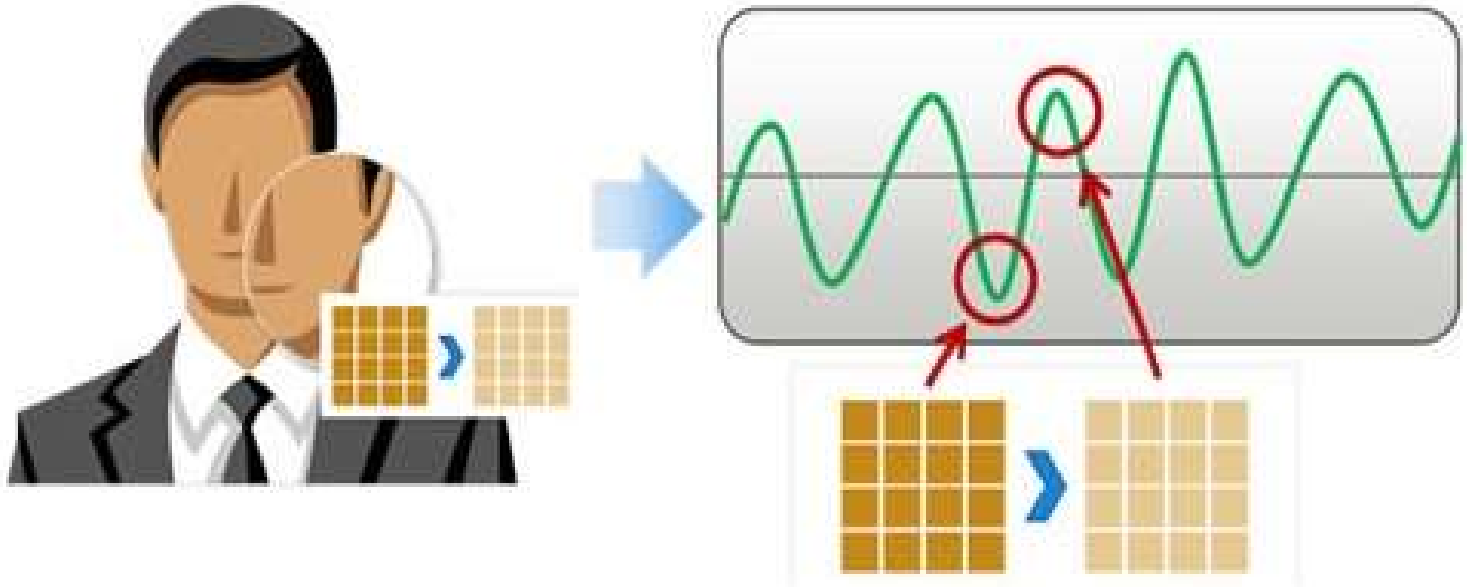
Real-Time Pulse Monitor 2/3

- V dalším kroku odstraní irelevantní data pro výpočet ze všech tří barevných složek a extrahuje křivku jasu zelené složky. Tepová frekvence se poté vypočte na základě amplitud průběhu křivky jasu zelené složky.
- Systém dokáže automaticky rozpoznat data, která jsou ovlivněna pohyby obličeje či celého těla (pohyby hlavou, mluvení, chůze) a automaticky tato data eliminuje z výpočtů. Proces probíhá zcela bezkontaktně s danou osobou. Kompletní procedura trvá přibližně 5 sekund.
- Technologie je zajímavá především svou jednoduchostí, jelikož pro snímání obrazu lze využít standardní digitální kamery
- Lze využít pro vyhledávání osob s podezřelým chováním, ale i jedinců ve špatném zdravotním stavu

Real-Time Pulse Monitor 3/3

Detekce změn světlosti pokožky obličeje

Výpočet srdeční frekvence



Systém WeCU 1/7

- WeCU Technologies je Izraelská společnost, zabývající se výzkumem a vývojem technologií pro „čtení mysli" pro účely detekce potenciálních teroristů na letištích.
- Systém WeCU vznikl z důvodu obnovení teroristických útoků v Izraeli v roce 2002.
- 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 nezpozorovatelný.

Systém WeCU 2/7

- Technologie zahrnuje promítnutí infračerveného podprahového obrazového vjemu, který by rozpoznal pouze terorista (symbol teroristické organizace, obrázek výbušniny, atd.).
- Celý princip fungování je založen na faktu, že lidé vždy reagují na jim dobře známý obrazový vjem, pokud ho spatří na neobvyklém místě. Například pokud člověk nečekaně spatří obraz své matky na obrazovce, jeho tvář a tělo na tuto skutečnost zareagují.
- Pro účely detekce teroristů jsou reakce lidí vyhodnocovány bezpečnostním personálem, ale také skrytými kamerami a senzory, které jsou schopny detekovat mírný nárůst tělesné teploty, srdeční frekvence a pohyby očí.

Systém WeCU 3/7

- Databáze promítaných obrázků je velmi rozsáhlá a rozmanitá
- Je potřeba zvolit různá místa, kde probíhá promítání obrázků, aby bylo možné v co nejvyšší míře eliminovat připravenost teroristů na přítomnost tohoto systému.
- Dokonce trénovaní teroristé dle prozatímního výzkumu společnosti nedokázali ovládat svá těla do té míry, aby změny jejich fyziologických parametrů systém nedokázal detekovat
- Metoda fungování je založena na principu propojení detekčních elektrických senzorů se znalostmi získanými z behaviorálních studií.

Systém WeCU 4/7

- Cestující je kontrolován během rutinních činností na letišti, jako je například Check-in u automatického letištního kiosku.
- Cestujícímu je promítnut téměř neviditelnému stimul, který ihned spouští fyziologické reakce těch osob, které skrývají svůj úmysl.
- Senzory umístěné v tomto kiosku snímají reakce dotyčné osoby a upozorňují bezpečnostní personál.
- Systém také dokáže odlišit pouze vystresovanou osobu

Systém WeCU 5/7

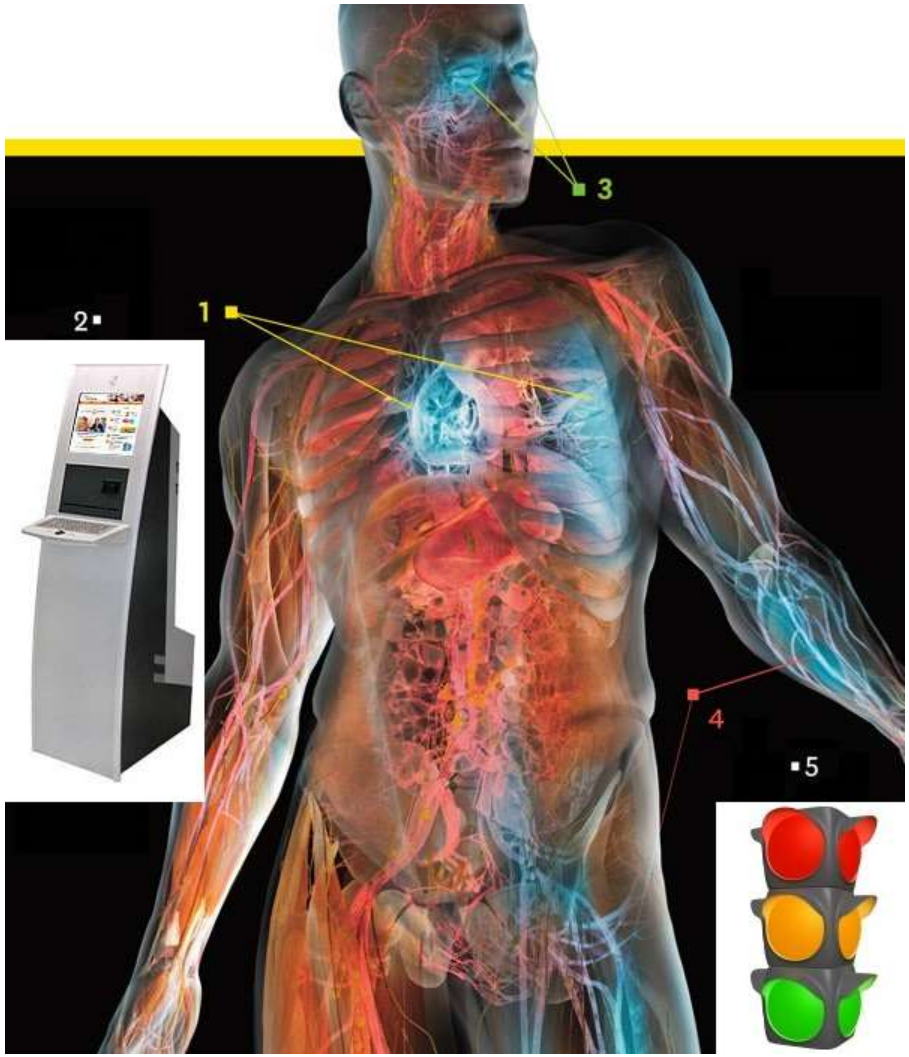
- **Princip fungování systému WeCU:**

1. Systém senzorů je založen na měření srdeční frekvence, tělesné teploty a frekvence dýchání cestujícího.
2. Systém vystavuje osobu nenápadným podnětům. Jako příklad lze uvést situaci, kdy je u check-in kiosku uživatel vyzván „Zadejte jméno" ale krátce se objeví příkaz „Zadejte skutečné jméno" („Enter name" -> „Enter real name"). Většina cestujících by na tento podnět neměla reagovat s výjimkou těch, kteří skrývají svou pravou identitu.

Systém WeCU 6/7

3. Senzor měří pohyby očí a zaznamená jakékoli zrychlení pohybu nebo mrkání v reakci na podněty.
4. Infračervená kamera měří teplotu cév, shromažďuje údaje o teplotě a srdeční frekvenci. Tato data pak porovnává s referenční hodnotou.
5. Systém upozorňuje bezpečnostní personál prostřednictvím blikajících světel. Zelená barva signalizuje normální stav, červená označuje zareagování na podněty, oranžová nejednoznačné vyhodnocení reakcí.

Systém WeCU 7/7



Přístroj Malintent aneb „Zlý úmysl“ 1/3

- Technologický systém pro detekci potenciálně podezřelých osob z terorismu, který byl vyvinut ministerstvem vnitra Spojených států.
- Umožňuje na dálku detekovat stav mysli člověka a jeho případný „špatný“ úmysl prostřednictvím senzorů.
- Systém snímá tělesnou teplotu, srdeční frekvenci, frekvenci dýchání, tělesný pach a nonverbální projevy (mimika obličeje, pohyby těla).
- Využívá se velké množství snímačů pro detekci a analýzu lidské mimiky s následným vyhodnocením potenciálu páchání trestné činnosti.

Přístroj Malintent aneb „Zlý úmysl" 2/3

- Systém může obsahovat také senzory pro analýzu pohybu osoby, oční skener a senzor feromonů. Celá procedura trvá maximálně v řádu jednotek minut.
- Při vývoji byl kladen důraz také na rozeznání vystresovaného jedince od osoby s úmyslem páchání trestného činu.
- Skenovaná osoba není schopna rozeznat proces snímání.
- V případě vyhodnocení poplachu je tato informace předána bezpečnostnímu personálu, který rozhodne, zdali bude osoba podrobena dalšímu posouzení (například metoda dotazování).

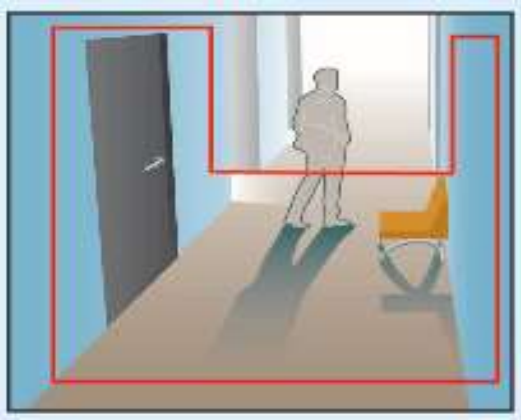
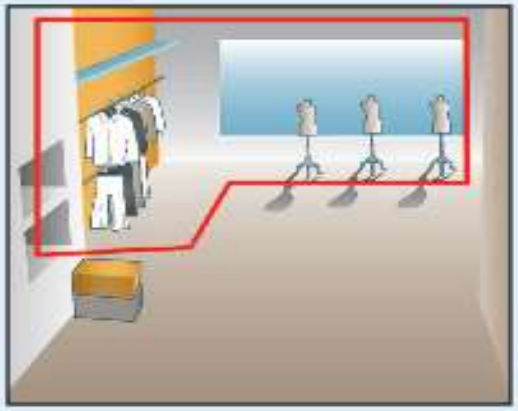
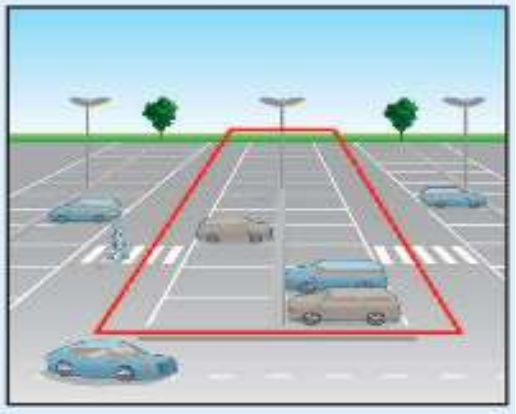
Přístroj Malintent aneb „Zlý úmysl" 3/3

Videoanalýza 1/7

- Moderním prostředkem pro zajištění bezpečnosti s omezením vlivu lidského faktoru a úsporou nákladů na provoz je využití inteligentní videoanalýzy kamerového záběru.
- IP kamery disponují digitálním obrazovým výstupem, který je možné prostřednictvím analytického software zpracovávat a vyhodnocovat.
- Poté je obsluze systému nebo PCO poskytnuta informace o překročení prahové hodnoty a ta má možnost provést další opatření.
- Sofistikovanější systémy dovolují automatizaci reakce na vyvolaný poplach například spuštěním mechanických zábranných prostředků, elektrické požární signalizace atd.

Videoanalýza 2/7

- Pro potřeby zajištění ochrany civilního letectví před protiprávními činy lze využít následující funkce videoanalýzy:
  - zónování monitorovaného prostoru,
  - vzdálený monitoring předmětů,
  - počítání osob,
  - heat mapping.

Videoanalýza 3/7

- **Zónováním monitorovaného prostoru** se rozumí SW (dále jen softwarové) rozdělení obrazu kamerové jednotky na oblasti.
- Jakmile dojde ke vstupu osoby do střežené zóny, kamerový systém vyvolá poplach a dále je postupováno dle nastavených opatření (upozornění na lokální dispečink nebo PCO s online přenosem obrazu, upozornění na mobilní telefon vybrané osoby, atd.).
- Pro realizaci popsané funkcionality je zapotřebí zvolit vhodnou kombinaci hardware a software

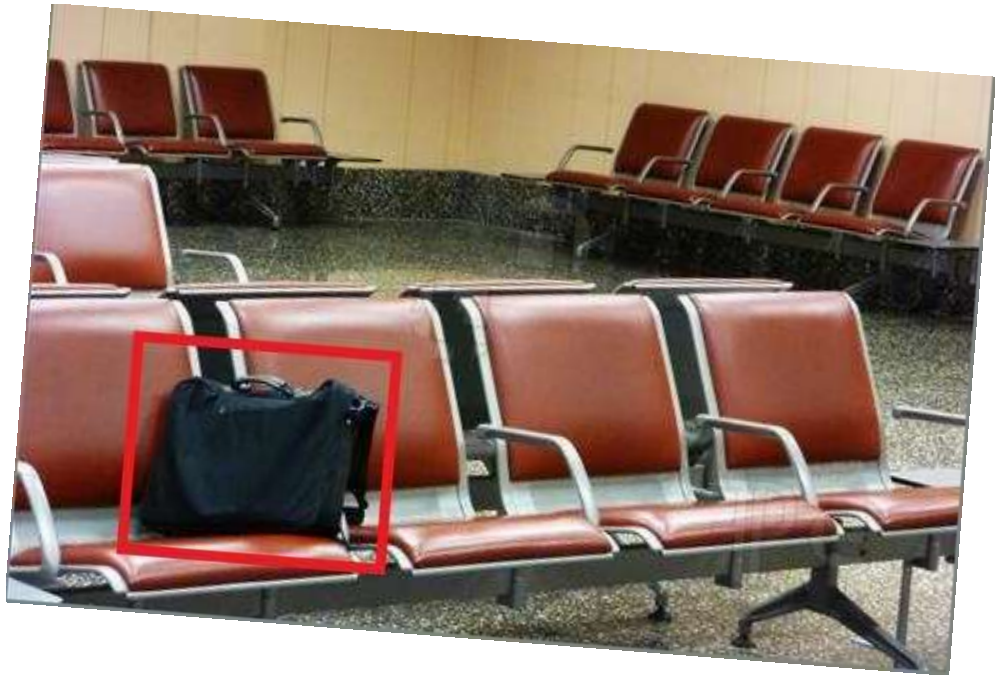
Videoanalýza 4/7

- **Vzdálený monitoring předmětů** lze využít ve dvou rovinách.
- První možností je ***střežení vybraného předmětu*** umístěného v obrazu kamerové jednotky s aplikovanou videoanalýzou.
- Jakmile dojde k odstranění nebo přemístění předmětu ze záběru, kamerový systém tuto změnu detekuje a vyhlásí poplachový stav.
- Druhou možností z pohledu zajištění bezpečnosti letiště daleko zajímavější je ***detekce ponechaného předmětu*** v prostoru monitorovaném kamerovým systémem.
- Systém umožňuje rozpoznat změnu obrazu vzhledem k původním parametrům a zároveň eliminovat dynamické vlivy (průchod osob se zavazadly).

Videoanalýza 5/7

- Tuto vlastnost lze využít například pro detekci umístěná nástražného výbušného systému (NVS) do monitorovaného prostoru s následným informováním bezpečnostního personálu.

- Příklad analýzy odloženého předmětu



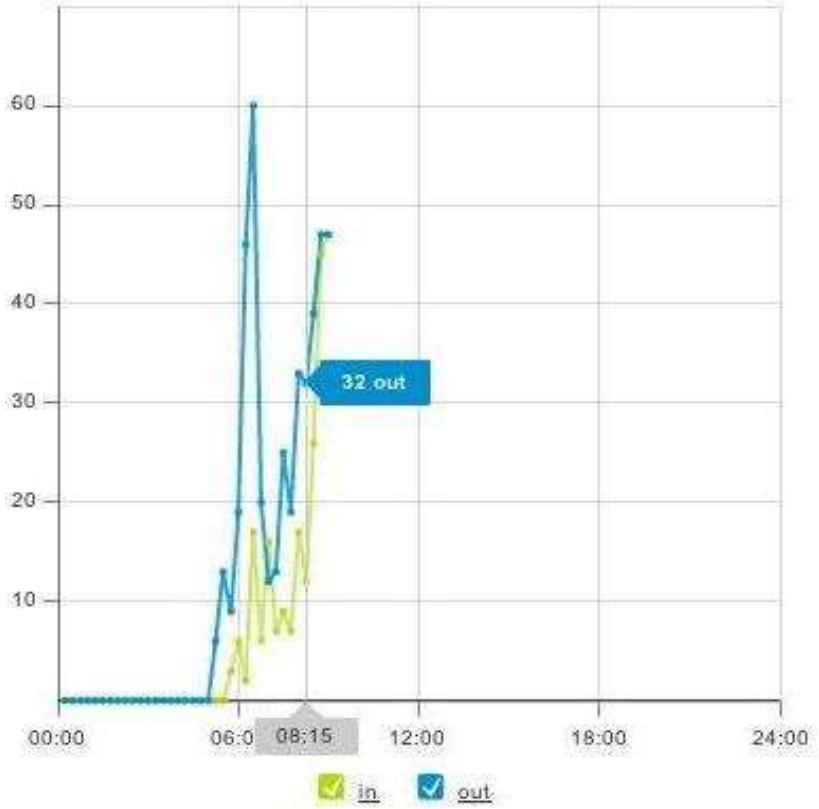
Videoanalýza 6/7

- **Počítání osob** (neboli people counting) lze zajistit aplikací úsečky (úseček) do zorného pole kamerové jednotky
- Pokud dojde k jejímu překročení (v nastaveném směru, možno i oběma směry), je tato informace zaznamenána.
- Problém nastává při aplikaci na větší skupinu osob, kdy systém není schopen stoprocentně rozeznat veškeré pohybující se objekty.
- Počítání osob lze využít pro sledování prostorů s omezeným pohybem, nebo pro zjištění počtu osob v daném úseku v případě evakuace, kdy je možno porovnat počet osob, které vstoupily do objektu s počtem osob, které ho opustily, a vyhodnotit rozdíl.

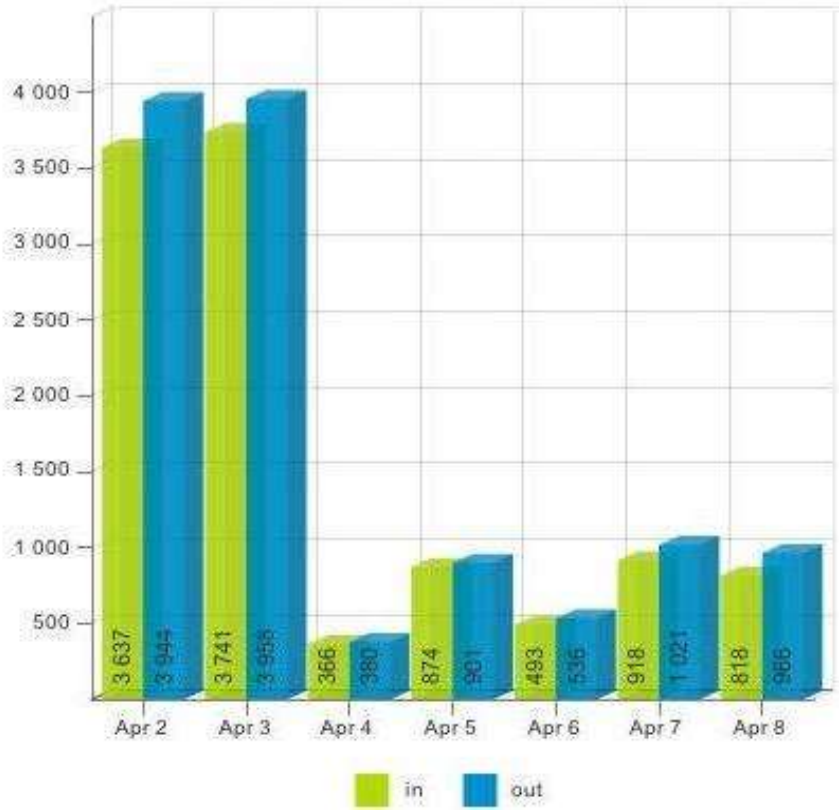
Videoanalýza 7/7

	2/4	3/4	4/4	5/4	6/4	7/4	8/4	9/4	Average
In	3637	3741	366	874	493	918	818	1162	1150
Out	3944	3958	380	901	536	1021	966	1329	1672

Day chart

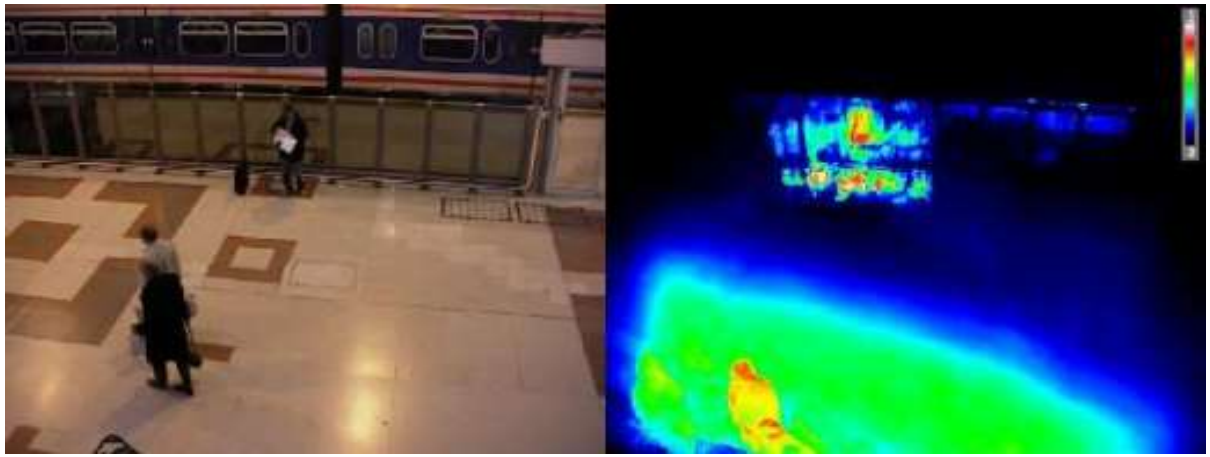


Week chart



Heat mapping

- Tato funkce byla původně vyvinuta pro marketingové účely.
- Prostřednictvím propojení IP kamer a analytického software umožňuje grafické znázornění pohybu osob po monitorované scéně a grafické odlišení prostor scény dle hustoty pohybu.
- V oblasti bezpečnosti lze uplatnit při profilování osob, v případě analýzy nestandardního pohybu jedince po monitorované scéně, včetně analýzy trajektorie pohybu.



Analýza hlasu 1/5

- Jedná se o jednu z moderních technických metod pro zajištění bezpečnosti
- Metodu technologie analýzy hlasu vyvíjí například izraelská společnost Nemesysco, která se zabývá výzkumem a vývojem technologií pro analýzu hlasu, za účelem odhalování emocí, předcházení podvodům, zvládání stresu a jiné.
- Nezaobírá se analýzou obsahu řeči, ale prvků a abnormalit toku lidské řeči, které jsou charakteristické pro různé situace, proto není závislá na jazyku, kterým posuzovaná osoba hovoří.

Analýza hlasu 2/5

- Technologie funguje na principu přednastaveného setu vokálních parametrů definovaných výzkumem v korelaci s klíčovými lidskými emocemi v různých kombinacích, aby byla schopna odhalit podvodné úmysly v běžných situacích.
- Mnoho z posuzovaných parametrů je přitom ve světě fonetiky nových a zaměřených na prozatím neobjasněné vlastnosti lidského hlasu.
- Analýza může být provedena v reálném čase na uskutečněném hovoru nebo telefonátu, ale také na nahraném vokálním materiálu. Technologie není detektorem lži.
- Používanou analýzou je takzvaná **LVA** (Layered Voice Analysis), neboli vrstvená analýza hlasu.

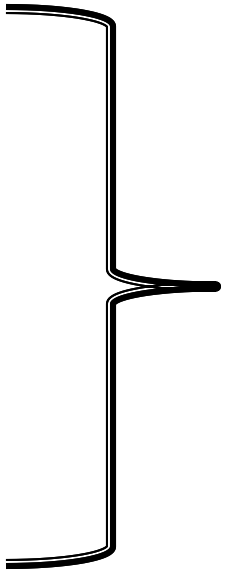
Analýza hlasu 3/5

- Užívána je například při bezpečnostních kontrolách, kontrolách vstupu, sběru informací nebo zákonném odposlouchávání.
- Technologie je schopna zachytit emoční křivky v lidském hlasu, čímž lze analyzovat duševní stav a emoční rozpoložení posuzované osoby.
- Detekované jevy jsou matematicky vyhodnocovány a přiřazeny emočním stavům.
- Z těchto informací je možno získat náhled na myšlenkové pochody pachatele, příčiny jeho trápení, nadšení, nejistoty v projevu, témata přitahující jeho pozornost, citlivá témata, atd.
- Analýza je v současnosti zaváděna na letištích, v bankách, pojišťovnách, atd.

Analýza hlasu 4/5

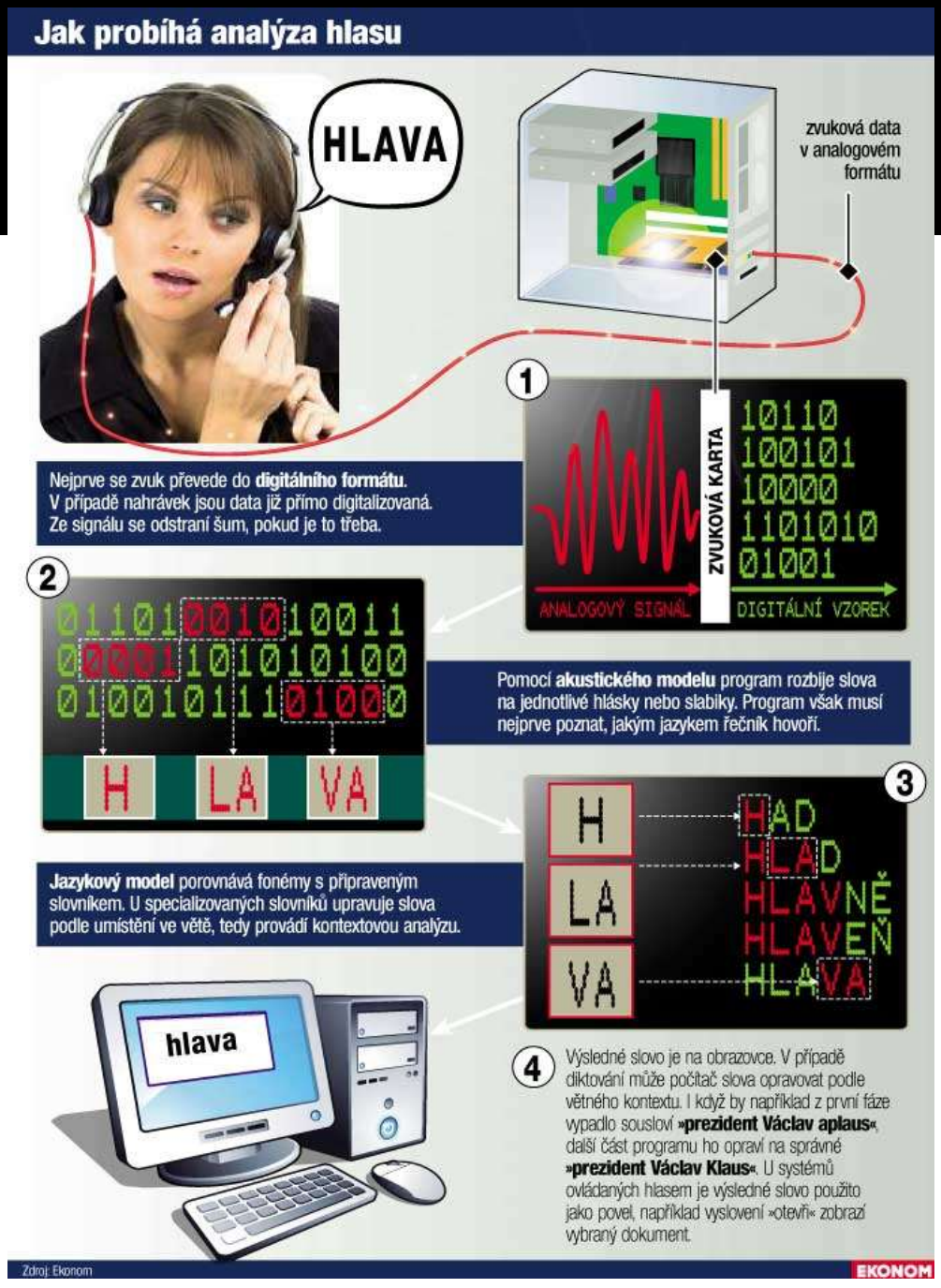
Identifikované jevy:

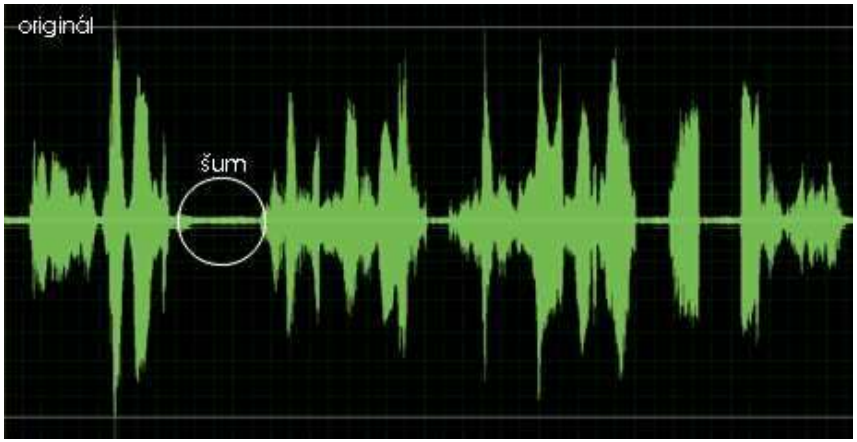
- různé typy stresu,
- nadšení,
- zamyšlení,
- zmatenost,
- kognitivní (myšlenkové, rozumové) procesy,
- emocionální reakce,
- atd.

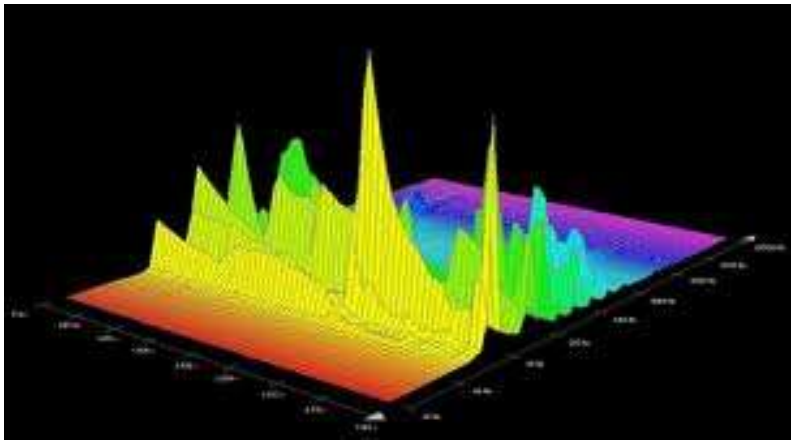


SPECIFICKÉ VLASTNOSTI LIDSKÉHO HLASU

Analýza hlasu 5/5







BEMOSA

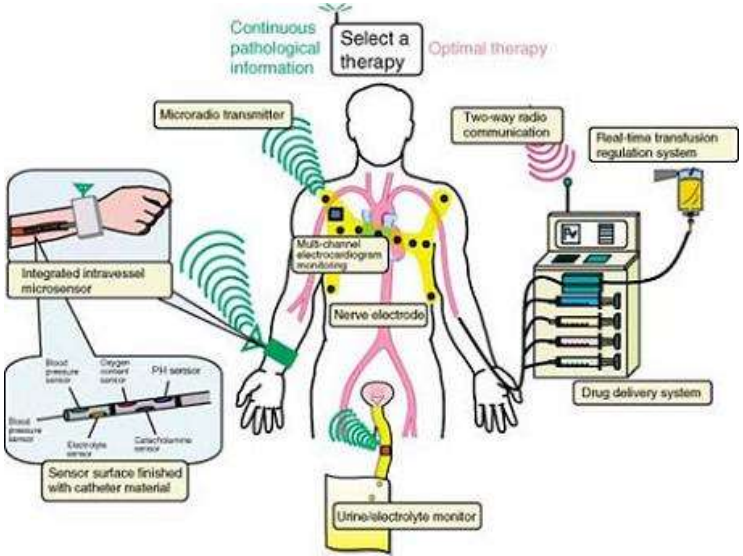
- BEMOSA (zkratka anglického Behaviour Modelling for Security in Airports) neboli **Behaviorální modelování pro bezpečnost na letištích**
- Jedná se o celoevropský výzkumný projekt zaměřený na zvýšení bezpečnosti na letištích.
- BEMOSA vyvíjí behaviorální SW model, jehož cílem je popsat, jak lidé realizují rozhodnutí v bezpečnostních otázkách za standardních podmínek nebo při krizových situacích.
- Hlavním cílem projektu je zvýšení bezpečnosti na letištích a optimalizace nákladů.

Systém řízení bezpečnostních pracovníků

- Systém řízení bezpečnostních pracovníků (neboli Guard management system) umožňuje efektivně a dynamicky reagovat na poplachové stavy systémů technické ochrany v případě potřeby zásahu bezpečnostního personálu letiště.
- Monitoruje polohu a stav jednotlivých bezpečnostních pracovníků a případě vzniku mimořádné události, umožňuje dispečerovi zvolit bezpečnostního pracovníka, který je nejblíže místu poplachu a má možnost zasáhnout.
- Systém je založen na principu přenosných zařízení s integrovaným mobilním telefonem, GPS, tísňovým tlačítkem, fotoaparátem, atd. (například v provedení PDA), kterými bezpečnostní pracovníci disponují. Toto zařízení umožňuje příjem poplachového stavu ze systému profilace v dané lokaci

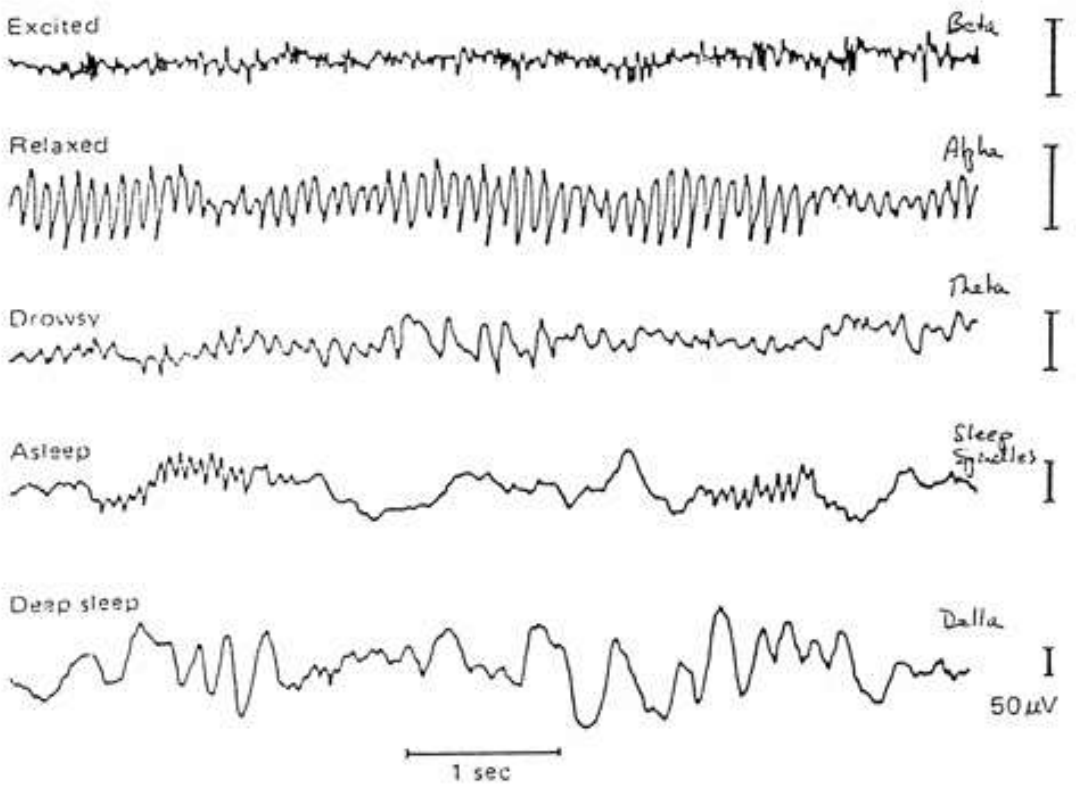
Biosignály 1/7

- Aby bylo možné exaktně měřit míru reakce člověka na vnější podněty, lze využít takzvané fyziologické funkce a jejich biosignály.
- Tyto signály jsou proměnné v čase dle míry působení vnějšího podnětu a citlivosti daného jednice na daný podnět.
- Různí lidé reagují na stejný podnět rozdílným způsobem.



Biosignály 2/7

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



Biosignály 3/7

- **Elektrické biosignály** generují nervové a svalové buňky jako výsledek elektrochemických procesů.
- Při působení stimulu přesahující prahovou hodnotu buňky je generován akční potenciál (tok iontů), který lze změřit například mikroelektrodami.
- Potenciál je předáván okolními buňkami a umožňuje vytvářit elektrické pole v tkáni, které je měřitelné na povrchu těla.
- **Impedanční biosignály** lze měřit aplikacemi elektrického proudu o nízkých hodnotách proudů (mikro až miliampéry) do lidského těla.

Biosignály 4/7

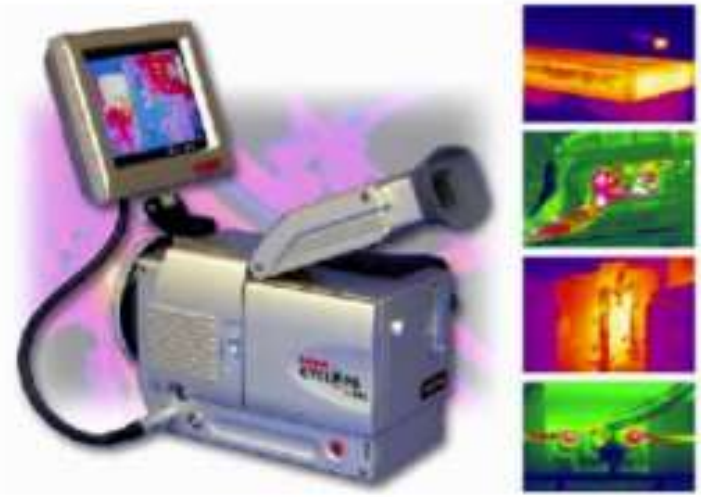
- Z vypočítaného odporu lze poté určit nervovou a endokrinní aktivitu, objem krve, nebo skladbu tkání.
- **Magnetické biosignály** jsou generovány orgány, jako například mozek či srdce a vypovídají o aktivitě těchto tkání.
- Přesné měření generovaných magnetických polí je však v současnosti velmi obtížné vzhledem k nízkým hodnotám ve srovnání s geomagnetickým polem Země.
- **Akustické biosignály** jsou generovány například průtokem krve srdečními chlopněmi a cévami, průtokem vzduchu dýchacími cestami, zažívacím ústrojím nebo klouby.
- Měření těchto signálu probíhá prostřednictvím mikrofonů a vypovídá o funkci zkoumaných orgánů.

Biosignály 5/7

- **Chemické biosignály** jsou reprezentovány stanovením koncentrací iontů v buňkách prostřednictvím speciálních elektrod, stanovením parciálních tlaků plynů a měřením hodnoty pH. Získané hodnoty vypovídají o stavu zkoumané tkáně
- **Mechanické biosignály** jsou odvozeny z mechanického pohybu nebo průtoku. Prostřednictvím mechanických mikrosnímků lze změřit například tlak krve.
- **Optickými biosignály** se rozumí změna optických vlastností organismu. Například okysličení krve lze měřit na základě intenzity odraženého světla (dle vlnových délek) od tkáně nebo užívání abiotických tekutin (barvící tekutiny) při získávání informací o plodu.

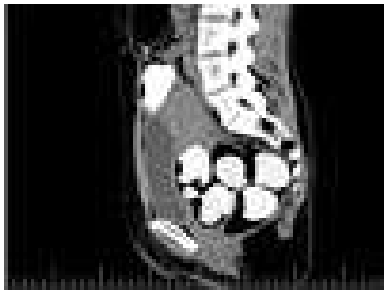
Biosignály 6/7

- **Tepelné biosignály** vypovídají o stavu fyzikálních a biochemických procesů v organismu a jejich rozložení po těle je různé. Měření je možno provádět kontaktním způsobem klasickými teploměry nebo bezkontaktně například termokamerou.



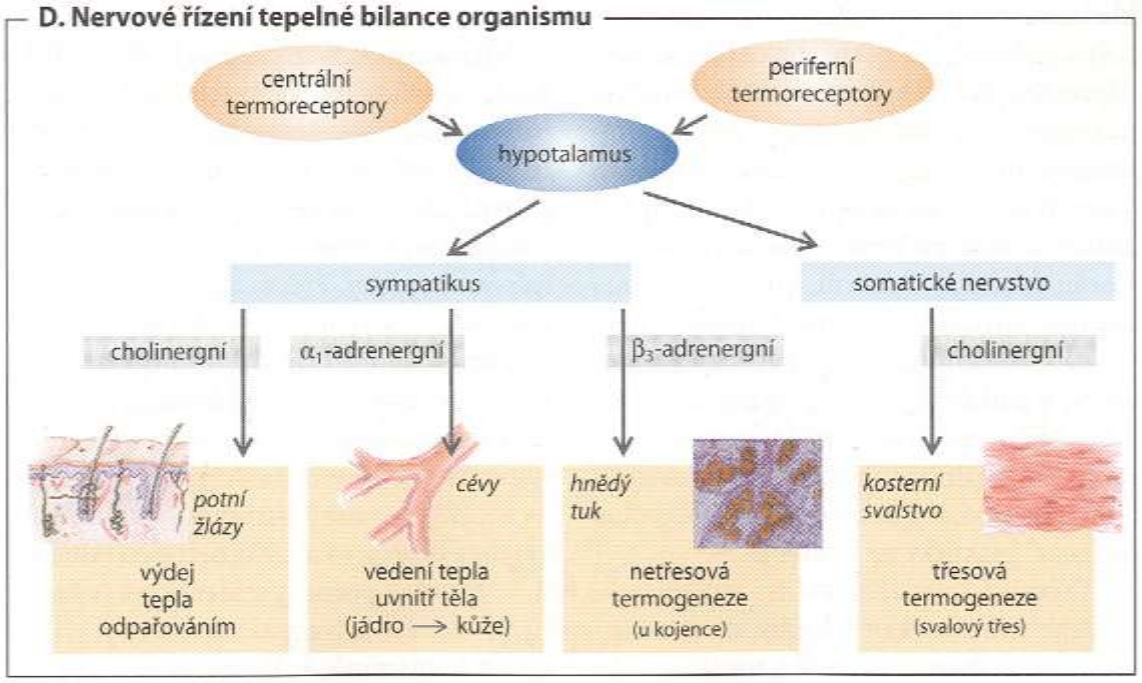
Biosignály 7/7

- **Radiologické biosignály** lze využít pro získání informací o vnitřních anatomických strukturách. Vznikají reakcí ionizujícího záření s buňkami organismu.
- **Ultrazvukové biosignály** vznikají interakcí ultrazvuku s buňkami (tkáněmi) a umožňují získání informací o velikosti objektu a charakteru pohybu. Měření probíhá piezoelektrickými senzory.



Tělesná teplota 1/2

- Tělesná teplota vyjadřuje rovnováhu mezi vyráběným teplem organismem a jejím výdejem a ztrátami.
- Ovlivňují ji následující faktory:
  - věk,
  - denní doba,
  - tělesná aktivita,
  - hormony,
  - psychický stav (stres),
  - vlivy okolního prostředí (podněty).



Tělesná teplota 2/2

- Z pohledu typování a profilace potenciálních pachatelů hraje důležitou roli změna tělesné teploty v reakci na uměle vytvořený podnět, kterým je osoba testována.
- Jelikož v prostředí letiště není možné zjišťovat tělesnou teplotu konvenčními metodami (klasický rtuťový teploměr – kontaktní metoda měření), je potřeba aplikovat bezkontaktní metody měření.
- K tomuto účelu lze využít například infračervenou kameru, případně infračervený bezkontaktní teploměr, který dokáže změřit tělesnou teplotu v čase jednotek sekund (při vzdálenosti v jednotkách centimetrů).
- Bezkontaktní teploměry lze rozdělit na tepelné pyroelektrické a kvantové polovodičové.

Srdeční frekvence 1/2

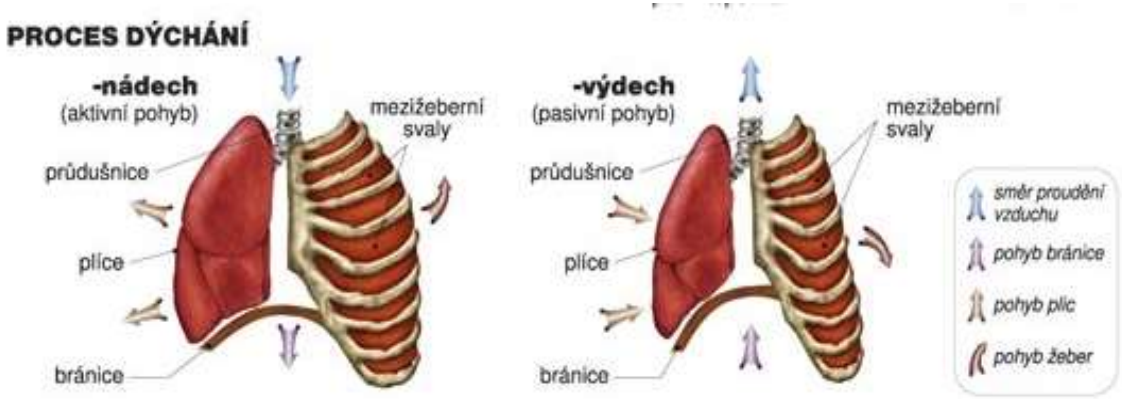
- Srdeční frekvence (neboli tepová frekvence) vyjadřuje počet srdečních pulzů za jednotku čas (1 minutu). U zdravého dospělého člověka se tato hodnota pohybuje v intervalu od 70 do 80 pulzů za minutu.
- Srdeční frekvenci ovlivňují následující faktory:
  - věk,
  - pohlaví,
  - tělesná teplota,
  - kondice,
  - přítomnost krvácení,
  - stres (psychický stav),
  - podněty z okolního prostředí.

Srdeční frekvence 2/2

- Z bezpečnostního hlediska jsou důležité změny vyvolané reakcí na podněty z vnějšího prostředí a přítomnost stresu, které reflektují nestandardní stav osoby – zvýšená srdeční frekvence.
- Bezkontaktní měření srdeční frekvence umožňuje například metoda balistografie, kterou lze aplikovat i přes oděv, nebo měření prostřednictvím infračervené kamery.
- Další možnou metodou měření je snímání intenzity pohlcování zeleného světla hemoglobinem v krvi.
- K měření lze také využít princip snímání elektrického potenciálu vygenerovaného elektrickou aktivitou srdeční tkáně.

Frekvence dýchání 1/2

- Frekvence dýchání vyjadřuje počet nádechů a výdechů za jednotku času (1 minutu). U zdravého dospělého člověka se hodnota pohybuje v rozmezí mezi 14 až 20 nádechy a výdechy za minutu.
- Frekvenci dýchání ovlivňují tyto faktory:
  - věk,
  - pohyb,
  - stres (psychický stav),
  - podněty z okolního prostředí,
  - nadmořská výška,
  - životní styl.

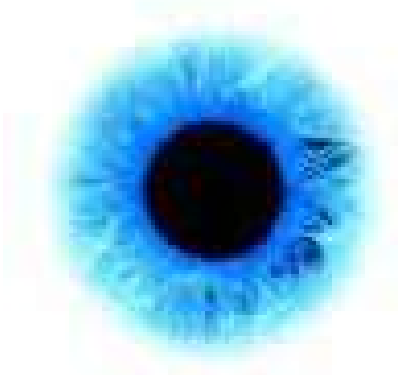


Frekvence dýchání 2/2

- Z bezpečnostního hlediska při typovaní a profilování osob hraje roli především změna frekvence dýchání vyvolaná vnějšími podněty nebo z důvodu stresových faktorů (psychický stav) jedince.
- Stejně jako v případě srdeční frekvence a tělesné teploty lze využít měření změn frekvence dýchání v reakci na vnější podněty, případně využít naměřených nestandardních hodnot z důvodu psychického stavu jedince.
- Bezkontaktní měření frekvence dechu umožňuje například metoda bioradiolokace, která využívá odrazu rádiových vln v relaci s pohyby lidského těla při dýchání.

Biometrie

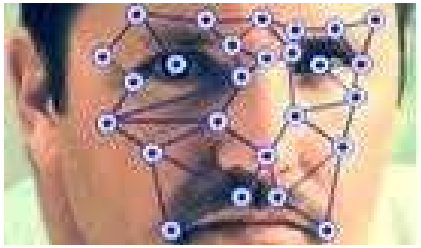
- z řečtiny „**bios**“ = život a „**metron**“ = měřit
- Obor zabývající se studií automatické identifikace osob na základě jejich fyzických vlastností nebo jejich chování

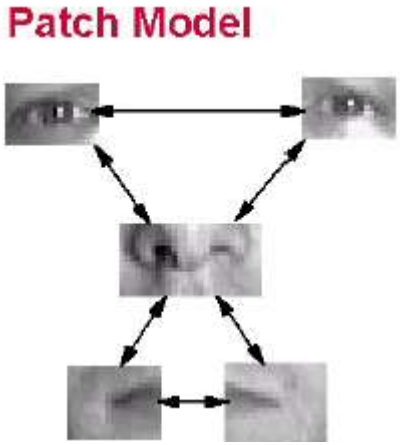


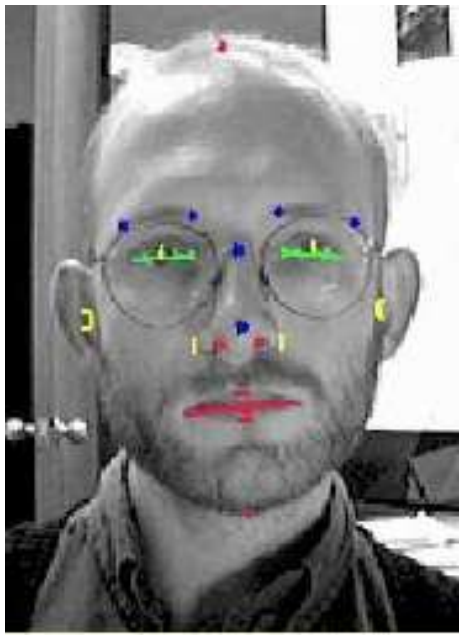
Jednoznačná identifikace osob na základě jedinečných fyziologických znaků

Biometrika

Automatické vyhodnocení neměnných fyziologických a behaviorálních lidských charakteristik

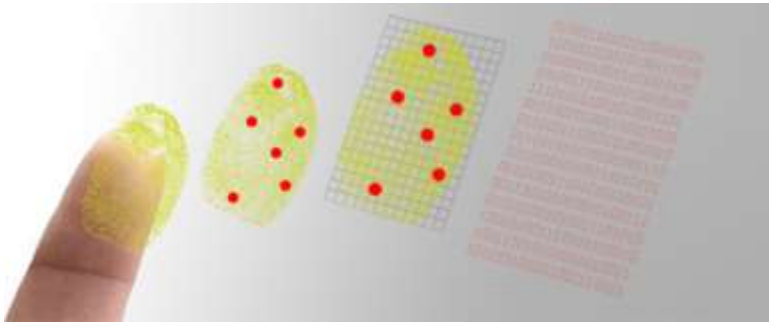






Historický náhled

- Rozpoznávání lidí pomocí biologických charakteristik je metoda využívaná historicky.
- Lidé se rozpoznávají pomocí vzhledu tváře nebo jsou známy otisky dlaní v jeskyních jako jakýsi podpis autora (některé z nich jsou až 30 000 let staré).
- S rozvojem počítačových technologií na konci 60. let se začalo i biometrické rozpoznávání člověka stávat automatizovaným



Základní pojmy z biometrie 1/2

- **Recognition (rozpoznávání)** je druhový termín, který nutně nemusí znamenat identifikaci ani verifikaci. Jedná se o rozpoznávání člověka použitím vhodné tělesné vlastnosti.
- **Verification (ověření nebo verifikace)** označuje proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku s již dříve zapsaným (tzv. šablonou neboli template). Jedná se o tzv. princip one-to-one.
- **Identification (identifikace)** je proces, kdy se biometrické systém pokouší určit totožnost neznámého jedince. Biometrická informace je sejmuta a porovnávána se všemi uloženými vzorky (šablonami). Princip je znám jako one-to-many.

Základní pojmy z biometrie 2/2

- **<u>Authentication</u> (autentifikace, autentizace nebo legalizace)** je pojem, který lze sloučit s termínem rozpoznávání. Ovšem na konci procesu v tomto případě získá uživatel určitý status, např. oprávněný/neoprávněný atd.
- Aplikace lze uplatnit například:
  - Docházka, komerční organizace všeho druhu (výrobní, obchodní, instituce, atd.) s hodinovou i úkolovou mzdou
  - Přístupové systémy, fyzická kontrola vstupů: režimová pracoviště, výpočetní centra, atomové elektrárny (75% atomových elektráren v USA používá HandKey), vývojové laboratoře, komunikační centra, vojenské objekty, kritická místa v nemocnicích, kanceláře vedoucích pracovníků, atp.
  - Osobní identifikace, stravovací systémy, identifikace majitele karty, elektronický podpis

Biometrické vlastnosti

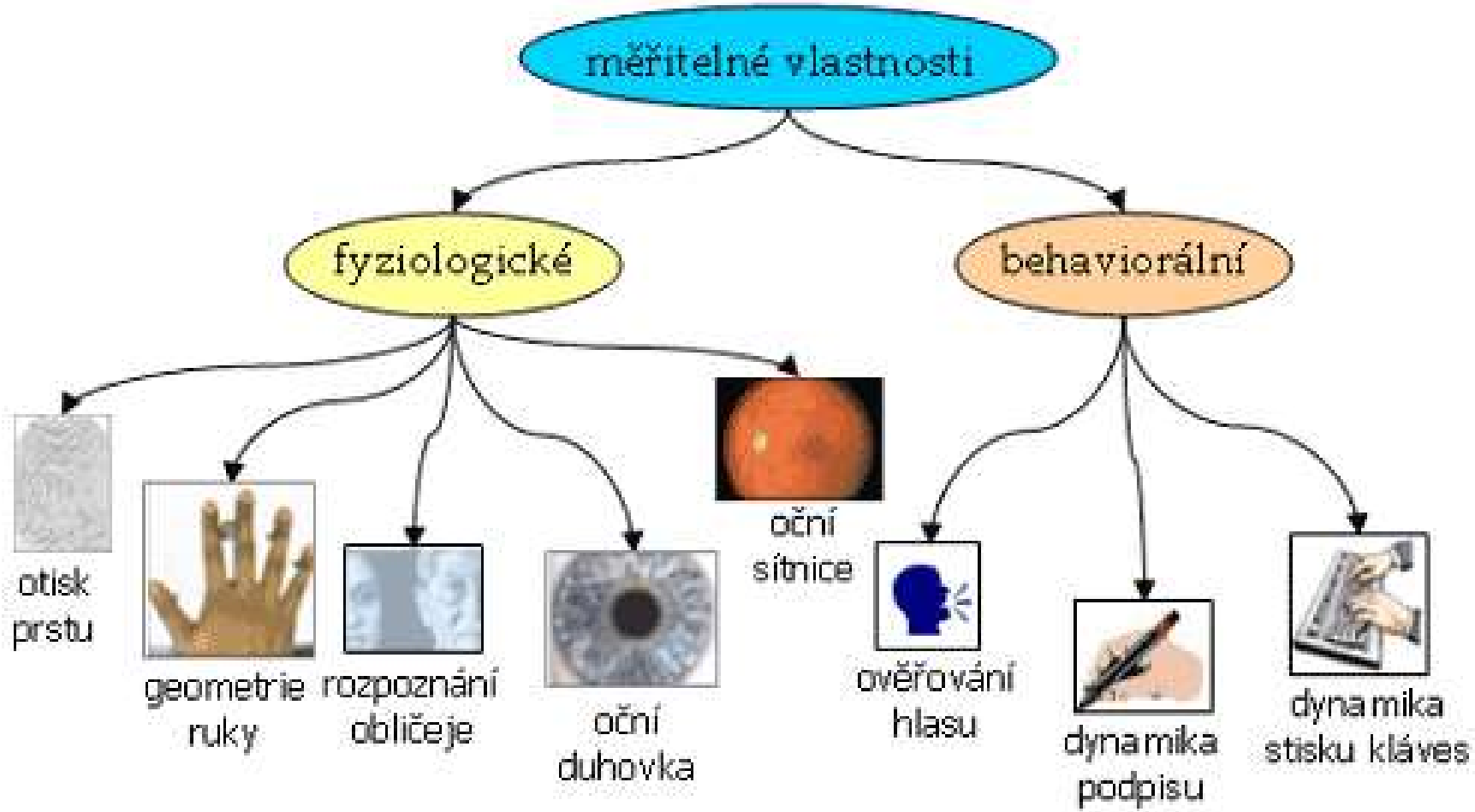
Způsoby, kterými biometrické vlastnosti člověka vznikají, jsou v základě tři:

- **Znaky získané geneticky DNA (*genotypické*),**
- **Znaky získané ve vývoji embrya *(randotypické)*,**
- **Znaky chování získané učením, *(behaviorální)***

Biometrický údaj je citlivým osobním údajem

Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších změn (fyziologická, psychická, kulturní, ekonomická, nebo sociální identita).

Měřitelné vlastnosti



Základní rozdělení biometrik

Autentizace

- **proces jednoznačného ověřování subjektu**

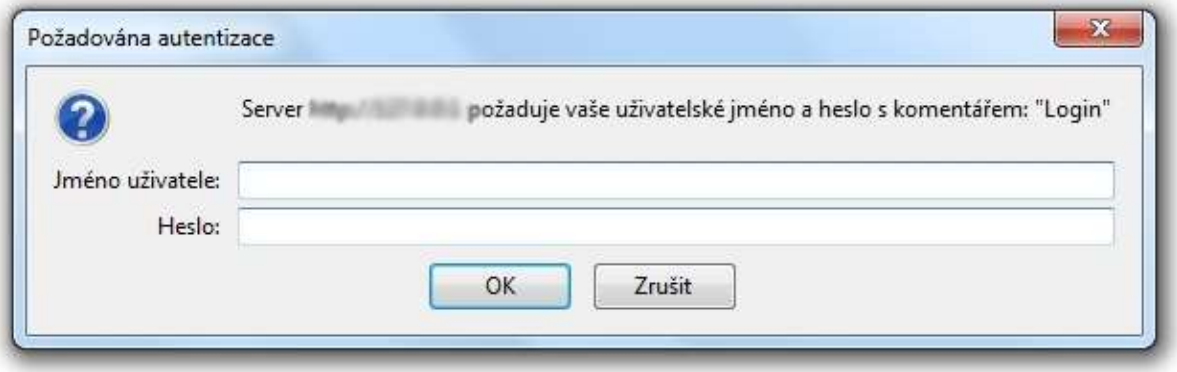
AUTENTIZAČNÍ METODY

- **autentizace heslem** – lze použít pro nejnižší stupeň zabezpečení, je možné se jich relativně snadno zmocnit, jsou přenositelná
- **autentizace předmětem** – tzv. token, vyšší stupeň zabezpečení, lze se jich snadno zmocnit, přenositelné
- **biometrika** – nejvyšší stupeň zabezpečení, nelze ztratit, nepřenositelné

všechny typy zabezpečení mohou být podrobeny útokům, hrozba může být zmenšena použitím jednotlivých metod ve vzájemné kombinaci

Autentizace heslem 1/2

- Použití hesla jako prostředku pro přístup do systému je stále **nejpoužívanějším principem zabezpečení**.
- Velký podíl na tom má i jeho globální použití v osobních počítačích, počítačových sítí, emailových účtech, u SIM karet mobilních telefonů a u platebních karet.
- Bezpečnost je v tomto případě zajištěna tím, že si omezený počet uživatelů (nejlépe jeden) pamatuje **určitou posloupnost znaků**, kterou mu umožní přístup do chráněné oblasti.



Autentizace heslem 2/2

- Výhody hesel jsou snadný způsob realizace a nízká cena pořízení. Velká řada nevýhod ovšem použití hesel omezuje na **systémy s nízkým stupněm zabezpečení**. Mezi největší nevýhody patří možnost dekódování speciálními programy, zapomenutí nebo vysledování neoprávněnou osobou.
- Bezpečnost lze v omezené míře zvýšit používáním vhodných zásad, jako je složení z malých i velkých písmen nebo speciálních znaků, dostatečná délka, neobvyklost slova nebo fráze a nesouvislost s osobou vlastníka. Zároveň musí být měněno v pravidelných intervalech, nesmí být nikde poznamenáváno a musí být distribuováno zabezpečeným způsobem.

Autentizace předmětem 1/2

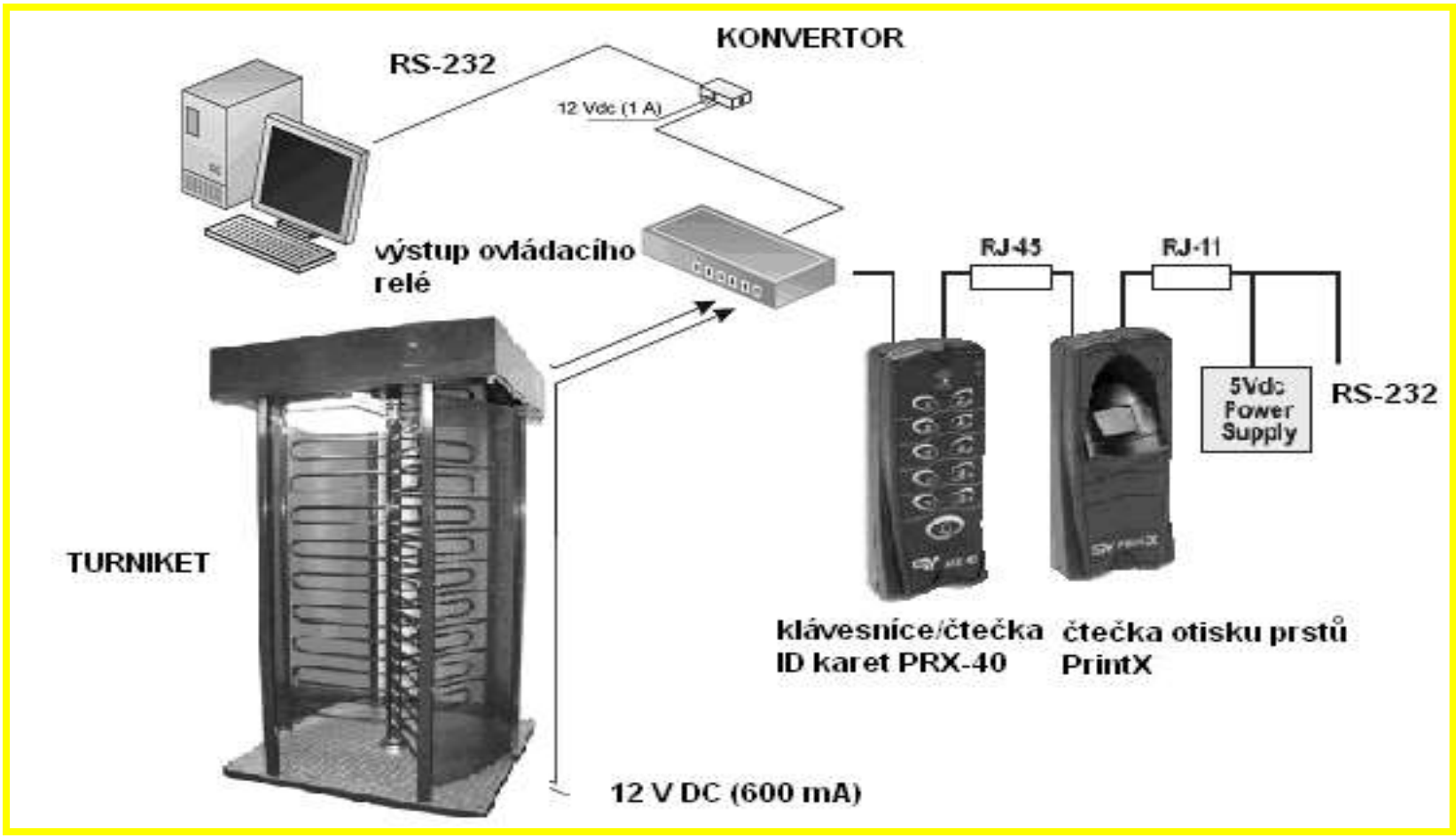
- Bezpečnost tohoto principu je zaručena **vlastnictvím speciálního předmětu** – **tokenu**, který je pro přístup do systému vyžadován.
- **Token** je jedinečný předmět, co možná nejhůře kopírovatelný, vybavený informací nutnou pro autentizační protokol, čímž se ověří identita uživatele. Výhodou a zároveň nevýhodou tokenu je jeho přenositelnost, proto by měl být token vždy používán jen v kombinaci s heslem anebo jako nositel biometrického vzorku uživatele.

Autentizace předmětem 2/2

- V praxi používanými tokeny jsou:
- **tokeny pouze s pamětí** (magnetické, elektronické nebo optické karty) jako obdoba mechanického klíče
- **tokeny s heslem** – vyžadují zadání hesla zároveň s použitím, např. platební karty
- **logické tokeny** – dokáží zpracovávat jednoduché podněty, např. vydej klíč/cyklickou sekvenci klíčů
- **inteligentní token** – mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, mohou umět šifrovat a generovat náhodná čísla

Kontrola oprávnění osoby

Nejvhodnější kombinace uvedených metod.



Výhody biometrické autentizace

- **vysoký stupeň spolehlivosti** (osvědčené technologie lze jen obtížně oklamat)
- **nulové provozní náklady** (žádná režie spojená s procesem autentizace)
- **rychlost, praktičnost** (není co ztrácet ani přenášet)
- **zřejmost** (výsledek je jednoznačný a okamžitý)
- **efektivnost** (přímé datové propojení s databází a počítači)
- **cena** (příznivá ve vztahu k bezpečnosti a v poměru cena/výkon, neexistující dodatečné náklady)

Biometrické systémy

Fáze zařazení uživatele do systému – ***enrollment***

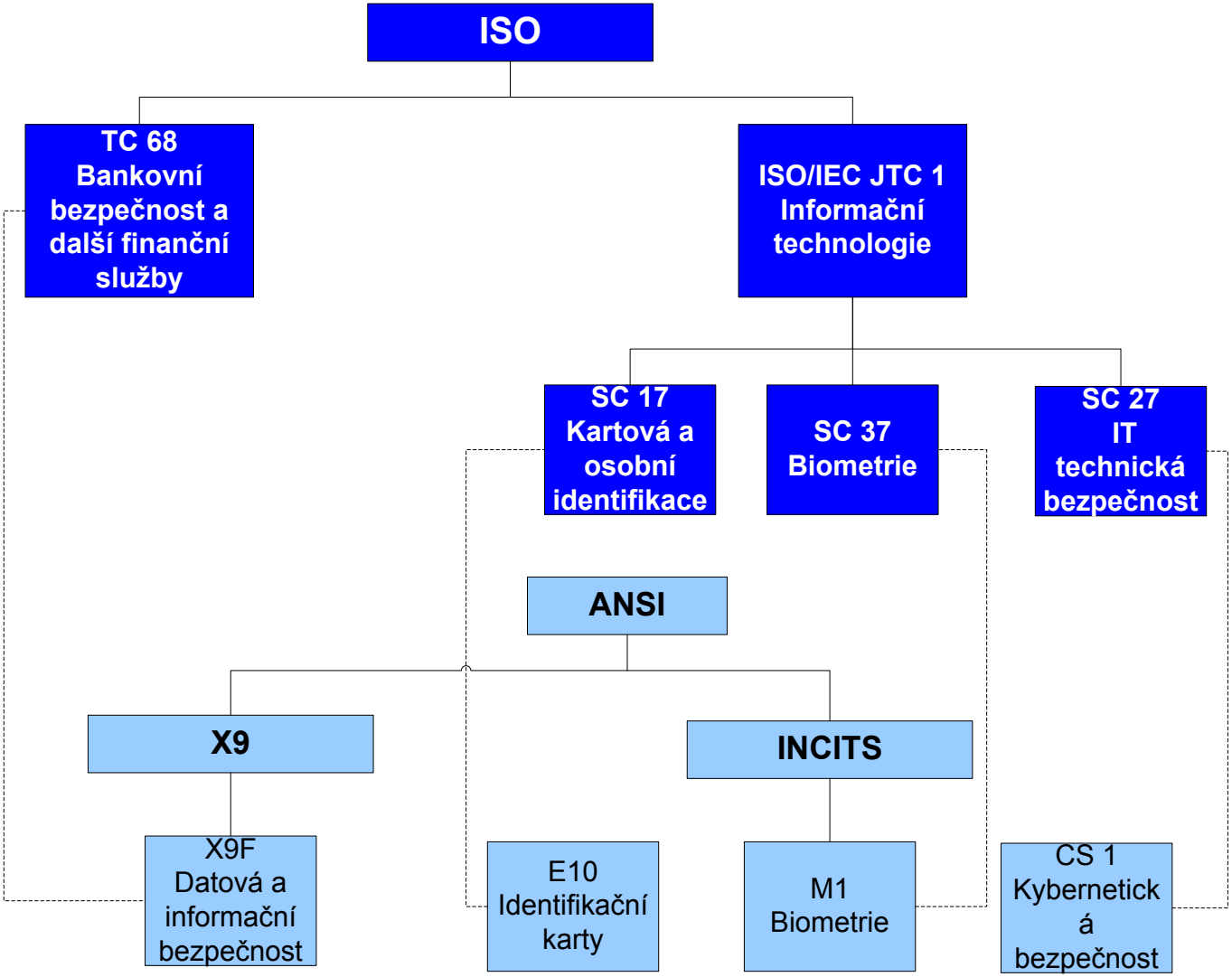
- sejmutí potřebných charakteristik a vytvoření referenčního profilu (vzorku)
- zpracování měření, vytvoření šablony (template)
- uložení šablony do identifikační databáze ve vazbě na určitý identifikátor

Biometrické systémy

Fáze ověření totožnosti – ***identification***

- aktuální snímání daných charakteristik
- zpracování výsledků
- vyhledání šablony v databázi podle ID přiřazenému danému uživateli a její porovnání s aktuálním měřením
- zaznamenání výsledku a následná verifikace nebo odmítnutí

Subordinace a spolupráce orgánů při tvorbě technických norem



Měření výkonnosti biometrických systémů 1/6

- Efektivnost biometrických rozpoznávacích systémů lze měřit mnoha statistickými koeficienty.
- Charakteristickými výkonnostními mírami jsou:
  - koeficient nesprávného přijetí
  - koeficient nesprávného odmítnutí
  - koeficient vyrovnané chyby
  - doba zápisu etalonu
  - doba ověření.
- Takových koeficientů existuje ovšem celá řada v závislosti na hloubce zkoumání problému.

Měření výkonnosti biometrických systémů 2/6

Efektivnost biometrických systémů lze měřit statistickými koeficienty. Charakteristickými výkonnostními mírami jsou :

Koeficient nesprávného přijetí, False Acceptance Rate (FAR).
Koeficient udává ***index míry bezpečnosti toho, že neoprávněná osoba je přijata jako oprávněná.***

$$FAR = (N_{FA}/N_{IIA}) \times 100\ [\%]$$

Měření výkonnosti biometrických systémů 3/6

Koeficient nesprávného odmítnutí, False Rejection Rate (FRR).
Koeficient udává ***index míry toho, že oprávněný uživatel je systémem odmítnut.***

$$FRR = (N_{FR}/N_{EIA}) \times 100\ [\%]$$

Chyby FRR a FAR jsou vyjádřeny v procentech, nebo poměrem. Např. FAR 0,001% odpovídá poměru 1: 100 000. V tomto případě to znamená, že jeden ze sto tisíc neoprávněných pokusů může být připuštěn do systému.

Měření výkonnosti biometrických systémů 4/6

- Udává ***poměr osob, u kterých selhal proces sejmutí vlastnosti***.
- Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti, která se snímá.
- Lze poté určit i tzn. osobní FER (Personál FER) udávající vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání.
- V případě, že byla uživateli správně sejmuta biometrická vlastnost, avšak systém ho chybně odmítl i po mnoha identifikačních/verifikačních pokusech, mluvíme o tzv. Koeficientu selhání přístupu, Failure To Acquire (FTA).

Měření výkonnosti biometrických systémů 5/6

- Abychom získali spolehlivé statistické údaje, je nutno provést velké množství pokusů o sejmutí biometrické vlastnosti. Pravděpodobnost neúspěchu sejmutí vlastnosti konkrétní osoby se vypočte podle vzorce:

$$FER(n) = \frac{počočneúspesnych\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n}{celkovy\ pocet\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n}$$

- Čím více pokusů provedeme, tím lepší hodnoty nám vycházejí. Celkové FER pro N účastníků (uživatelů) je definován jako průměr z FER(n) podle vzorce:

$$FER = \frac{1}{N} \cdot \sum_{n=1}^{N} FER(n)$$

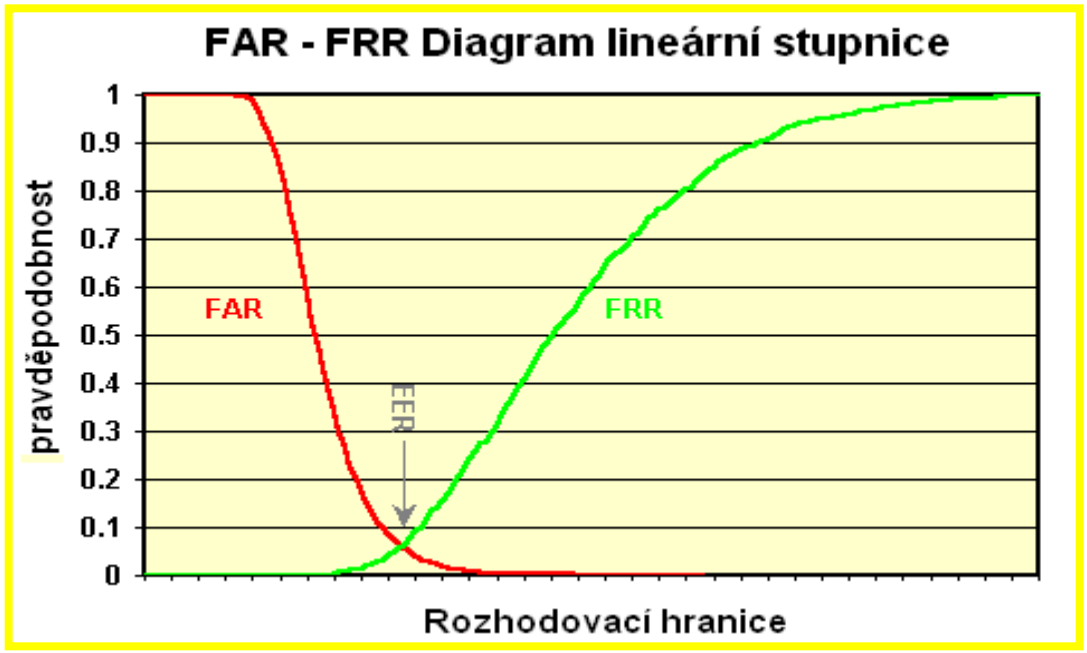
- Čím více uživatelů se bude započítávat, tím přesnější hodnoty nám budou vycházet.

Měření výkonnosti biometrických systémů 6/6

- Koeficient FIR udává ***pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně přiřazena k některému referenčnímu vzorku***.
- Koeficient FMR udává ***poměr neoprávněných osob, které jsou nesprávně rozpoznány jako akreditované během srovnávacího procesu.***
- Koeficient FNMR udává **poměr toho, že oprávněné osoby jsou nesprávně nerozpoznány během srovnávacího procesu**. V porovnání s FRR se liší v tom, že se nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu.

Koeficient vyrovnané chyby, Equal error rate (EER). Křížový koeficient je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR.

Biometrická charakteristika	FAR	FRR	Doba sejmutí a ověření
Otisk prstů	0,000 1 – 0,000 01 %	< 1,0 %	0,2 – 1 s
Geometrie ruky	0.1 %	0,1 %	1 – 2 s
Geometrie tváře	0,1 %	< 1,0 %	3 s
Obraz sítnice	0,001 %	0,4 %	1,5 – 4 s
Obraz duvovky	0.000 78 %	0,000 66 %	2 s
Charakteristika hlasu	Neuvádí se	Neuvádí se	1,5 s



FAR
pravděpodobnost, s jakou bude neoprávněný jedinec verifikován a autorizován k určitým činnostem,

FRR
pravděpodobnost, s jakou nebude oprávněný jedinec verifikován a autorizován k určitým činnostem

DIAGRAM CHYBY

Zvyšování bezpečnosti biometrických systémů 1/2

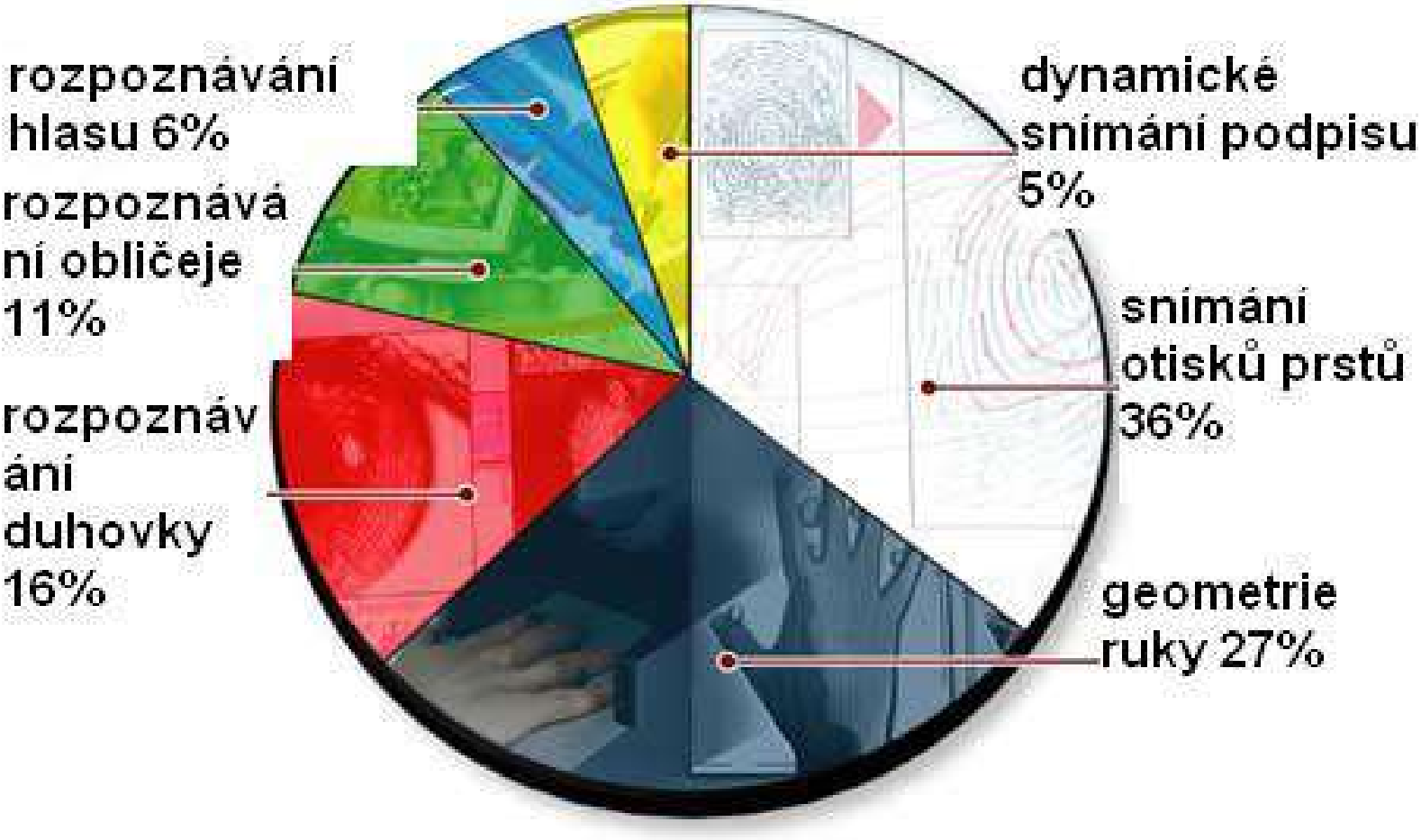
- Důvodem zvyšování bezpečnosti biometrických systémů, je přes jedinečnost biometrických znaků to, že reálné biometrické aplikace pracují s určitou chybovostí a to ve všech aplikacích nevyhovuje.
- Dále je zaznamenáno, že pachatelé trestných činů kromě klasické přístupových systémů (karta, PIN…), začínají napadat i biometrické aplikace.
- Objevují se pokusy o změny otisků prstů, odlívání otisků prstů do silikonu, plastické operace (změny v obličeji), což je nebezpečné pro bezpečnostní aplikace typu forenzní identifikace, tak i pro přístupové systémy.

Zvyšování bezpečnosti biometrických systémů 2/2

- Jedním z možných způsobů jak bezpečnost zvýšit je **aplikace ezoterické identifikace**, protože skryté znaky je mnohem obtížnější změnit, dokonce v některých případech i nemožné změnit.
- Druhým z možných způsobů jak zvýšit bezpečnost biometrických aplikací je tzv. **Multiple Biometric**, tedy **vícenásobná biometrie**. Jde o kombinaci vice biometrických znaků v jednom systému (nejméně dvou).
- Nejčastěji používanou kombinací je identifikace podle otisků prstů, geometrie obličeje (2D, 3D), geometrie oční duhovky nebo sítnice a identifikace podle hlasu. Lze očekávat, že v brzké době přibudou i kombinace jiných znaků.

Jednotlivé biometrické technologie

- V bezpečnostní praxi je využíváno mnoho metod k individuální identifikaci osob



Biometrické systémy řízení a kontroly vstupů 1/3

- Systémy kontroly a řízení vstupů v bezpečnostních aplikacích (ACS – Access Control Systems) hlídají vstup do chráněných prostor a vstup do těchto prostor umožňují pouze uživateli, který se prokazuje nějakou metodou autentizace. ACS systémy spadají pod normu **ČSN EN 50133.**
- Verifikace značí ověřovací proces v systému ACS, který vždy vyžaduje přihlášení uživatele do systému, kde je poté provedeno porovnání neskenovaného záznamu se záznamem v databázi.
- **Je důležité omezit počet možných přihlašovacích pokusů, než bude uživatel systémem definitivně odmítnut jako nepovolaná osoba**. Pro daný počet přihlašovacích pokusů je nutné vzít v úvahu úroveň zabezpečení systému.

Biometrické systémy řízení a kontroly vstupů 2/3

- Čím menší počet pokusů je zvolen, tím s větší pravděpodobností vyvoláme několik falešných poplachů kvůli neprovedené identifikaci oprávněného uživatele.
- Na druhou stranu, je ale nutné zvolit takový počet pokusů, aby neoprávněný uživatel neměl čas získat dostatek informací o systému, které by mu později pomohly systém prolomit.
- U vysoce zabezpečených systémů by měly být výsledky verifikace pro pozdější zpracování ukládány.
- Nabízí se tři možnosti ukládání:
  - přímo do zařízení (do hlavní jednotky snímače)
  - do vzdáleného počítače
  - přímo do tokenu pokud je použit.

Biometrické systémy řízení a kontroly vstupů 3/3

- Ukládání přímo do **snímače** je nevýhodné vzhledem k omezené paměti jednotky a ke snadnějšímu přístupu k uloženým datům pro narušitele.
- Při plné paměti by starší záznamy byly přepsány novějšími.
- Při ukládání do **vzdáleného počítače** není proces omezen velikostí paměti, ale existuje určité nebezpečí průniku do systému zvnějšku, čili je nutné tuto komunikaci i samotnou databázi dále zabezpečit.
- Třetí způsob, ukládání dat do **tokenu**, je nevýhodný z hlediska nutnosti složitější elektroniky a rozhraní pro token, tedy z hlediska ceny řešení a stupně zabezpečení.

Princip biometrických systémů řízení a kontroly vstupů 1/3

- Předpokladem pro provedení biometrické autentifikace je sejmutí a zápis biometrické vlastnosti osoby, která je dále uložena jako osobní referenční šablona buď decentralizovaně na čip ID karty nebo počítače, nebo centrálně do datové paměti systému nebo aplikace.
- Je nutné provádět snímání a zápis opatrně, jelikož kvalita pořízeného obrazu má zásadní vliv na proces autentifikace. Je zřejmé, že proces snímání musí být prováděn v důvěryhodném prostředí.

Princip biometrických systémů řízení a kontroly vstupů 2/3

- Většina biometrických systémů pracuje s následujícím postupem:

1. **Pořízení datového souboru** (obraz, zvuk, atd.), který obsahuje biometrickou vlastnost, která z něj jde vyextrahovat použitím vhodného snímače (senzoru).
2. **Prověření kvality dat:** pokud jejich kvalita nevyhovuje, jsou okamžitě odmítnuta nebo je uživateli poskytnuta vhodná rada pro zvýšení kvality sejmuté biometrické vlastnosti (např. upozornění na směr snímání, polohu části těla atd.)

Princip biometrických systémů řízení a kontroly vstupů 3/3

3. **Vyextrahování** požadované biometrické veličiny z datového souboru **a vytvoření šablony vzorku**
4. **Zápis**: uložení šablony jako referenční šablony do archívu referenčních šablon systému či aplikace (dle definování místa ukládání)
5. **Ověřování**: porovnání aktuální (vyžadované) šablony s referenční šablonou užitím algoritmu pro určení shody a vygenerování hodnoty (skóre), která je rozhodná pro determinování stupně shody **Výsledek ověřování**: pokud skóre shody překročí předdefinovanou hranici, tak je přístup umožněn, v opačném případě je žádost odmítnuta.

Biometrické informace používané pro identifikaci 1/4

- Kritéria pro výběr biologické nebo behaviorální vlastnosti člověka určené pro jeho další identifikaci jsou determinována co nejširším a nejefektivnějším způsobem užití.
- Takto vhodná vlastnost člověka musí splňovat:
  - **jedinečnost**: vlastnost musí být co možná nejvíc výjimečná, tzn. že se shodná vlastnost nesmí objevit u dvou lidí zároveň
  - **univerzálnost**: vlastnost musí být měřitelná u co možná největší množiny lidí
  - **trvalost**: vlastnost se nesmí měnit v čase
  - **měřitelnost**: vlastnosti musí být měřitelné shodnými technickými zařízeními
  - **uživatelská přijatelnost**: vlastnost musí být snadno a pohodlně měřitelná

Biometrické informace používané pro identifikaci 2/4

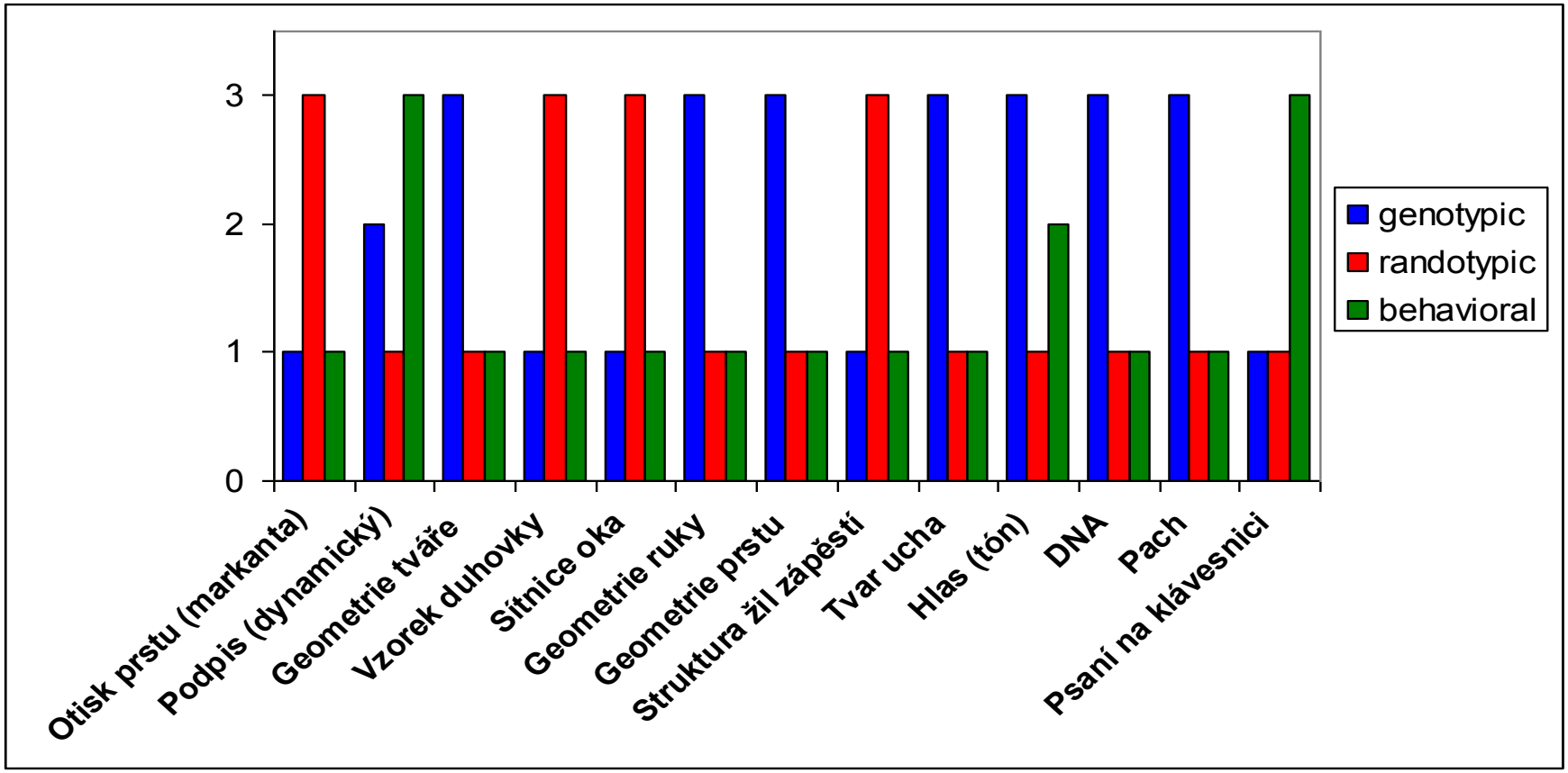
- Nejlépe prozkoumané a nejvíce rozšířené biometrické vlastnosti používané pro identifikační účely jsou uvedeny níže spolu se stručným popisem toho, co se měří:
  - otisk prstu (struktura papilárních linií a jejich detailů) dynamika podpisu (rozdíly v tlaku a rychlosti psaní)
  - geometrie tváře (vzdálenosti specifických částí – oči, nos, ústa…)
  - duhovka oka (obrazový vzorec duhovky)
  - sítnice oka (struktura žil na očním pozadí)
  - geometrie ruky (rozměry dlaně a prstů)
  - struktura žil na zápěstí (struktura žil)
  - tvar ucha (rozměry viditelné části ucha)
  - hlas (tón a zabarvení hlasu)

Biometrické informace používané pro identifikaci 3/4

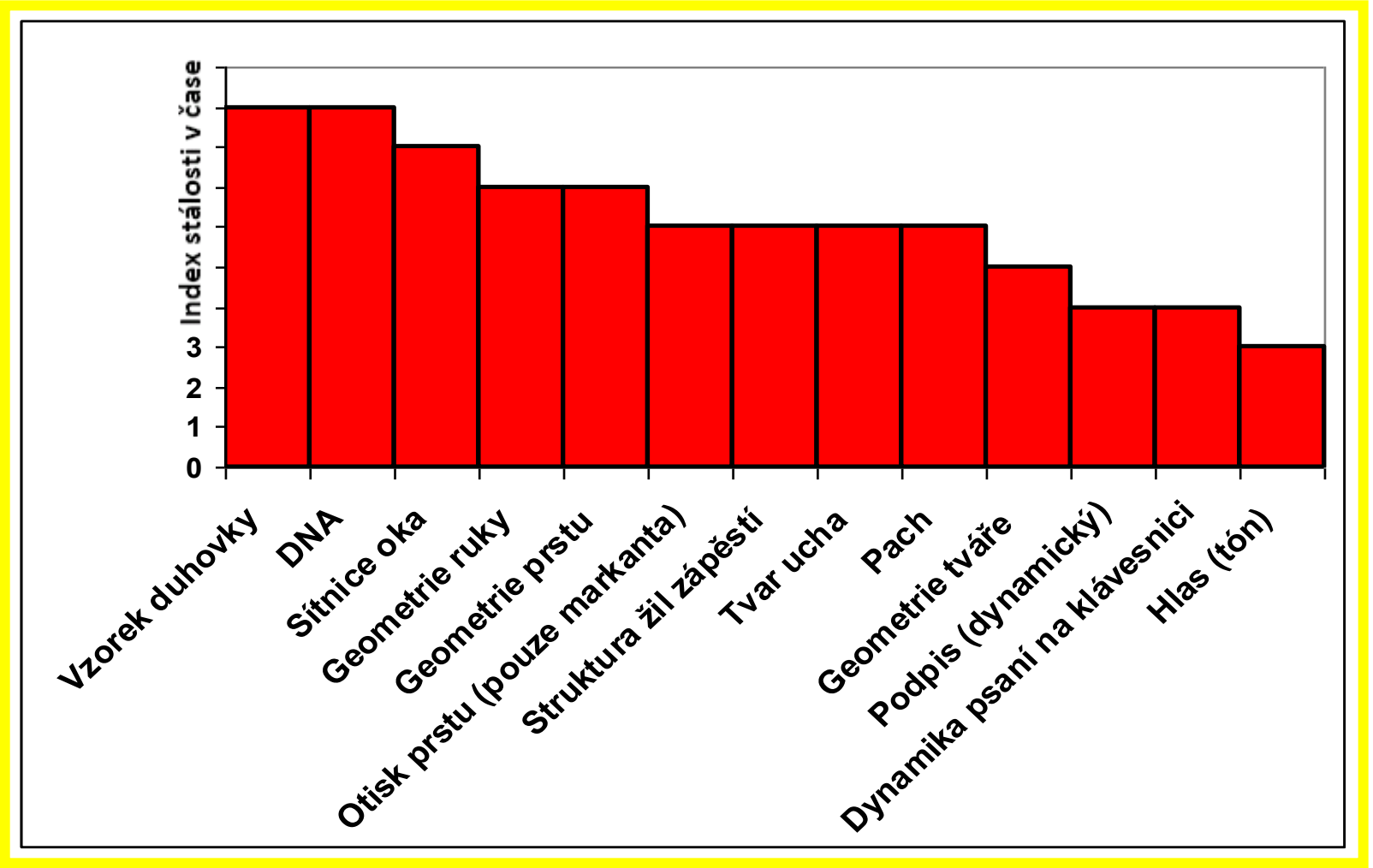
- DNA (řetězec deoxyribonukleové kyseliny)¨
- pach (chemické složení)
- psaní na klávesnici (rytmus úderů do klávesnice PC)

- Způsoby, kterými biometrické vlastnosti člověka vznikají, jsou v základě tři:
  - **skrze genetický vývoj**: uplatňuje se vliv dědičnosti (DNA) – genotypické
  - **skrze náhodné varianty vzniku v časném stádiu vývoje embrya** – randotypické
  - **skrze učení a výchovu**: chování jedince – behaviorální

Biometrické informace používané pro identifikaci 4/4



Stálost biometrické vlastnosti v čase



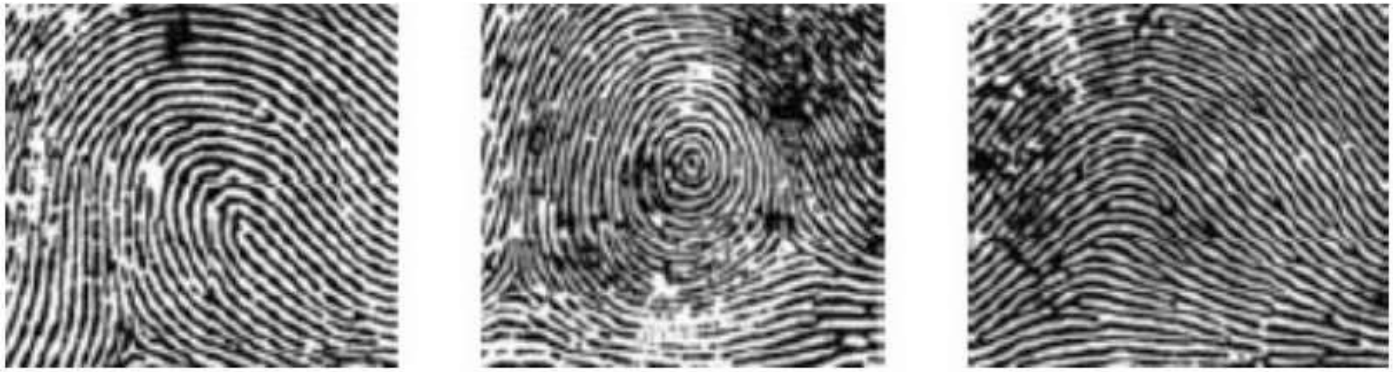
Výhody jednotlivých biometrických metod

Biometrická vlastnost	Index komfortu	Index přesnost	Index dostupnosti	Index ceny
Otisk prstů	7	7	4	3
Dynamika podpisu	3	4	5	4
Geometrie tváře	9	4	7	5
Vzorek duhovky	8	9	8	8
Sítnice oka	6	8	5	7
Geometrie ruky	6	5	6	5
Geometrie prstu	7	3	7	4
Struktura žil zápěstí	6	6	6	5
Tvar ucha	5	4	7	5
Hlas, akustická křivka	4	3	3	2
DNA	1	7	9	9
Pach, struktura	?	2	7	?
Dynamika psaní na klávesnici	4	1	2	1
Srovnání: heslo	5	2	8	1

- V poměru cena a přesnost vychází nejlépe otisk prstu.
- Duhovka oka má vysoké hodnocení v případě, že cena nehraje roli.
- DNA ztrácí v komfortu snímání, je zdlouhavá (jednovaječná dvojčata jí mají shodnou).

Multiple Biometric ⇨ Otisk prstu + další metody

Teorie snímání otisku prstů 1/2



Vzory útvarů tvořených papilárními liniemi

Papilární linie – plastické rýhy, které vystupují napovrch pokožky. Jejich výška je 0,1-0,4mm a šířka cca 0,2-0,7mm. Dohromady vytváří různé tvary - dělíme na **smyčky, víry a oblouky**.

Markanty - charakteristické znaky nepravidelnosti papilárních linií,které vytvářejí obraz (V České republice – **10 stejně umístěných a orientovaných markantů**, aby byly považovány za shodné)

Teorie snímání otisku prstů 2/2

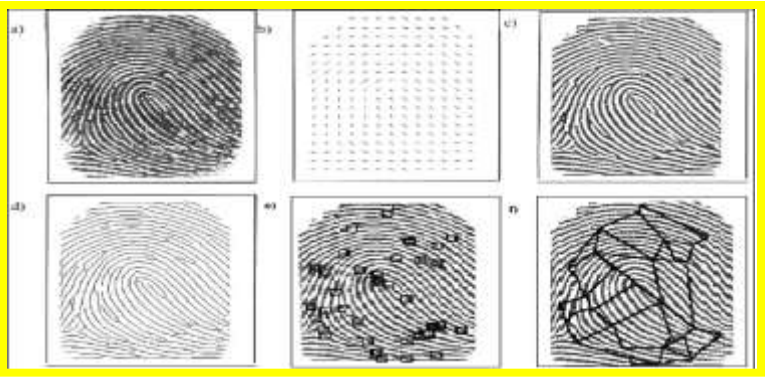
	ukončení		most
	vidlice		Dvojitá vidlice
	bod		Trojitá vidlice
	ostrůvek		Naproti umístěné vidlice
	oko		zkřížení
	háček		Ukončení vidlice

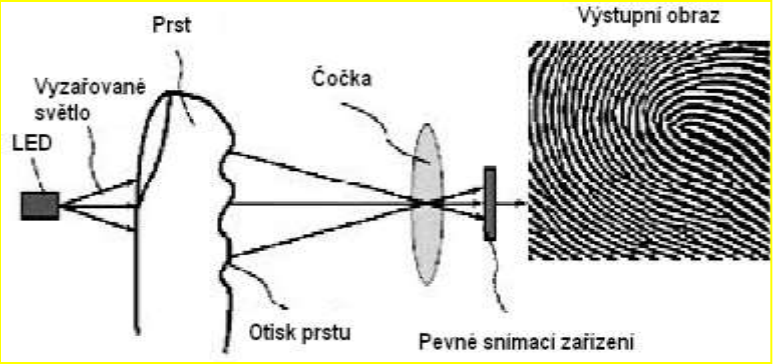
Charakteristické znaky nepravidelnosti papilárních linií

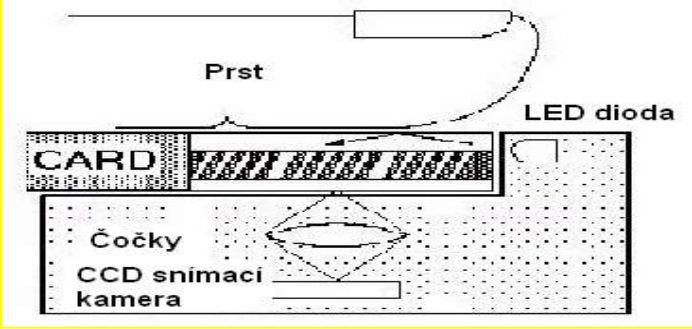
Otisk prstu s nalezenými markanty

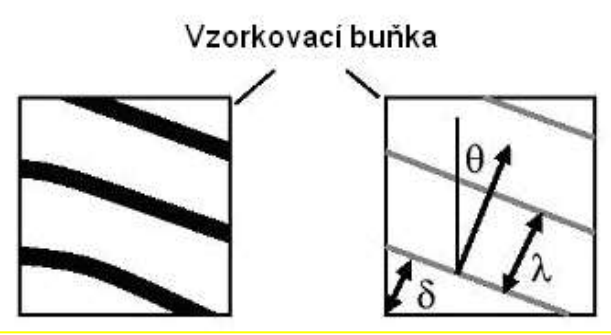
Metody zachycení otisku prstů

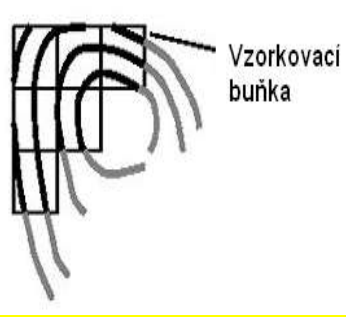
- Otisk získaný pomocí inkoustu a papíru
- Statické snímání
- Snímání šablonováním











Otisk získaný pomocí inkoustu a papíru

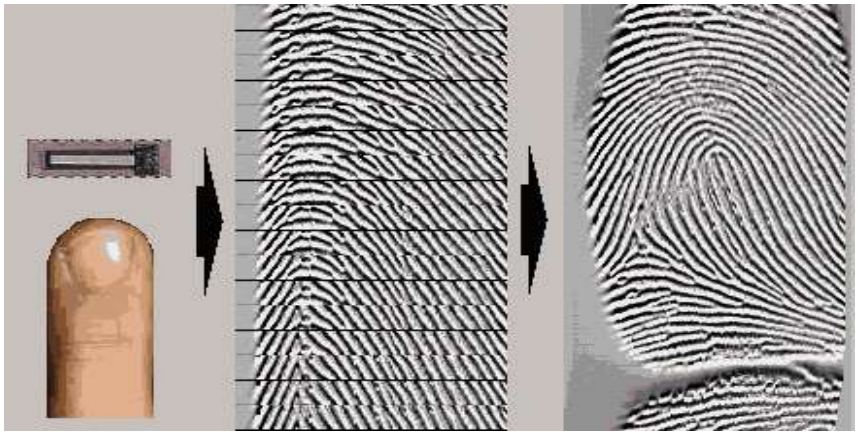
- Klasická metoda (rolled finger)
- Používá se **pouze ve forenzní sféře**, policií při vyšetřování
- Prst se po papíře roluje, aby se získal otisk celého prstu (prakticky od nehtu po nehet) s co možná nejvíce použitelnými markantami a aby se tím zvýšila i rychlost rozpoznání otisku

Statické snímání

- **Nejběžnější používaná metoda** snímání otisku prstu
- Uživatel přitiskne svůj prst na senzor bez jakéhokoliv pohybování s ním
- **Výhodou:** jednoduché ovládání (stačí pouze přiložit prst)
- **Nevýhodou:** přehnanou silou tlačení prstu může uživatel rozlomit snímací čočku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky

Snímání šablonováním

- Uživatel **přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů**
- **Výhodou:** snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor; na snímači nezůstávají skryté (latentní) staré otisky; uživatel nemá pocit zanechaného otisku prstu a snímání je rychlé
- **Nevýhodou:** obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup



Senzory snímání otisku prstů

Kontaktní

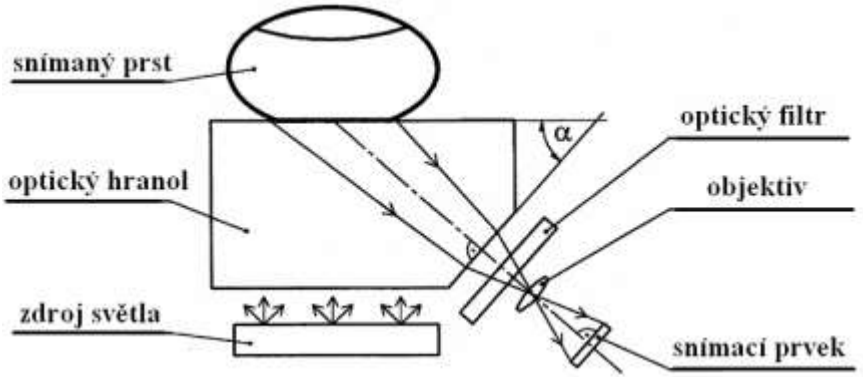
- Optoelektrické
- Transmisní optické snímače
- Elektroluminiscenční senzory
- Kapacitní senzory
- Teplotní senzory
- Tlakové senzory

Bezkontaktní

- Optické senzory
- Ultrazvukové senzory

Optoelektrické snímače

- **Osvětlují přiložený prst laserovým světlem**
- Dochází ke **zkoumání rozptylu nebo odrazu světla** v místech, kde se papilární linie přiloženého prstu stýkají se snímací plochou
- Světlo, které dopadne na papilární linii, je odraženo zpět, naopak světlo dopadající do rýhy prstu se neodráží



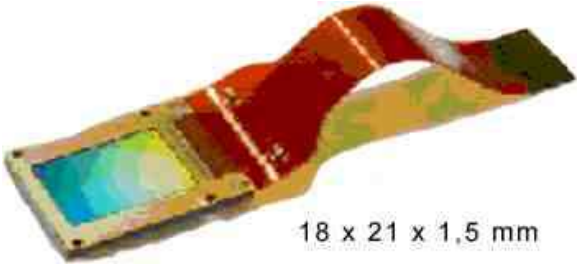
Kapacitní (silikonové) snímače 1/2

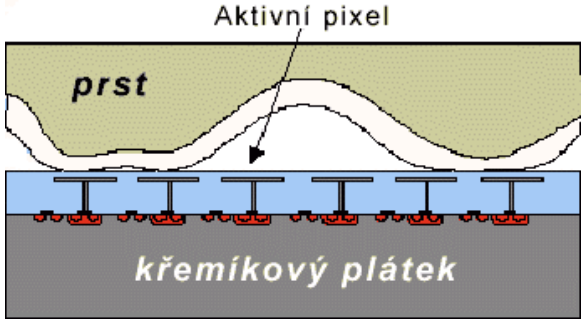
- **Měří kapacitní odpor v ploše dotyku prstu se snímací podložkou**
- Přiložený prst funguje jako jedna deska kondenzátoru a podložka zastává druhou
- Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor
- **Rozdíly těchto hodnot se zachytí a podle nich se vytvoří obraz otisku prstu**

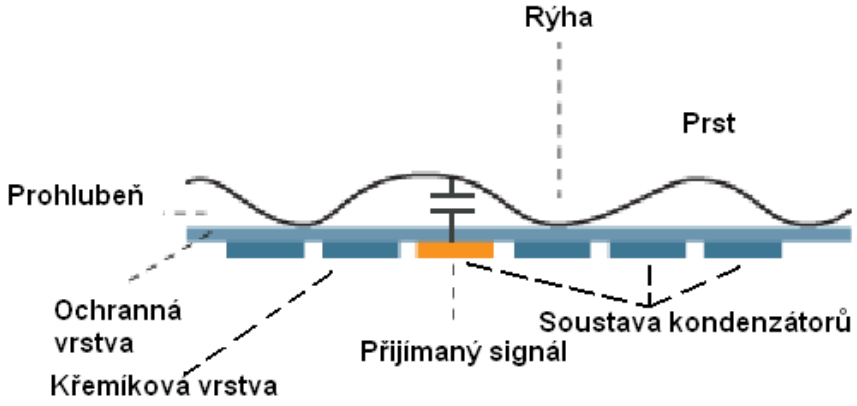
- *Mají menší rozměry než optické snímače*
- *Dokáží si ve větší míře úspěšně poradit s mírně zašpiněným prstem*

Kapacitní (silikonové) snímače 2/2

- Obraz otisků je získán z aktivních pixelů v digitální formě
- Pro získání obrazu stačí přiložit prst na citlivou plochu, která je osazena velkým množstvím mikroelektrod

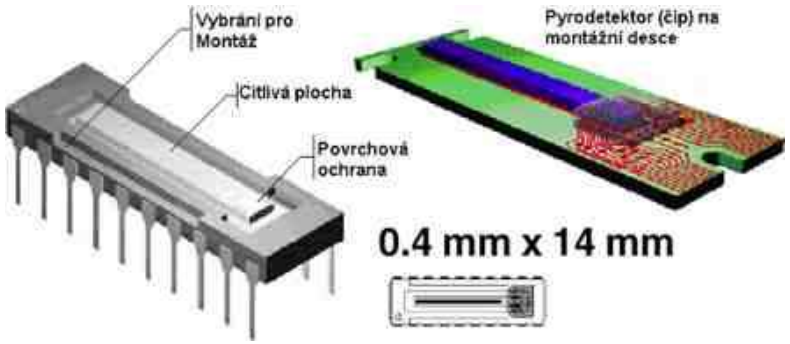


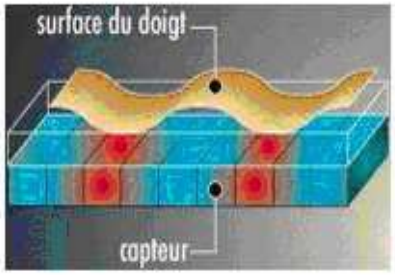


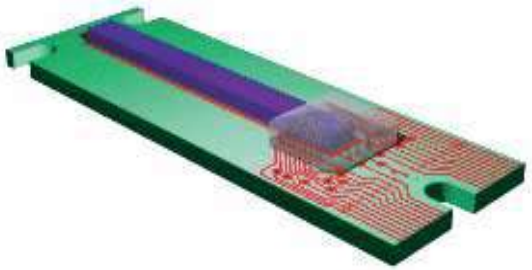


Teplotní snímače

- Jsou vybaveny miniaturním, velmi citlivým **pyrodetektorem** (čipem), který **snímá rozdíl teplot mezi papilárními liniemi**, které se dotýkají čipu a prostoru mezi liniemi, které se čipu nedotýkají
- Nízká kvalita získaných obrazů (činí problémy algoritmům rozpoznání na principu rozpoznávání podle identifikačních znaků (markant)

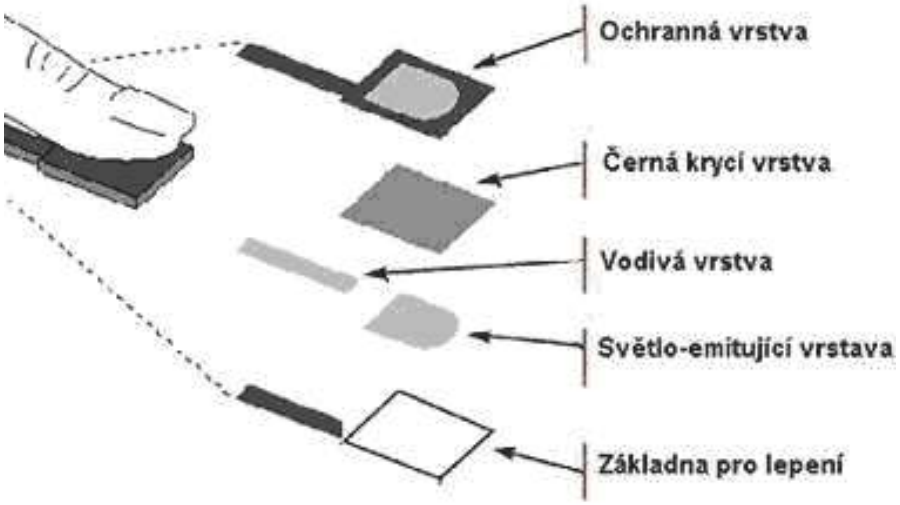




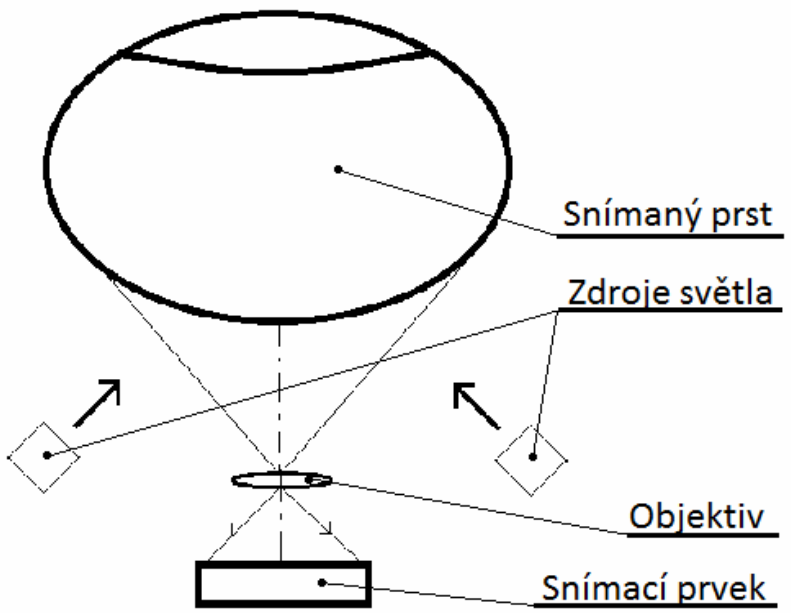


Elektroluminiscenční snímače

- snímací plocha je polymer skládající se z několika vrstev
- rozhodující vrstvou z hlediska funkce snímače je **světloemitující vrstva**, která při tlaku prstu emituje světlo v místech, kde na ní tlačí papilární linie po dotyku prstu



Bezkontaktní elektronické snímače otisku prstů

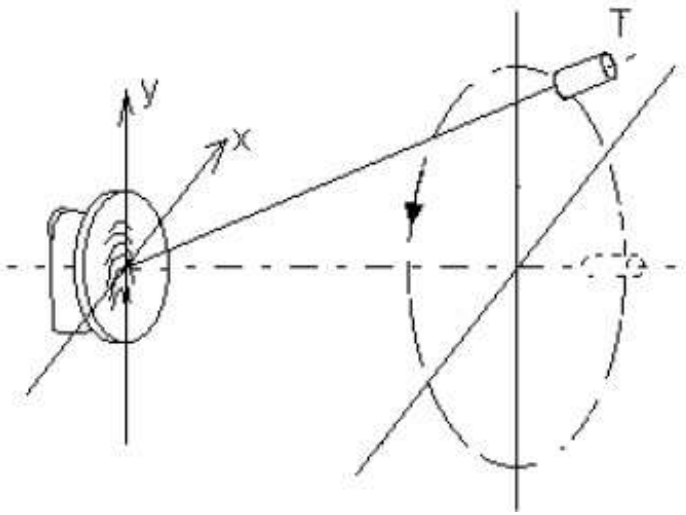


Optické bezkontaktní snímače a ukázka kvality výstupního obrazu

Ultrazvukové snímače 1/2

- **Patentovaná technologie** - vlastníkem společnost Ultrascan
- **Čtecí zařízení vysílá zvukové vlny**
- Následné měření odporu kůže a získání vzoru papilárních linií na snímaném prstu

- *Vysoká přesnost i při znečištění prstu*
- *Velké čtecí zařízení*



Ultrazvukové snímače 2/2

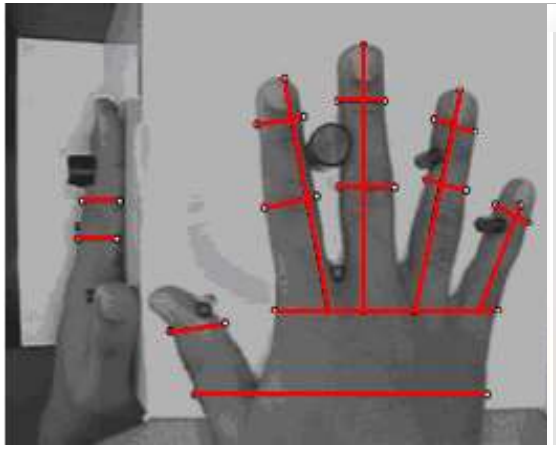
Čtecí ultrazvukové zařízení firmy Ultrascan a ukázka kvality získaného obrazu

Geometrické měření ruky 1/3

- **Nejstarším implementovaným biometrický principem**
- **Její aplikace v bezpečnostní sféře je omezena stupněm bezpečnosti**, kterého chceme dosáhnout
- Méně přesná, než předchozí metoda
- **Pouze verifikace**

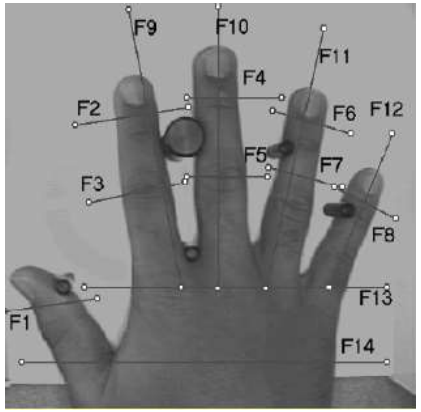
Geometrické měření ruky 2/3

- Zařízení pro rozeznávání geometrie ruky **využívají jednoduchého principu měření a** 3 dimensionálního (**3 D) snímání délky, šířky, tloušťky a povrchu ruky** (dlaně) konkrétního člověka umístěné na podložce s pěti polohovými kolíky pomocí CCD kamery



Geometrické měření ruky 3/3

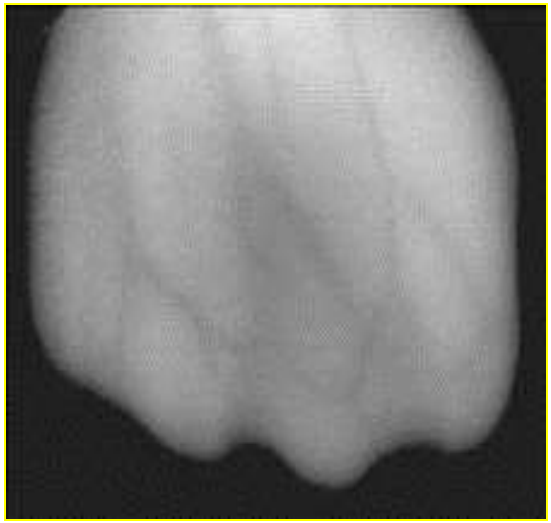
- Na obrazu ruky lze najít přes **31 tis. polohových bodů a provést 90 různých měření vzdáleností**

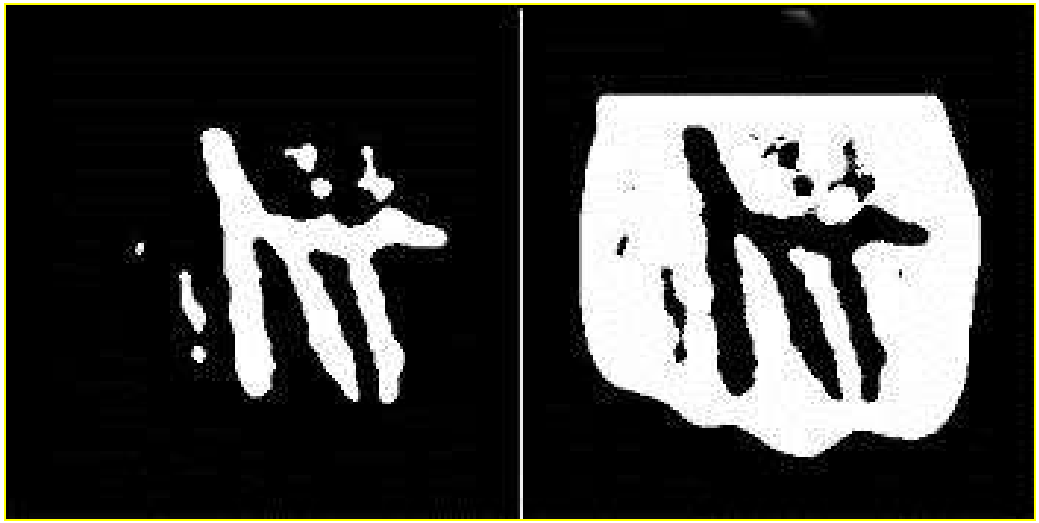


- Vybrané měřené informace se ukládají do 9 bitového souboru, což činí tyto systémy velice výhodné z hlediska **nízkého požadavku na paměť systému**
- Tyto systémy jsou používány v různorodých aplikacích docházkových systémů a přístupových systémech, kde jsou poměrně velmi rozšířené.

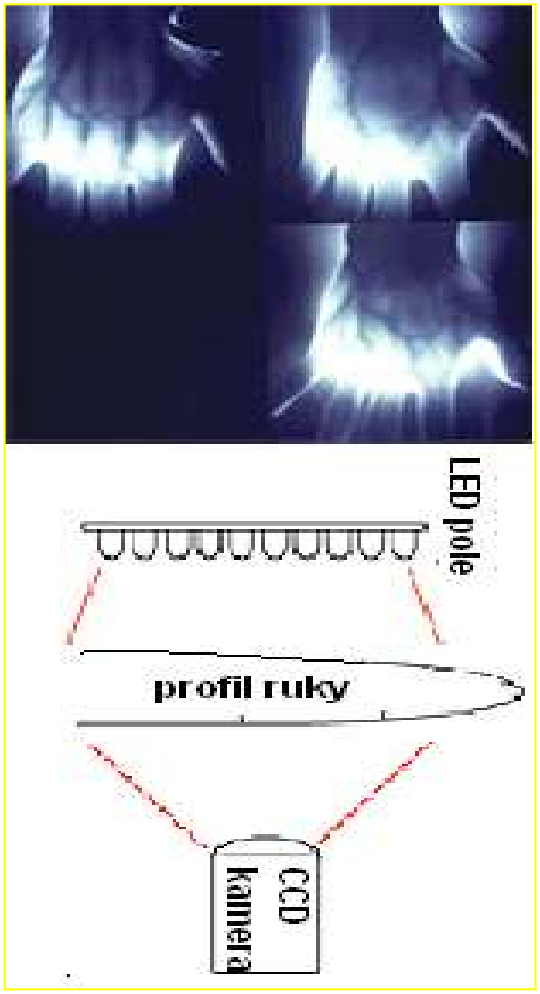
Krevní řečiště žil zápěstí 1/2

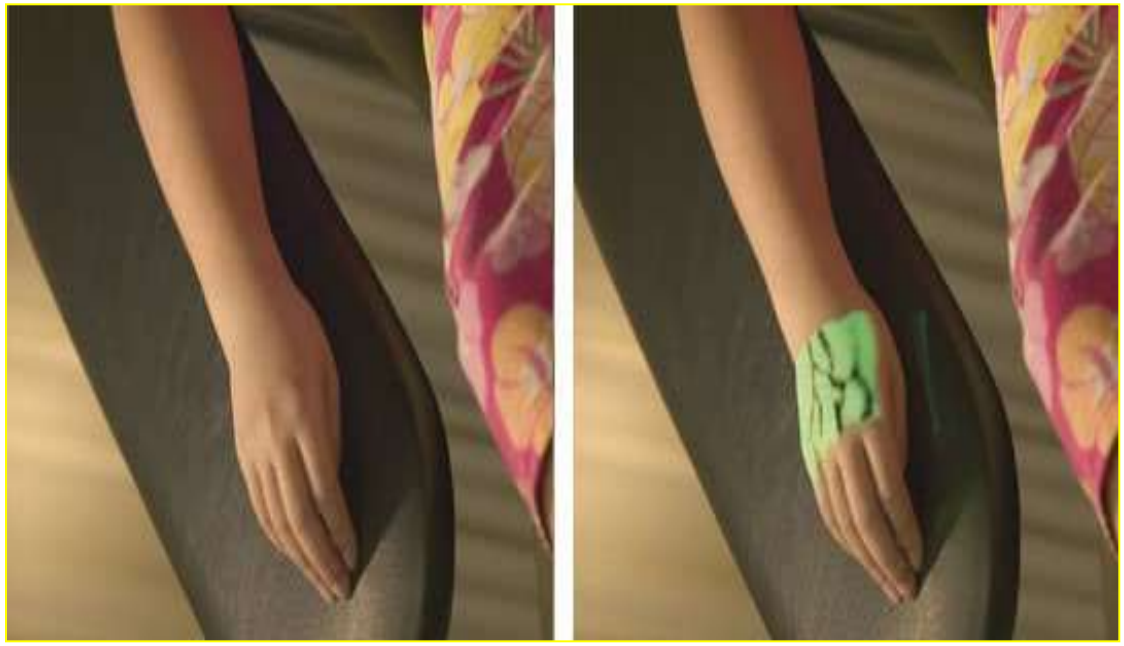
- Síť cév uvnitř ruky není bez prosvícení viditelná a snímání vyžaduje, aby byla ruka živá, tekla v ní teplá krev, obtížné napodobení





Krevní řečiště žil zápěstí 2/2





Rozpoznání obličeje 1/3

- **Srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi**
- K jednoznačné identifikaci slouží většinou tvar obličeje a poloha opticky významných míst na tváři (oči, nos, ústa,obočí)
- Obraz v počítači může být někdy uložen jako matice jasových úrovní, častěji je však diskriminován nějakou funkcí, která snižuje redundanci dat
- Neuchovává se tedy přesná poloha očí, nosu a rtů, ale **ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem**, atd.

Rozpoznání obličeje 2/3

Existují dva odlišné přístupy k rozpoznávání geometrie tváře:

- **geometrický** (založený na rysech tváře)
- **fotometrický** (založený na vzhledu obrazu tváře).

- Po zdokonalení systému rozpoznávání obličeje, by mohli odpadnout mnohé, méně efektivní systémy (např. docházkový systém do zaměstnání).

Je obrovský rozdíl v realizaci systémů, který porovnává dva statické obrazy a systému, který ověřuje totožnosti jednotlivce nacházejícího se ve skupině lidí

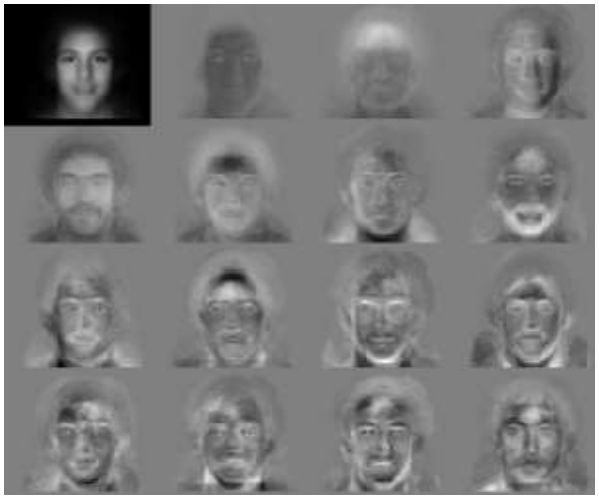
Rozpoznání obličeje 3/3

Tři nejlépe prozkoumané a studované algoritmy rozpoznávání tváře jsou:

- **Analýza hlavních částí** (**PCA** - Principal Components Analysis)
- **Lineární diskriminační analýza** (**LDA** - Linear Discriminant Analysis)
- **Elastický srovnávací diagram** (**EBGM** - Elastic bunch graph matching)

Analýza hlavních částí (PCA)

- **Využívá vektorů tváře odvozených s kovarianční matice** pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání
- Každá tvář lze rozdělit na tzv. **eigenfaces** (**vzory tváří** - matice jasových úrovní) a poté jde opět složit
- Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo

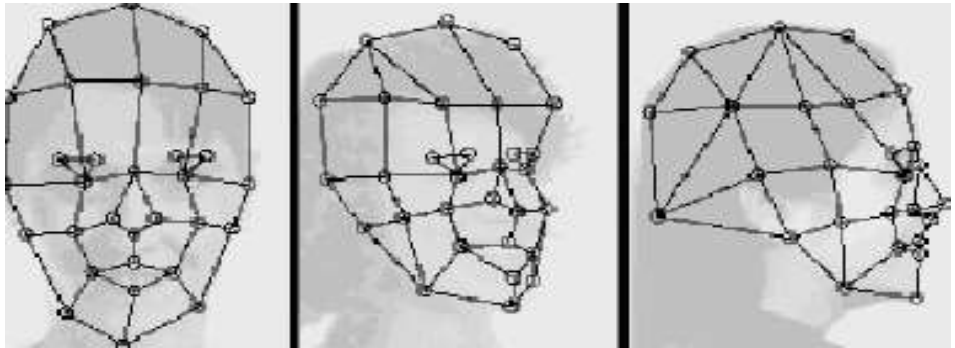


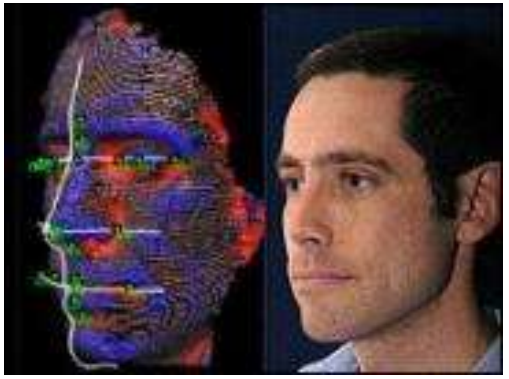
Lineární diskriminační analýza (LDA)

- Metoda, kdy se **třídí pořízené obrazy tváří do skupin**
- Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině, **každý blok snímků reprezentuje jednu třídu**

Elastický srovnávací diagram (EBGM)

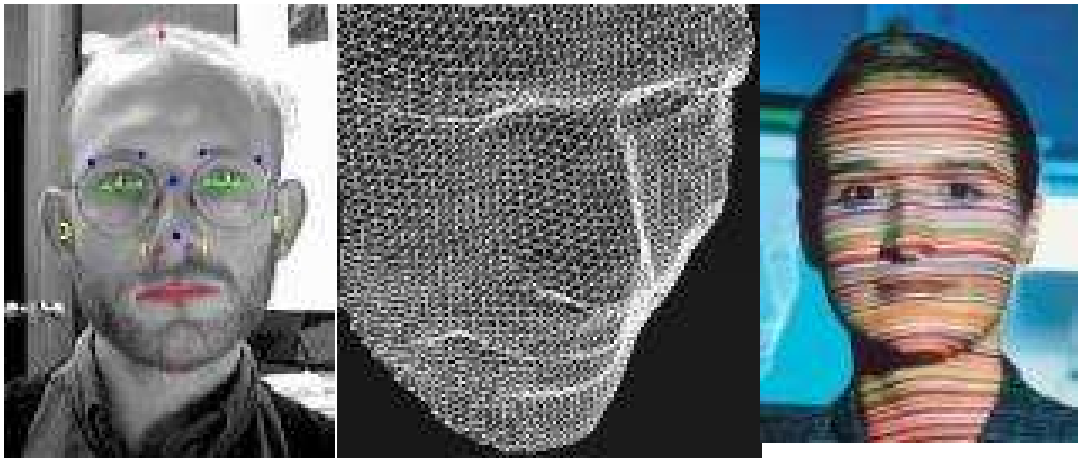
- Byla vyvinuta, jelikož předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení)
- **Na obličeji se definuji uzlové body, které se poté propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje**
- Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat





Rozpoznání obličeje

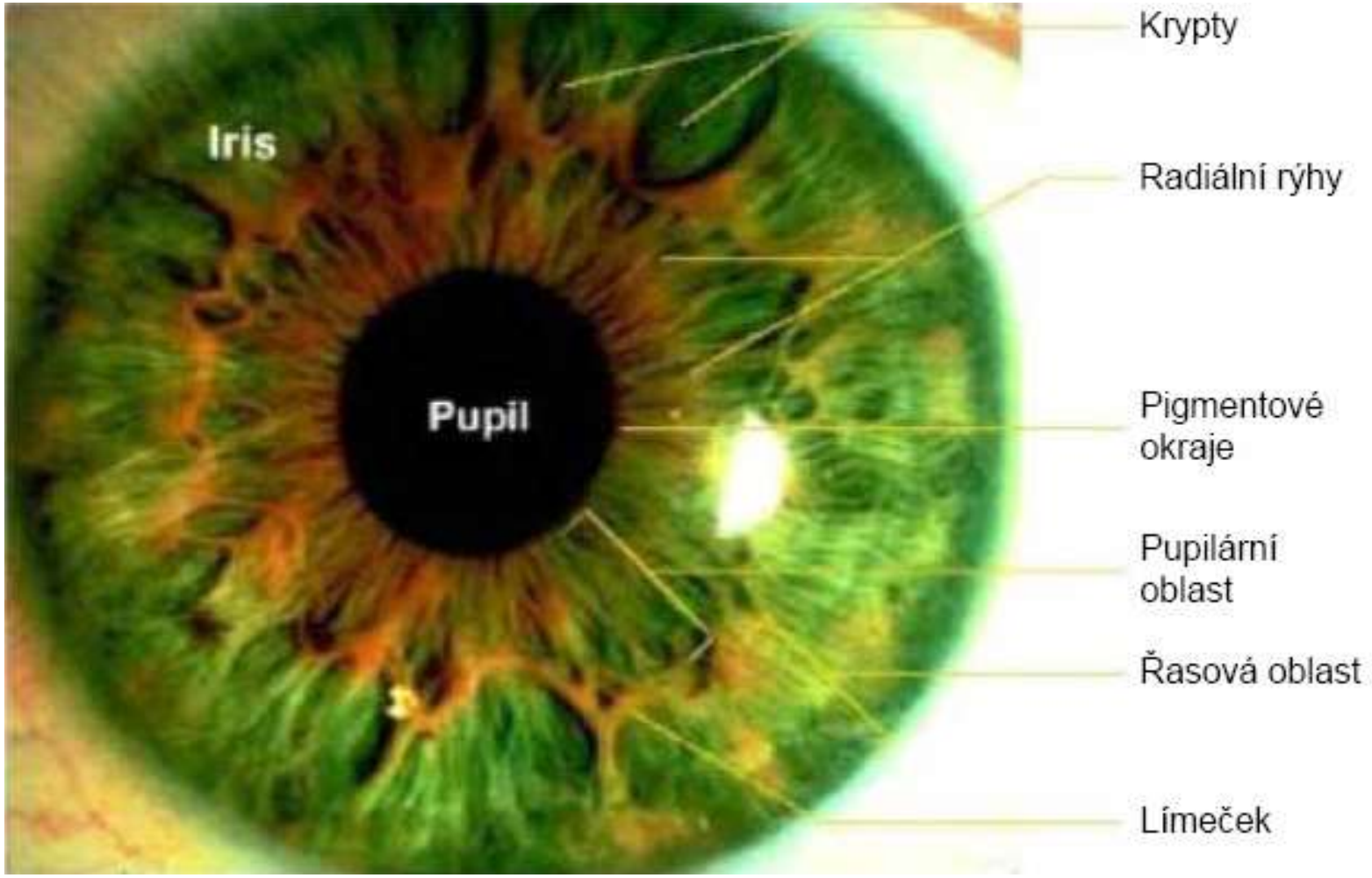
- Dochází k jejímu nasazování **na letištích, nádražích, rušných ulicích** a náměstích a všeobecně na místech, kde by se mohli pohybovat pohřešované a hledané osoby apod.



Nepřesnosti detekce tváře

- jestliže je **tvář osoby vyfotografována venku**, a to z úhlu 45°, typický automatizovaný systém **selhává v 80 % případů**
- **vliv má proměnlivost osvětlení**, **odlišností oblečení** (systém ve 40% případů nedokáže danou osobu identifikovat na základě uložené fotografie)
- **k prohledávání databází fotografií osob**, ale fotografie musejí obsahovat záběr celé tváře a musí být k dispozici dostatečné množství manuálních pracovníků, kteří budou schopni spojit fotografii hledaného jedince s fotografií v databázi

Oční duhovka 1/4

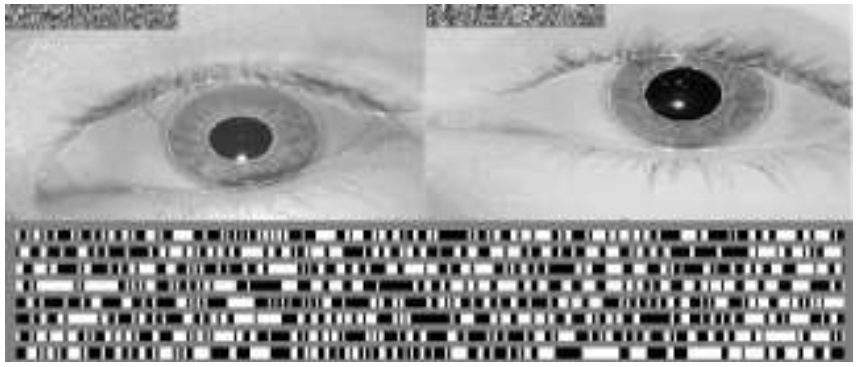


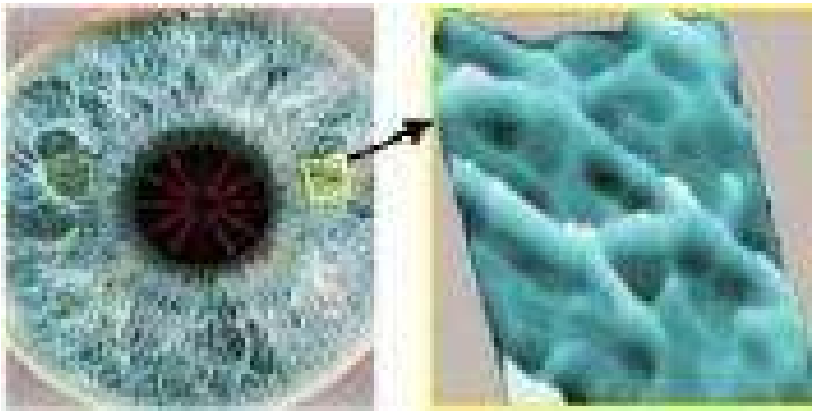
Oční duhovka 2/4

- Relativně nové vyvinuté (první patent roku 1994)
- Duhovka je **sval uvnitř oka**, který reguluje velikost čočky (tedy zaostření oka) na základě intenzity světla dopadajícího na oko.
- Duhovka je barevná část oka, jejíž zabarvení odpovídá množství meletoninového pigmentu uvnitř svaloviny
- Duhovka se vyvíjí během **prenatálního růstu plodu a její vzorkování je náhodné, tudíž jedinečné pro každého člověka** i dvojčata, dokonce i **jeden člověk má každou duhovku jinou**, což činí tyto systémy **nejpřesnějšími ze všech**

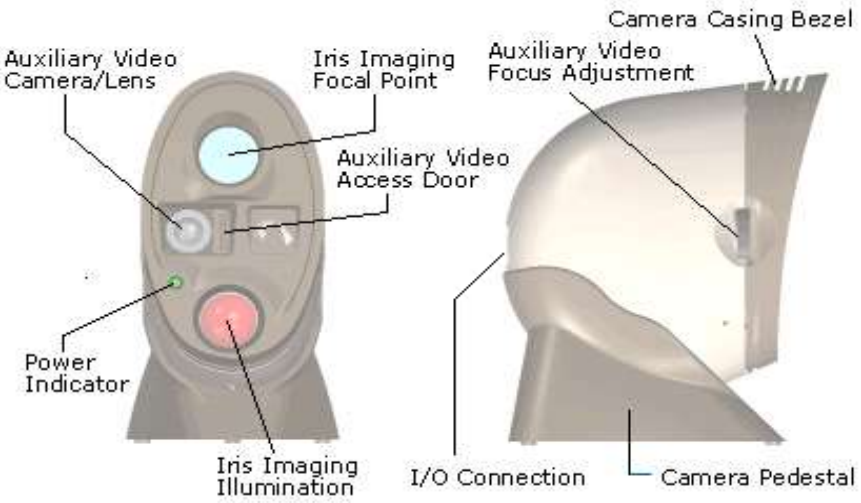
Oční duhovka 3/4

- Snímání duhovky vyžaduje kvalitní digitální kameru a infračervené osvětlení oka
- **Během snímání se duhovka mapuje do fázorových diagramů**, které obsahují informaci o orientaci, četnosti a pozici specifických plošek (tzv. kruhy, rýhy, skvrny, korónky a další)
- Tyto **informace pak slouží k vytvoření duhovkové mapy a šablony pro identifikaci**

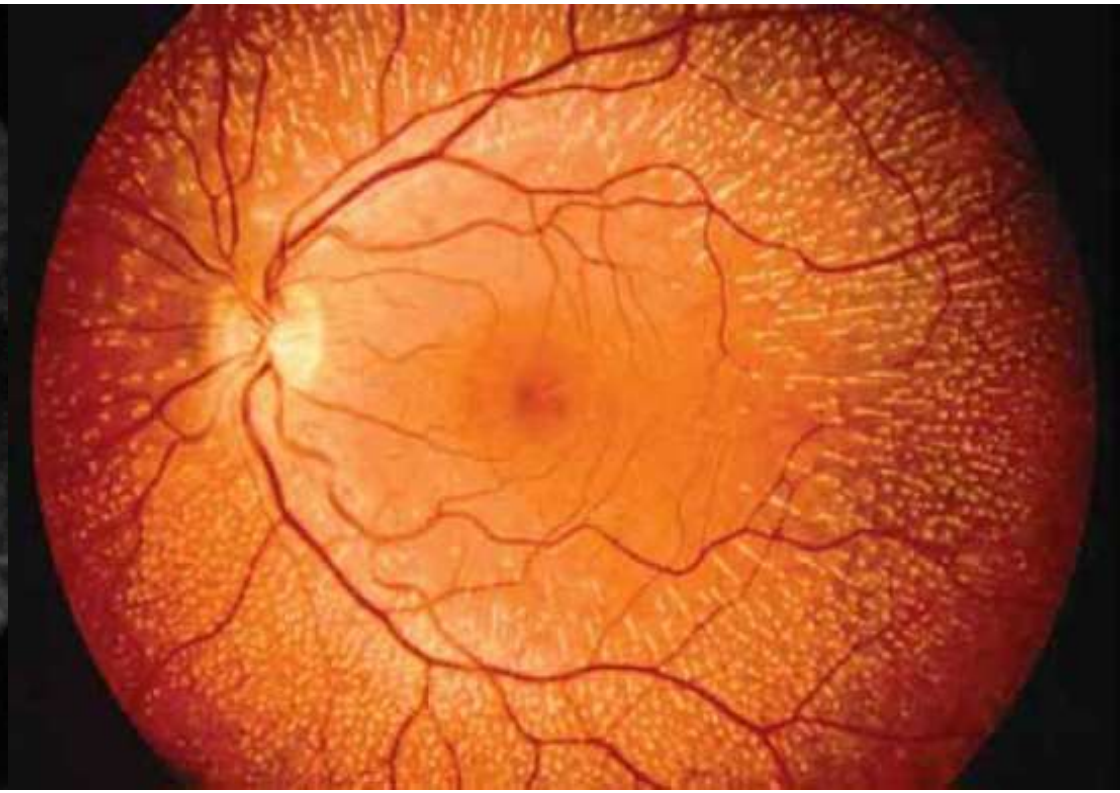




Oční duhovka 4/4

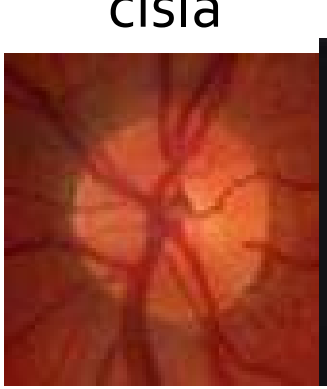
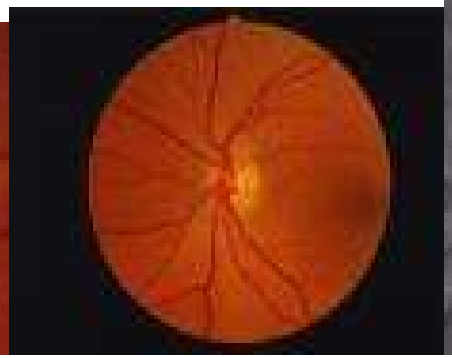
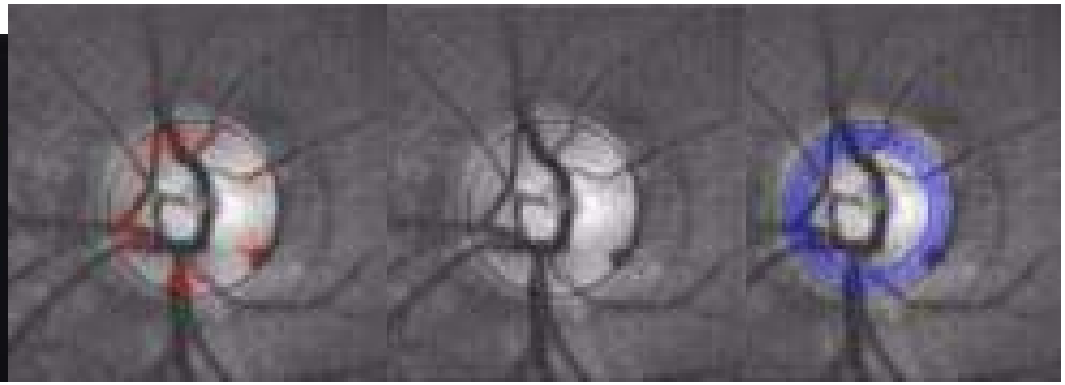


Oční sítnice 1/3



Oční sítnice 2/3

- Pro rozpoznávání osoby se používá **obraz struktury cév na pozadí lidského oka v okolí slepé skvrny**
- Sítnice je **světlo-citlivý povrch na zadní straně oka** a je složena z velkého množství nervových buněk
- **Pro získání obrazu** se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém (**infračervená LED dioda**)
- Neskenovaný obraz je poté převeden do podoby 40 bitového čísla

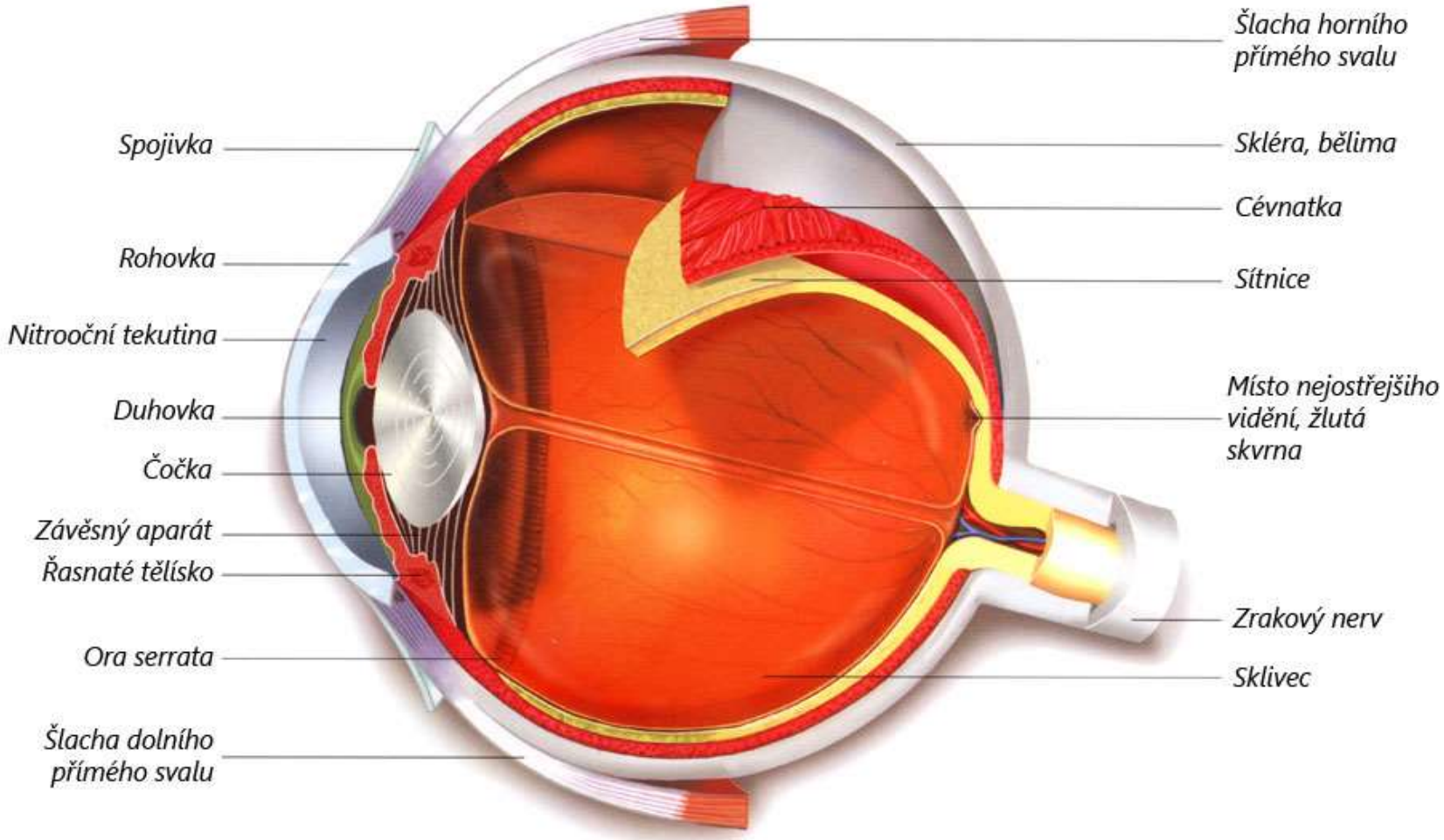




Oční sítnice 3/3

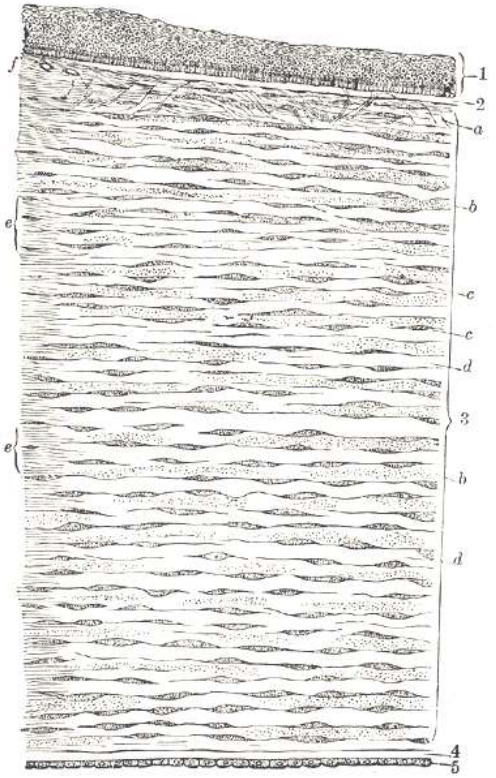
- Její používání vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné

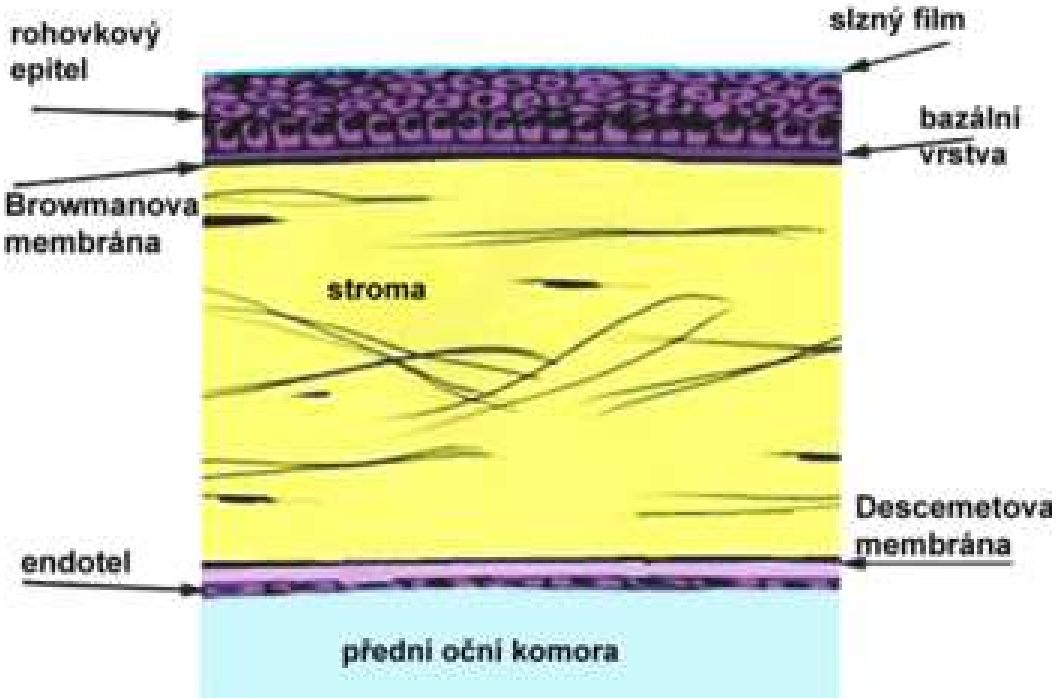
Její použití se shrnuje na oblasti nejvyššího stupně zabezpečení

Rohovka


Šlacha horního přímého svalu
Spojivka
Skléra, bělima
Cévnatka
Rohovka
Sítnice
Nitrooční tekutina
Místo nejostřejšího vidění, žlutá skvrna
Duhovka
Čočka
Závěsný aparát
Řasnaté tělísko
Zrakový nerv
Ora serrata
Sklivec
Šlacha dolního přímého svalu

Oční rohovka



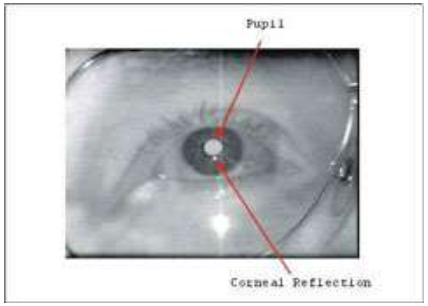


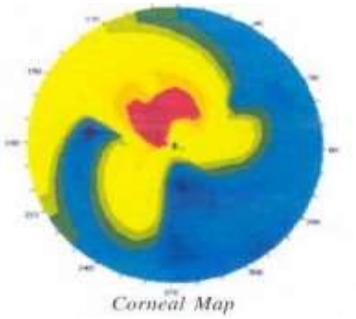
Rohovka

- je průhledná kopulovitě zakřivená vrstva pokrývající přední část oka
- je naprosto čirá a má lesklý povrch. Průhlednost rohovky a její optické vlastnosti umožňují světlu dosáhnout sítnice a vyvolat zrakový vjem.
- Základním úkolem rohovky je prostup a lom světla. Z vnitřní strany je rohovka omývána komorovou tekutinou. Z vnější strany je přes slzný film vystavena přímému kontaktu s vnějším okolím.
- Rohovkou neprocházejí žádné krevní cévy proto je vyživovaná částečně výměškem slzného aparátu a částečně komorovou vodou z přední oční komory.
- obsahuje mnoho nervových zakončení a tak je extrémně citlivá na dotyk, chemické nebo tepelné podráždění. Tato podráždění spouštějí rohovkový reflex, který uzavírá víčko a zvyšuje přítok slz.
- Průměr rohovky dospělého člověka je 11,5 mm. Uprostřed je rohovka 0,5-0,6 mm silná, u okraje pak 0,6-0,8 mm

Oční rohovka

- Princip metody je založen na tom, že infračervené světlo malého výkonu (vydávané diodou LED) zaměřené na střed čočky osvětluje oko.
- Světlo se odráží od rohovky a podle jeho intenzity oko reaguje.
- Tato reakce je u každého jedince v závislosti na čase a rozšíření čočky oka jiná.
- Reakce je kamerou snímána a srovnána s údaji v databázi.





Rohovková topografie

- Rohovková topografie je proces **mapování povrchu rohovky** za účelem získání podrobného popisu tvaru a lomivé síly rohovky v celém průměru.

- Nedílnou součástí dnešních topografů je počítač, který naměřená data zpracovává. Díky tomuto propojení topografy nabízejí řadu grafických presentací usnadňující interpretaci a využití získaných dat.

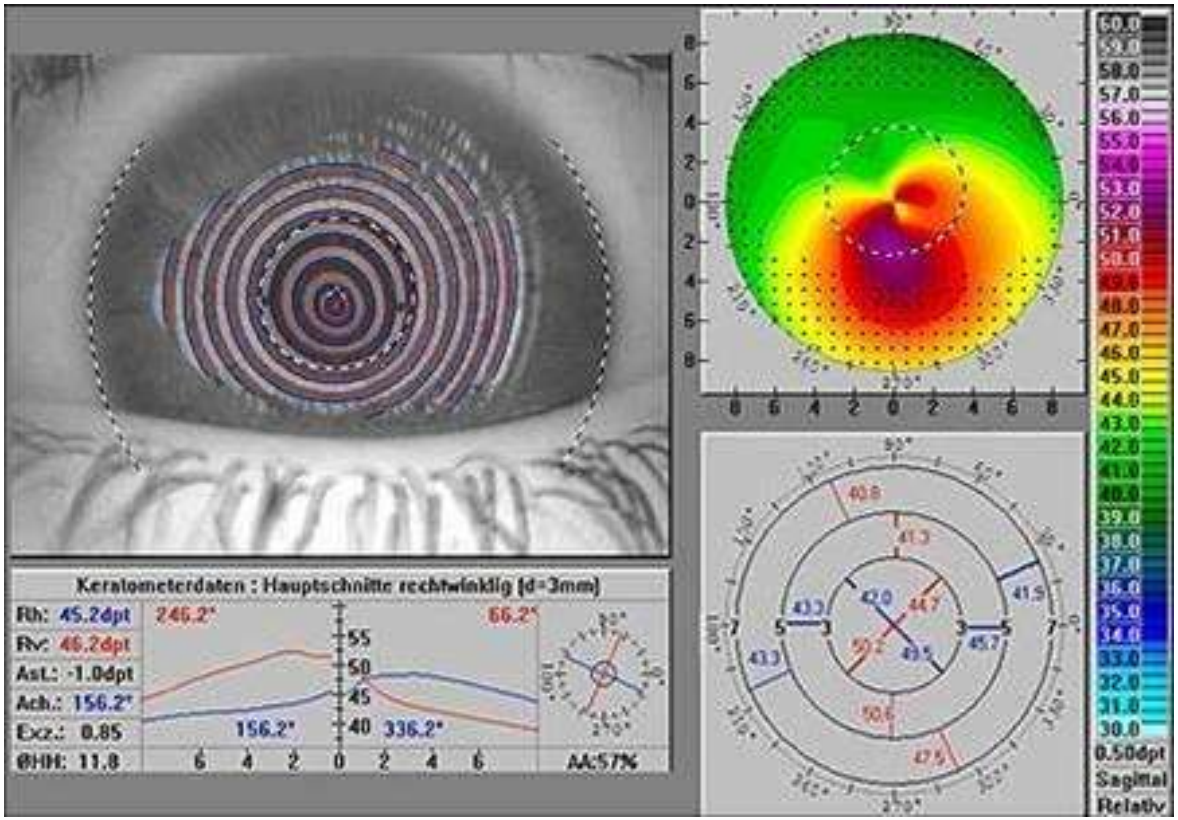
- Rohovková topografie představuje pokročilejší metodu měření poloměru křivosti rohovky ve srovnání s předešlými. Na trhu najdeme širokou škálu přístrojů. Podle principu jsou děleny na přístroje založené na **Placidově kotouči**, **rasterstereografii** nebo
systému **slit-imaging**.

- Dostupné topografy vyhodnocují od **8000** do **10 000** **datových bodů**
z celého průměru rohovky

Topografy s Placido kotoučem

- Placido-kotouč se skládá ze souboru osvětlených soustředných kružnic ve středu s pozorovacím otvorem.
- Projekcí Placidova kotouče na rohovku dochází k odrazu části světelného svazku od rohovky. Tyto paprsky jsou zachyceny kamerou a tvar rohovky je rekonstruován pomocí polohy a deformací kružnic Placidova kotouče.
- Paprsky odražené od rohovky nesmí být zaměněny s paprsky odraženými od jiného povrchu např. nitrooční čočky

Data zjištěná rohovkovou topografií jsou běžně znázorňována dvourozměrnými mapami. Třeti rozměr je vyjadřen barevnym schematem, kdy bodům se stejnymi hodnotami odpovida stejna barva. Většinou teple odstiny odpovidaji místům strmějším.



Systém slit-imaging

- V případě systému slit-imaging přístroj souvisle promítá na rohovku z různých úhlů. Světlo se tak odráží nejen od rohovky, ale i od duhovky a čočky. Tímto způsobem proměření předního segmentu oka jsou získány informace o přední a zadní ploše rohovky, duhovce, komorovém úhlu, přední ploše čočky

Hlavní využití

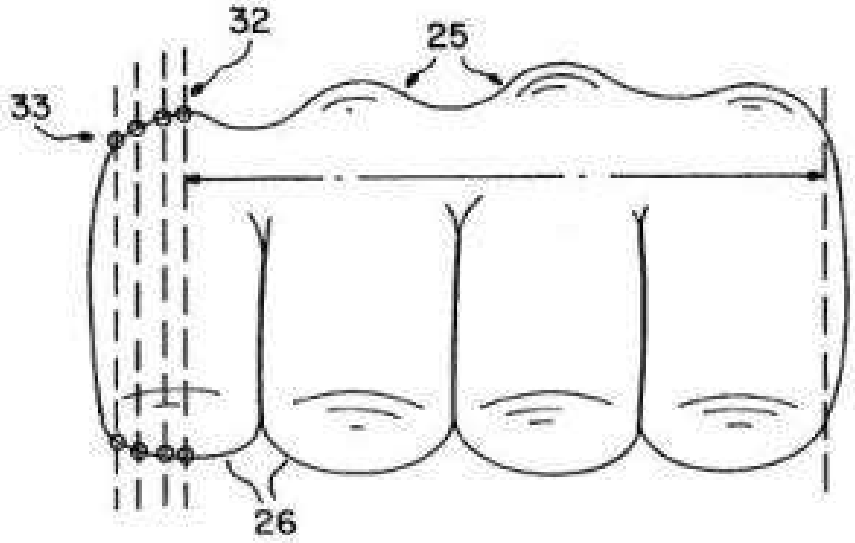
- je nepostradatelná pro refrakční chirurgii
- poskytuje informace pro předoperační screening, plánování operace, vyhodnocení výsledků operace
- při diagnostice astigmatismu, keratokonu, korekci afakie
- pri aplikacii kontaktních čoček
- verifikácia osôb pri vstupe do chránených objektov a pod.

Verifikace podle způsobu pohybu očí

- Na Slezské univerzitě v Gliwicích v Polsku byl vyvinut biometrický snímač pohybu očí při pozorování cílů na obrazovce počítače
- Při této metodě jsou **nutné brýle**, **které na principu infračerveného světla snímají pohyby očí a ty srovnávají se záznamy uloženými v databázi**
- Tento způsob zatím není však využíván komerčně

Verifikace podle tvaru článku prstu a pěsti

- K individuální identifikaci se využívají biometrická **měření článků prstů na sevřené dlani ve vnější části**
- Podle potřeb na přesnost se využívá až 35 parametrů, resp. měření sevřené dlaně na digitální fotografii uložené v paměti počítače s parametry sejmutými například při vstupu do chráněného objektu u snímače

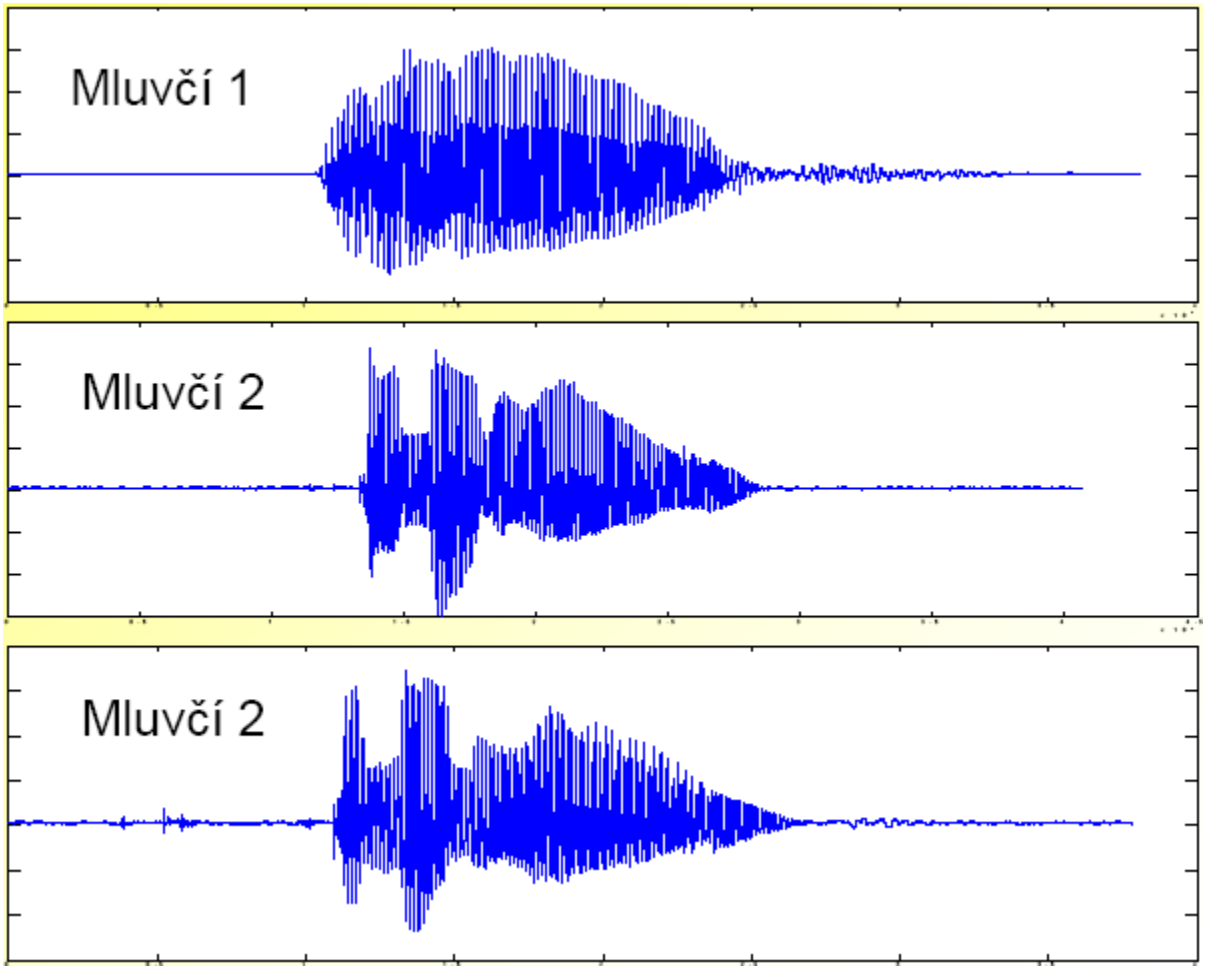


Ověřování hlasu 1/3

- Porovnávání vzorků hlasu používají kriminalisté již desítky let
- V civilní praxi se ale tato technologie začíná prosazovat až nyní
- Pro ověření identity subjektu slouží **předem uložené vzorky hlasu** – ***namluvené klíčové věty***
- Uživatel je vyzván, aby vyslovil předem určenou větu
- Sebelepší imitátor bez znalosti klíčové věty nemůže ošálit identifikační systém

Tvar a rezonance ústní dutiny, jazyka a zubů

Ověřování hlasu 2/3

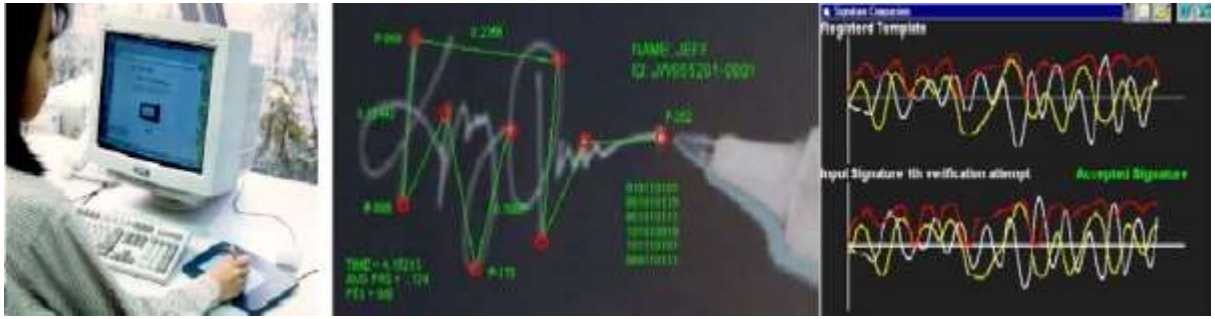


Ověřování hlasu 3/3

- Identifikace pomocí hlasu, tedy rozpoznání hlasu mezi jinými v reálném prostředí je mnohem náročnější a v současnosti neexistuje dostatečně přesný systém
- Hlavní výhodou verifikace identity pomocí digitálních otisků hlasu je **nízká cena, poměrně vysoká spolehlivost** a naprostá neinvazivnost technologie i široké možnosti nasazení od telefonního bankovnictví po vzdálený přístup k informačním systémům

Dynamika podpisu 1/3

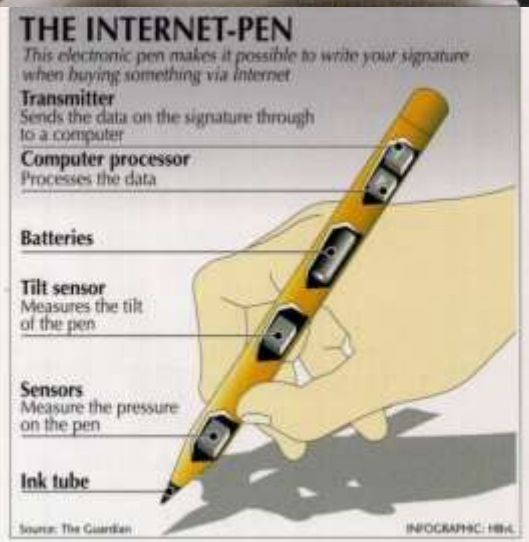
- Datována k roku 1977
- Využívá jedinečnosti **kombinace anatomických a behaviorálních vlastností člověka, které se projeví, když se podepisuje**
- Zařízení na dynamický podpis se často mylně zaměňují s pojmy jako je elektronický podpis (šifrovaný klíč) nebo se zařízeními na snímání podpisu jako obrazu
- **Z ručního podpisu lze elektronicky zjistit tah, tvar a tlak při psaní**, což lze použít pro verifikaci osoby

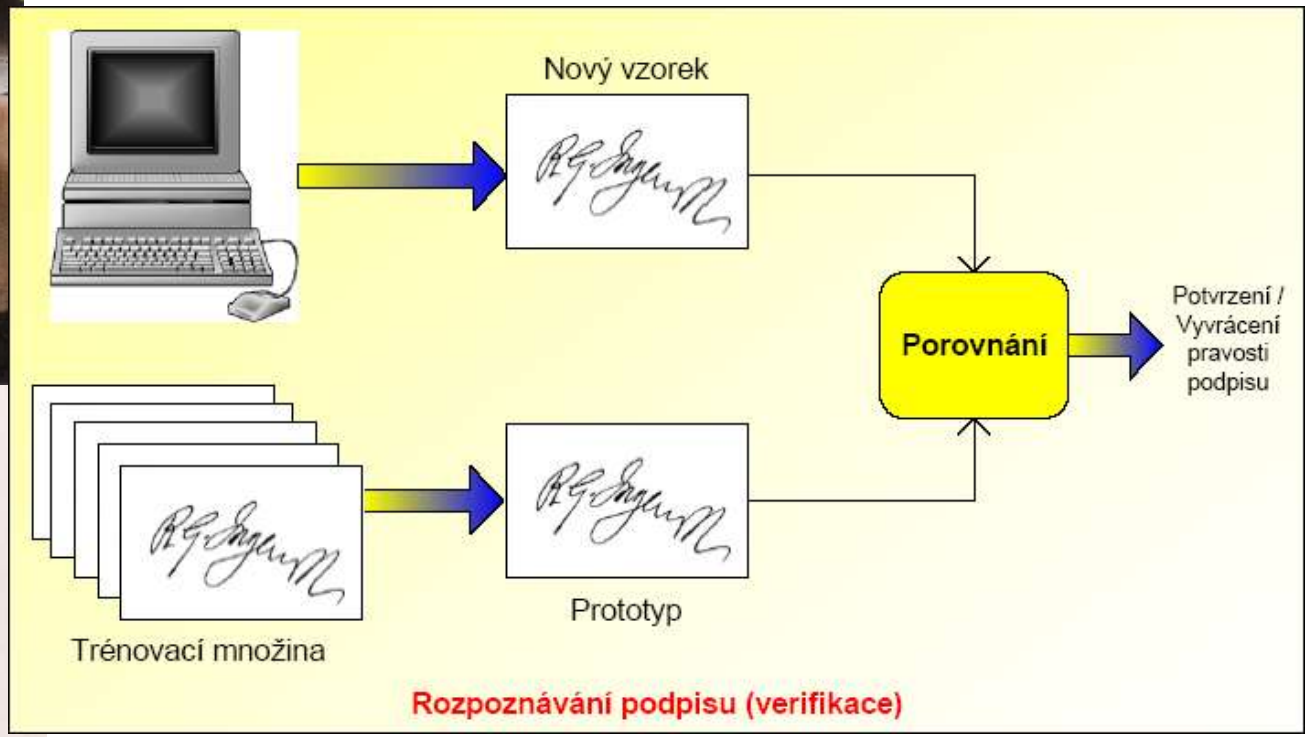


Dynamika podpisu 2/3

- **Většina zařízení využívá dynamických vlastností podpisu**, ačkoliv existují i kombinace se statickými a geometrickými vlastnostmi podpisu
- Základními dynamickými vlastnostmi jsou **rychlost, akcelerace, časování, tlak a směr tahu**, které jsou zaznamenávány v trojrozměrném souřadnicovém systému
- Problémy s uživateli, jejichž styl podpisu se pokaždé výrazně liší

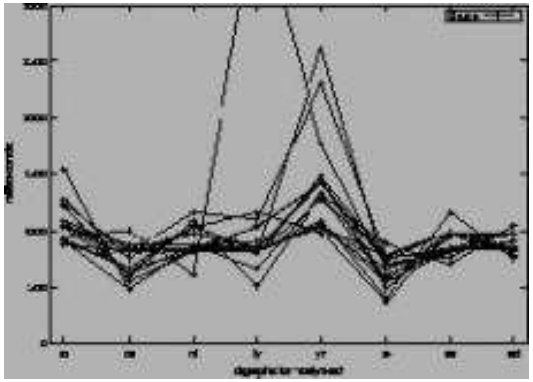
Dynamika podpisu – Dynamic signature 3/3

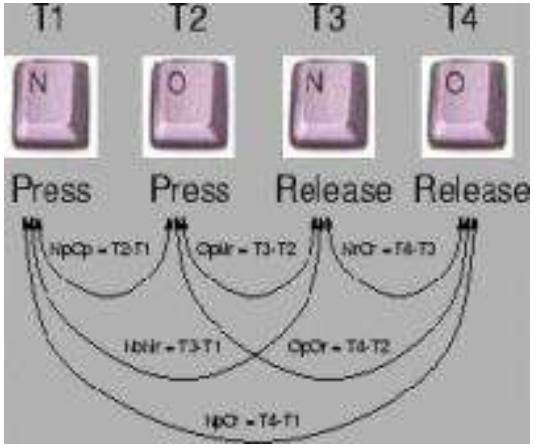




Dynamika stisku kláves 1/2

- Obdobou dynamického podpisu
- **Sleduje dynamiku úhozů na klávesnici,** která se u různých lidí liší
- **Sleduje se doba, po kterou jsou klávesy drženy, stejně jako prodleva mezi jednotlivými stisky kláves**
- Vytvoření „otisku" psaní na klávesnici trvá trochu déle než sejmutí otisku prstu do databáze, ale přesto jde o neinvazivní a dobře přijímanou metodu identifikace



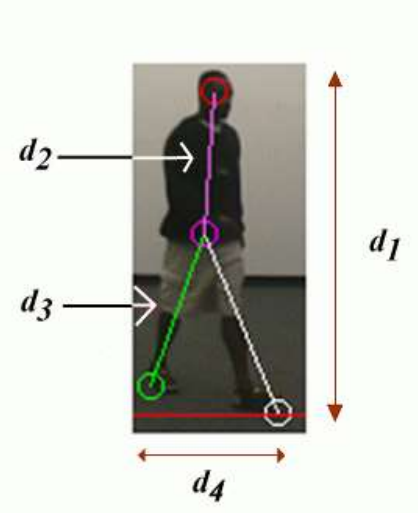


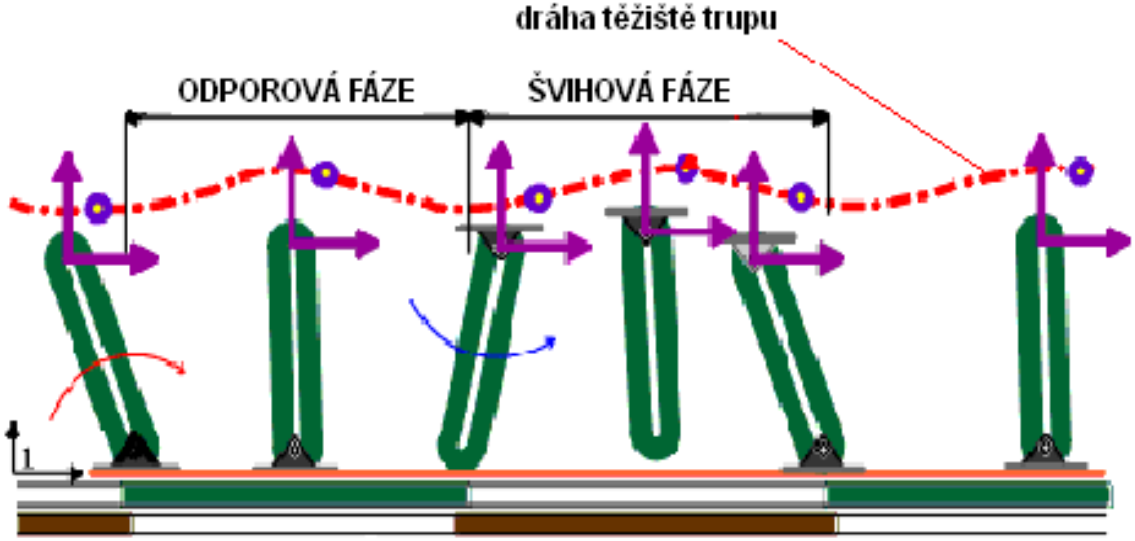
Dynamika stisku kláves 2/2

- **Určeny pro ochranu nežádoucích přístupů k osobním počítačům i ke vzdáleným informačním systémům** pracujících v režimu on-line
- Nevýhodou je poměrně velká **pravděpodobnost „zaměnitelnosti"** charakteristik psaní na klávesnici u více uživatelů
- **Dynamika psaní se navíc s časem může měnit**
- Jde o zajímavou metodu sekundární autentizace přístupů, protože rozpoznávání může běžet na pozadí a při zjištění odchylky od uloženého vzorku může například vyvolat žádost o další identifikaci

Dynamika chůze 1/2

- **Pohyb člověka je jedinečný a svým způsobem neměnný** v relativně širokém časovém období neměnný
- České kriminalistice a jejímu výzkumu patří přední místo ve světě ve vývoji identifikace člověka podle stylu chůze, tedy „pohybu po dvou nohách" ,nebo bipedální lokomoce
- Velký podíl na rozvoji této metody má i rozmach záznamové a snímací techniky





Dynamika chůze 2/2

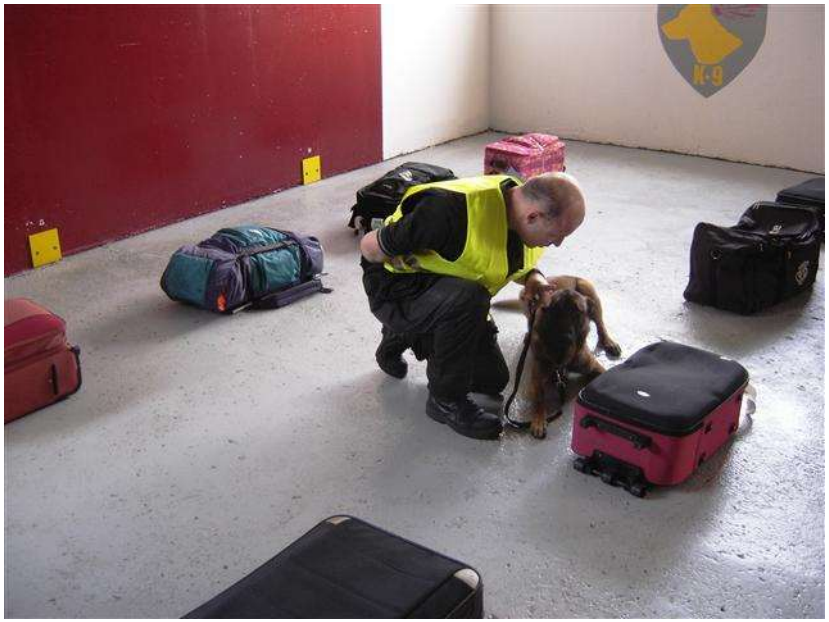
- **Dynamický stereotyp celého pohybu těla**
- Její uplatnění je tedy pouze ve forenzní sféře, kde však **dosud stále neexistuje databáze srovnávacích materiálů**
- Celá metoda pracuje na základě **porovnávání křivek drah, které opisují určité body na lidském těle**, tedy hlavně jeho těžiště
- Jelikož je každý člověk jedinečný svým pohybovým svalově kosterním systémem a svým dynamickým stereotypem, jsou i **křivky uvažovaných bodů unikátní** a vhodné pro srovnávání a 1:1 identifikaci

Verifikace a identifikace podle pachu 1/2

- Pachových stop používá policie jako nepřímého důkazu již desítky let, v civilní branži se ale tato technika stále jeví jako okrajová
- Lidský pach může být při dostatečně přesném měření poměrně spolehlivým identifikačním vodítkem
- **Lidský pach se skládá přibližně ze třiceti chemických sloučenin, jejichž intenzita či absence vytváří jedinečný profil u každého člověka**
- Kriminalistická praxe místo senzorů používá s vysokou spolehlivostí **psy**

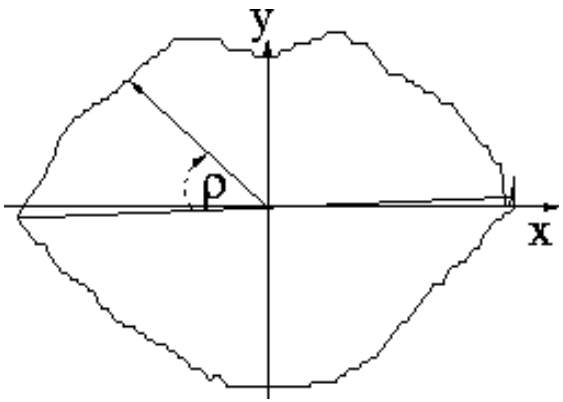
Verifikace a identifikace podle pachu 2/2

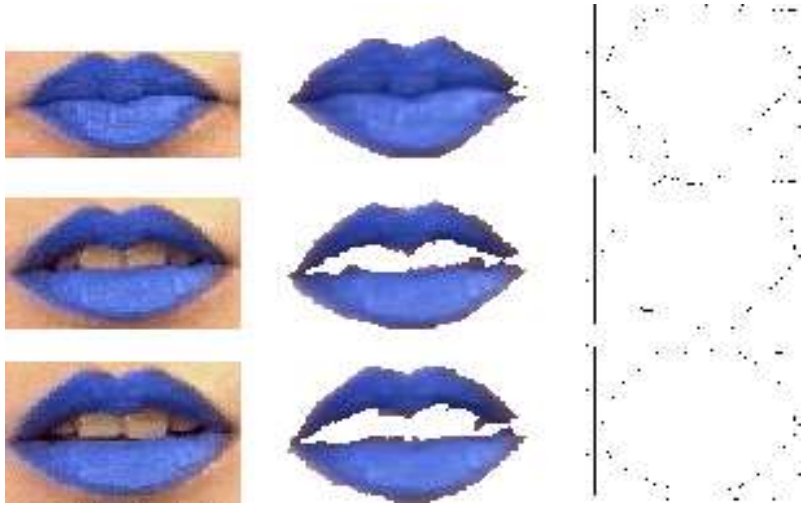
- **Problémem jsou změny ve skladbě pachových stop při emocionálních či hormonálních výkyvech**
- **Možnost využití spektrografie**



Verifikace osob podle tvaru a pohybu rtů

- Pohyb a výraz obličeje lze využít v biometrické identifikaci rovněž na detekci pohybu rtů
- Rty jsou pomocí PC na obličeji zvýrazněny a je **sledována jejich dynamika při hovoru**
- Tato se pravidelně opakuje a tento pohyb lze využít k individuální identifikaci osoby

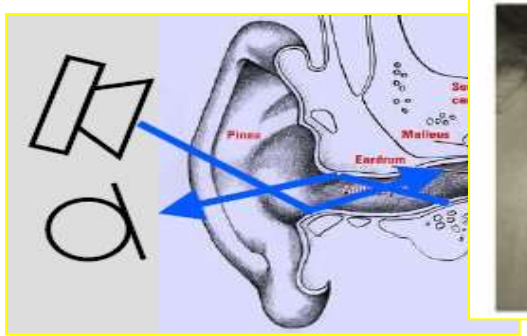


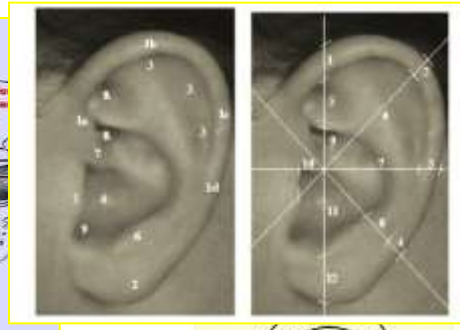


Ostatní biometrické systémy 1/3

Biometrie ucha

(boltec a zvukový kanálek)
Morfometrické vztahy v geometrii ušního boltce. Rozložení teploty na ušním boltci





Spektroskopie kůže

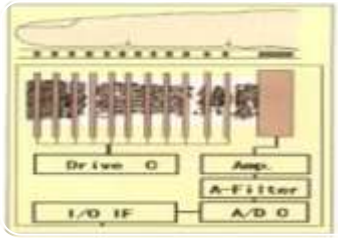
Vrstvy mají odlišnou tloušťku. Vlnová délka světla se láme a odráží v jiné vrstvě pokožky

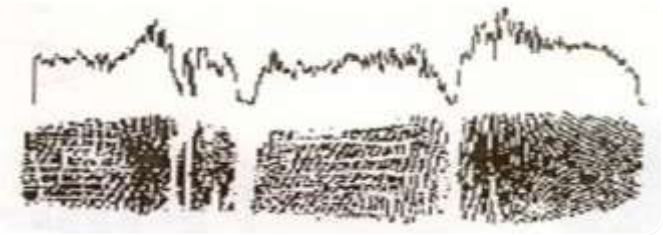
Krevní řečiště dlaně

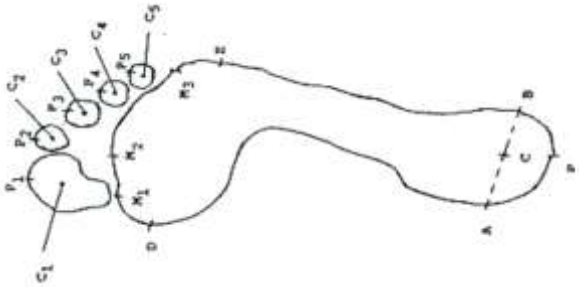
Ostatní biometrické systémy 2/3

Vrásnění článků prstů a kloubů prstů

Elektrostatické kapacitní reaktance
měření vrásek za klouby prstu

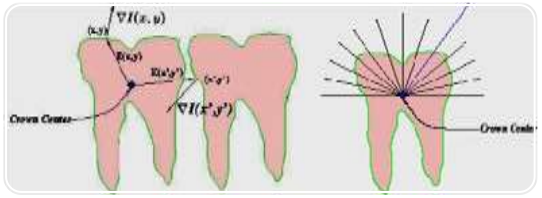




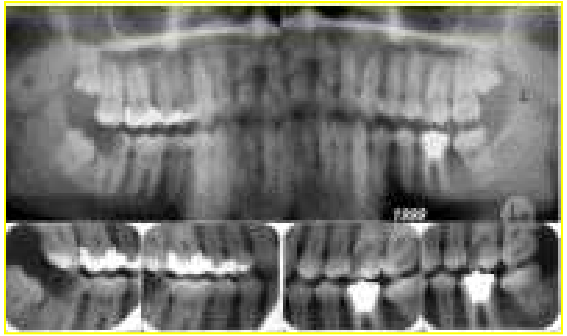


Plantogram

Vnitřní stavba chodidla, Kresba papilárních linií. Kombinace 38 rozměrů



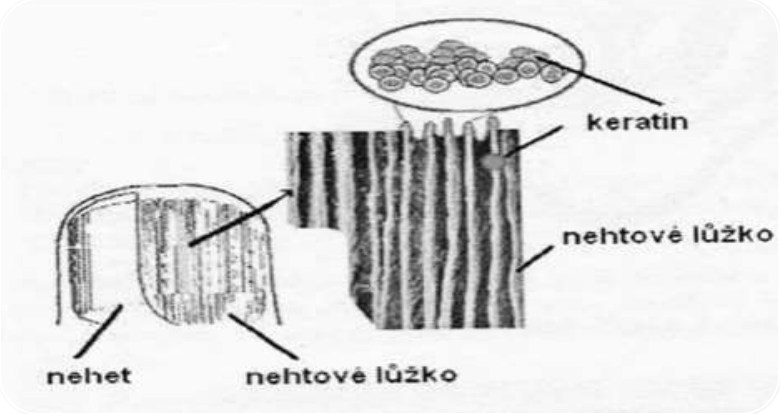
Vlastností zubů a čelisti

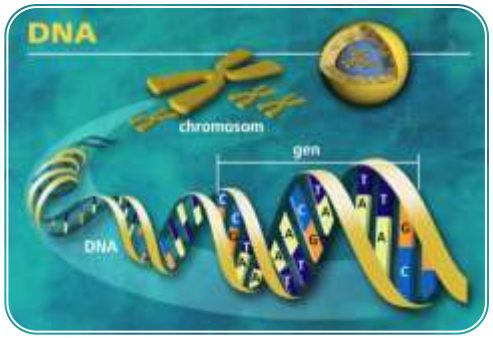


Ostatní biometrické systémy 3/3

Podélné rýhování nehtů

K identifikaci je využito keratinu v prostoru mezi nehtem a nehtovým lůžkem





DNA

DNA odlišná , výjimka jednovaječných dvojčat.Zdlouhavá procedura

Porometrie

Vzhled a lokalizace kožních pórů

Praktické využití

Speciální technologie využívané v bezpečnostní praxi

- Technické prostředky ochrany veřejných objektů a veřejného pořádku
- Nesmrtící zbraně

Technické prostředky

- zajištění veřejného pořádku mezi obyvatelstvem je jedním z předpokladů rozvoje jakékoliv společnosti
- tyto prostředky používají státní bezpečnostní organizace (PČR, vojenská policie)
- patří mezi **opatření,** která bezpečnostní složky využívají **k eliminaci negativních jevů a** v mezích zákona **udržují veřejný pořádek**

Technické prostředky ochrany veřejných objektů a veřejného pořádku

- **Dělí se na:**
  - **Zásahové prostředky** – slouží k otupení agresivity u protispolečenského davu (obrněné transportéry, vodní děla, slzotvorné granáty, štíty, přilby ochranné vesty atd.)
  - **Dokumentační prostředky** – záznámová zařízení, kamery, magnetofony
  - **Informační prostředky** – dohledová průmyslová televize, zavedení linky bezpečnostního informačního systému 112

Technické prostředky zásahové, hromadné

Tyto prostředky lze rozdělit na:

- **útočné -** obrněné transportéry, vodní děla, slzotvorné prostředky
- **ochranné -** pletivové nebo mřížové zátarasy, nákladní vozidla

Obrněné transportéry

- **Využitelnost:**
  - jako dopravní prostředek na místo zásahu
  - poskytují ochranu osádce
  - k vytlačování davu
  - nosič jiné techniky (vrhače slzotvorných granátů)

Služební vozidla s radlicí

- **Vytlačuje se jejich prostřednictvím agresivní dav** z veřejných prostranství a to **pomalou jízdou proti davu**, kdy vytlačování sledují bezpečnostní složky
- Často kombinovány s vodními děly

Vodní děla

- Skupina speciálních nebo speciálně upravených vozidel pro vedení zákroku resp. pro jeho podporu proudem vody
- Proud vody aplikovaný k obnovení veřejného pořádku je účinným prostředkem

Technické prostředky zásahové individuální

Tyto prostředky lze rozdělit na:

- **aktivní -** pryžové obušky, kapesní rozstřikovače slzotvorných látek, služební pouta, jednorázová plastiková pouta, služební zbraň
- **ochranné -** ochranná přilba, ochranný štít, ochranné brýle, ochranná maska, ochranný charakter stejnokroje

Obušky 1/2

- **Jsou jedním ze základních technických prostředků**
- Všechny druhy a velikosti obušků, včetně obušku s příčnou rukojetí (tonfa - příčná rukojeť, tvrzený plast)
- Slouží zejména k překonání odporu
- Je nutné omezit údery **na svalnatá místa těla**, kde se nenacházejí důležité orgány (záda, hýždě, stehna, paže)
- Prodlužuje účinný dosah policisty při zásahu

Obušky 2/2

- **Protikonfliktní policejní týmy**, určené k vyjednávání s útočníky jsou vybaveny **kovovými teleskopickými obušky**
- Jsou nošeny složené skrytě **ve vnitřní kapse kombinézy**, aby policista vzbuzoval dojem, že není ozbrojen
- Použit **pouze při útoku na policistu**

Služební pouta

- Jsou **nezastupitelným prostředkem faktického zajištění** osob (např. pouta RALK)
- **Ke spoutání eskortované osoby**, která ohrožuje svoji bezpečnost, jiné osoby, policisty, poškozuje cizí majetek
- Ke spoutání rukou **vpředu nebo za zády**, případně k vzájemnému připoutání dvou či více osob
- Ze všech pout se dá uvolnit a mohou být pak použita jako zbraň proti policistovi

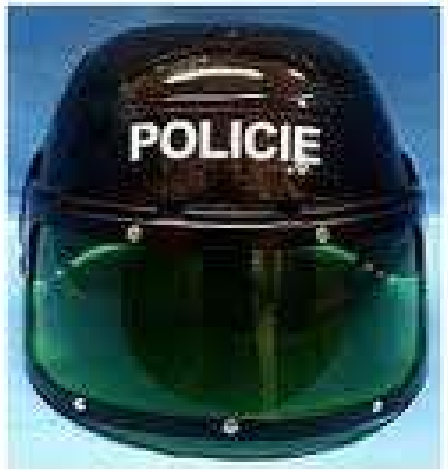
Jednorázová plastiková pouta RALKPLAST

- **Mají malou hmotnost** a lze je lépe nosit v oděvu
- Nestávají se zbraní, jako klasické pouta
- Vyproštění z těchto pout není při dozoru nad osobou tak snadné, jak se mnohdy uvádí
- Jejich hlavní nevýhodou je ten fakt, že je při kladení i malého odporu nemůže nasadit jednotlivec
- Pouta jsou **pouze na jedno použití**, snímají se rozříznutím

Služební pouta – další typy

Ochranná přilba

- Plní úlohu **ochrany hlavy**
- Hlavní požadavky jsou **mechanická odolnost, schopnost kompenzace energie nárazu a nízká hmotnost**
- Obličejový ochranný štít by měl být barevně tónován tak, aby **nebylo vidět do tváře policisty**
- Nejedná se pouze o psychologický moment, ale o výrazný prvek zabezpečení ochrany policisty



Ochranný štít

- Má podobnou roli jako ochranná přilba
- Jsou na něj kladeny i podobné požadavky jako na přilby
- **Nemá zabezpečit vždy pouze ochranu jednoho policisty**
- Slouží i **ke krytí ostatních policistů**, případně k vytvoření chráněného koridoru pro odsun raněných, a to nejen policistů

Ochranný charakter stejnokroje

- Kladná role ve **zvýšení ochrany policistů**
- Oděv by neměl skýtat možnost uchopení za jeho součásti ani za popruhy
- **Vyztužení exponovaných částí** a o**dolnost proti vodě** by měla být jedním z hlavních předpokladů
- Za nevhodné pro zásah v pořádkové jednotce je možné považovat i nošení služební zbraně vně oděvu na opasku

Ochranné brýle a ochranná maska

- Oba prostředky jsou určeny **k ochraně před vlivem chemických prostředků**
- Ochranné protichemické **brýle chrání pouze zrak** (ostatní orgány nejsou na působení slzotvorných prostředků tak citlivé, míra podráždění je snesitelná)
- Ochranná **maska chrání** nejen zrak, ale i **dýchací orgány** a citlivou pokožku obličeje

Nesmrtící zbraně „non-lethal weapons"

- Skupina prostředků, resp. nesmrtících a neničivých zbraní, **určených výlučně k zneschopnění a odpuzení osob** s velmi nízkou pravděpodobností jejich trvalého poškození, **nebo k vyřazení techniky**
- Vyvíjeny se záměrem **minimalizovat ztráty na zdraví, majetku, okolního prostředí** při zachování účinnosti
- Jejich používání musí být vždy uvážené

Nesmrtící zbraně „non-lethal weapons"

- **Využití:**
  - **vyřadit z činnosti vybranou skupinu lidí**
  - vyřadit z činnosti vybrané **druhy vojenské techniky**
  - pro **boj proti teroristům** a únoscům bez ohrožení rukojmích a nezúčastněných osob
  - k **zásahům proti povstalcům** a ozbrojeným bandám v místech s vysokou koncentrací obyvatelstva
  - **při lokálních konfliktech** nižší úrovně nebo při potlačování nepokojů

Nesmrtící zbraně

- **Rozdělení do podle technologií a fyzikálních vlastností prostředků:**
  - **Elektromagnetické** – usměrněná energie (paprsek) v ultrafialové, viditelné a IR části spektra, elektromagnetická energie jako milimetrové vlny, mikrovlny, rádiový kmitočet…
  - **Chemické** – organické a anorganické sloučeniny, které reagují s jinými sloučeninami a látkami
  - **Akustické** – zvuková energie se slyšitelnými i neslyšitelnými kmitočty (způsobující bolest hlavy)
  - **Optické** – světelné záblesky (světelné, laserové zbraně)

Nesmrtící zbraně

- **Mechanické a kinetické** – šoková munice s malou energií využívající své hmotnosti a zrychlení k zasažení cíle (pryžové střely) nebo jako zásahová rozbuška, která vytváří před davem akustický detonační a optický efekt, ale nemá žádné střely
- **Doplňkové** – technologie umožňující skladování, dopravu a užití (nosiče) neničivých prostředků.
- **Biologické** – mikroorganismy a hmyz, které poškozují různé prvky elektronických - izolaci, desky plošných spojů, těsnicí a umělohmotné materiály, kovy a slitiny i pryž, konzervační přípravky a tepelné izolace

S mechanickým účinkem
Jednoúčelové prostředky

- **Mají porážecí a bolestivý účinek**
- Vystřelují dle typu a počtu hlavní počet gumových míčků o průměru 35 mm, které se pro zmírnění bolesti při dopadu na útočníka rozpadnou na dvě poloviny
- **Efektní** zásahy těchto zbraní jsou **do 15 m**
- Nebezpečné při zásahu do hlavy, krku a břicha

S mechanickým účinkem
Univerzální granátomety

- Na přímou a nepřímou střelbu do davu

- **Používají se:**
  - kouřové,
  - slzné,
  - barvicí světelné,
  - zvukové nábojnice.

- Nejčastěji náboj (cca 200 ks gumových kuliček), které se po vystřelení odrážejí od země a takto působí kinetickými údery na osoby

Univerzální granátomety - Zásahová výbuška P-1

- **Prostředek aktivní ochrany**, omezuje možnost aktivního odporu
- Plášť výbušky je kovový, po jejím iniciování dochází po 3 sek. k vytržení zátky třecího rozněcovače
- Z pouzdra vyletí **14 létavic** s raketovými motorky, které nevypočitatelně **létají po prostoru, odrážejí se od stěn**, předmětů a vydávají oslňující záblesky
- Po vyhoření motorků létavice explodují
- Výbuchy jsou pro sluch na hranici bolestivosti
- **Pouze modřiny a šok**

S mechanickým účinkem
Vystřelovací sítě 1/2

- k polapení agresivních lidí, zvířat a zamezení jejich útěku
- používá se síťová puška (hlavně ve vězeňské službě)
- **puška má čtyři hlavně**, do kterých se vloží prachová náplň a na ni se nasadí náboje z pěnového plastu, ke kterým jsou přivázány konce sítě uložené ve vaku střelce
- po odpálení jsou pěnová závaží vystřelena a táhnou za sebou síť, která omotá osobu na útěku
- síla sítě není příliš veliká a nezpůsobuje zranění

S mechanickým účinkem

Vystřelovací sítě 2/2

S mechanickým účinkem
Rychle tuhnoucí pěny

- Používají se při **potlačování davových nepokojů**
- Na dav se dopraví **větší množství roztoku tvořícího bohatou pěnu**, která **rychle tuhne a znemožní pohyb** osob i vozidel
- Po zpacifikování je dav postupně vysvobozován pomocí další chemické látky po jednotlivci
- Výsledkem je volně odtékající, zdraví a přírodě nezávadná kapalina, která steče do kanalizace
- Syntetická pěna se stříká z přenosného rozprašovače až na vzdálenost **10 metrů**

S mechanickým účinkem
Vodní děla 1/2

- Používají se vozidla k tomuto účelu určená
- Při méně agresivním davu postačí osoby kropit
- Automobilová stříkačka se používá také k vytlačení, rozptýlení a zastavení davu (zátaras ulice)
- **V policejní praxi se využívá:**
  - **přímý proud vody** na nohy první řady davu do vzdálenosti **50 m**
  - **nepřímý postřik** nad hlavy davu do vzdálenosti **100 m**

S mechanickým účinkem
Vodní děla 2/2

- Do vody se může **přidávat barvivo** k označení agresivních osob a **slzotvorné prostředky**
- **Pro zvýšení účinku** na agresivní dav se může proud vody **elektrifikovat**
- Zásah takto elektrizovaným proudem vody se slzným plynem je k rozptýlení davu nejúčinnější
- Zpacifikované výtržníky je pak možné zadržet díky barevnému označení i v pozdější době
- Proudnice se ovládá z kabiny řidiče pomocí joysticku

S chemickým účinkem 1/2

- Používají se **slzotvorné prostředky CN, CS, OC** a jejich směsi
- Účinek je závislý na duševním stavu nepřátelských osob a jejich hladině adrenalinu
- Slouží **k otupení agresivity menšího davu**, popřípadě jednotlivce.
- **Nejčastěji kapesní aerosolové rozstřikovače:**
  - CN – chloracetofenon
  - CS – 2 chlorbeniliden malonnitril
  - CR – dibenz(a)oxazepin
  - OC – oleum capsicum, pepper

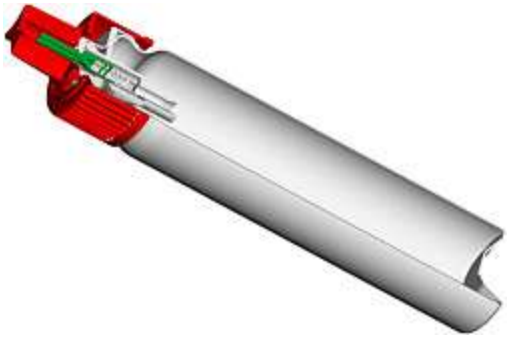
S chemickým účinkem 2/2

- **CN** (chloracetofenon) – způsobuje slzení, škrábání v nose, tečení z nosu, pálení v hrdle a nezadržitelný kašel
- **CS** (2 chlorbeniliden malonnitril) – způsobuje stejné, ale závažnější účinky jako předchozí, protože je silnější
- **CR** – (dibenz(a) oxazepin)
- **OC** – (oleum capsicum, pepper) – kajenský pepř, na rozdíl od předchozích se nevypařuje a působí tak déle

- Obsluze se doporučuje **používat ochranné brýle**, masku, **nepoužívat proti větru**
- Prostředky s chemickým účinkem se aplikují také jako narkotizační střely, aerosol, kouř, pěna, prášek, atd.

S chemickým účinkem
Kapesní aerosolové rozstřikovače

- **KASR** slouží k aplikaci aktivní aerosolové náplně ve formě **úzkého a dlouhého paprsku** do požadovaného směru
- Aerosolová náplň je vystříkána z pohotovostního tlakového zásobníku, který se jednoduchými úkony do rozstřikovače vkládá a po vyprázdnění vyměňuje



S chemickým účinkem

Ruční granát slzotvorný RGSL - 85

- Využíván **k vytvoření slzotvorné clony**, resp. zamoření prostoru (chloracetofenon)
- Tělo (plášť) granátu tvoří tenkostěnná hliníková nádobka
- V důsledku tlaku plynů je proražena krycí fólie **výfukových otvorů**, ze kterých **proudí** intenzívně značné množství **slzotvorného plynu** a tělo granátu má poměrně vysokou teplotu (přes 200° C)

- Granát **je aktivní již na dráze letu**
  (ztíženo jeho odhození)

S elektrickým účinkem

- **Nesmrtící prostředky s elektrickým účinkem lze rozdělit na:**
  - Dotekové paralyzéry
  - Elektrické štíty
  - Elektrické opasky
  - Mobilní zátarasy
  - Tasery

S elektrickým účinkem
Dotekový paralyzér

- **Výboj 50 až 200 kV**, napájený běžnou 9V baterií
- Silný elektrický výboj okamžitě zneškodní útočníka již při letmém dotyku s jeho tělem (15 pulsů /s)
- Účinkuje přes silnou vrstvu oděvu (i koženého)

- **Použití a účinky paralyzeru:**
- ***0,5 s krátký úder*** - svalová křeč a úlek
- ***1 až 2 s střední úder*** - pád k zemi, duševní otřes
- ***3 až 5 s plný úder*** - pád útočníka, ztráta orientace a šok na několik minut

S elektrickým účinkem

Elektrické štíty

- Slouží k potírání agresivního davu
- **Povrch štítu je pokryt kovovými pásky** tak, aby měl zasahující orgán mezi nimi výhled
- Každá páska po sobě jdoucí je jiného elektrického potenciálu
- Při kontaktu tělem se osoba dotýká více pásků na štítu
- Spoušť se nachází v držadle štítu

S elektrickým účinkem

Elektrické opasky

- Používají se **k transportu zadržených osob**
- Jedná se o opasek, který si sama transportovaná osoba **nemůže sundat**
- Může pachatele paralyzovat elektrickým výbojem při jeho útěku, nebo jen jeho svévolným vzdálením se od prostředku
- Elektrody bývají dvě, na každé části zad jedna

S elektrickým účinkem

Tasery 1/3

- Jde o **malé ruční paralyzéry**
- Po stisknutí spouště je vystřelena **dvojice elektrod s hroty a zpětnými háčky**, které za sebou táhnou tenké izolované vodiče (drátky)
- Jedním drátkem postupuje proud, který prochází tělem a vychází druhým drátkem zpět do pistole
- Šipky mají **tupé rozšíření bránící hlubšímu vniknutí** do těla útočníka, ale jsou schopny proniknout i silnějším oděvem a zachytit se v kůži či oděvu

S elektrickým účinkem
Tasery 2/3

- **V okamžiku kontaktu** (přiblížení) hrotů elektrod k tělu **dojde k elektrickému výboji** a zasažená osoba je vystavena paralyzujícím účinkům vysokonapěťových pulzů (do těla však nejde 50 000 V), které jsou přivedeny ze zbraně pomocí izolovaných vodičů
- Vysílání elektrických pulsů lze opakovat pouhým stisknutím spouště
- K provedení dalšího výstřelu je třeba odstranit zbytek pouzdra náboje a vložit náboj nový
- Míří se vždy do hrudníku a do zad
- **Dostřel je cca 5 – 30 m**

S elektrickým účinkem

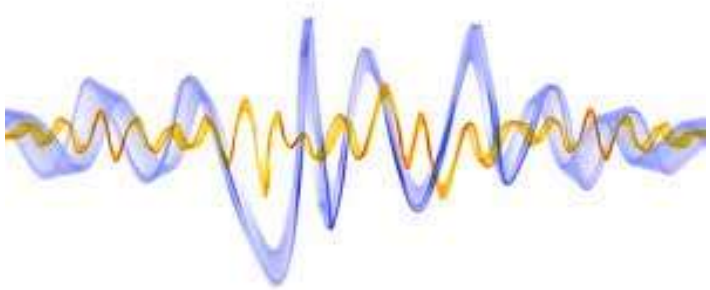
Tasery 3/3

Se světelným účinkem

- Jedná se o **ruční svítilny** se zábleskovou funkcí a munici pyrotechnického principu (**granáty**)
- Vlivem výrazného záblesku světla dochází ke stažení zornic zasažené osoby a ta tímto dočasně ztrácí schopnost vidění (5-10 min.)
- V kombinaci se silným zvukovým efektem je tato osoba dezorientována

Se zvukovým účinkem 1/2

- Jedná se o zbraně, které vedle světelného využívají také zvukový efekt
- Zvuk výborně proniká do budov
- **Při intenzitě okolo 100 dB** - působí na uši a nervový systém, způsobuje pocity nevolnosti a narušuje rovnováhu pachatelů
- **Při 130 až 150 dB** - překračuje hranici bolestivosti a narušuje se dýchání a zažívání, vznikají stavy typické pro epilepsii



Se zvukovým účinkem 2/2

- Dnes se vyvíjejí **přesné směrově paprskovitě působící akustické nesmrtící zbraně**

- **V praxi se užívají:**
  - **ruční akustické granáty** - dočasně ohluší a šokují agresivní osobu a odvádějí její pozornost
  - **kapesní sirény -** spoléhají na to, že zvukem odradí útočníka, jelikož tím na sebe upozorní okolí
  - **generátory ultrazvuku** - proti útočícím psům s dosahem cca 5 m

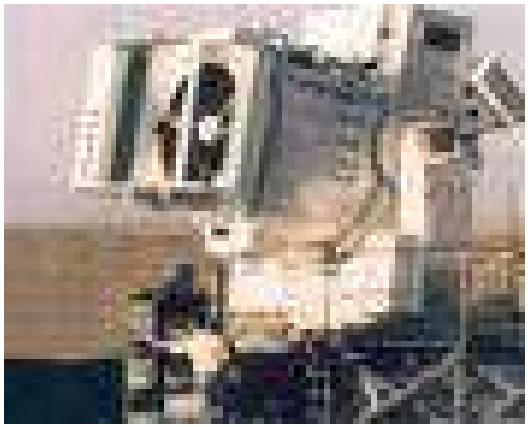
NOVINKY V OBLASTI NESMRTÍCÍCH PROSTŘEDEKŮ

Nesmrtící akustická zbraň 1/2

- Vyvinutá v USA armádě pod názvem **LRAD** (Long Range Audio Device) o hmotnosti cca 20 kg
- Prostřednictvím svého 84 cm diskovitého vysílače umí nasměrovat **vlnu ostrého 150 dB silného pronikavého zvuku**
- Koncentruje zvukové vlny na zvolený cíl a pak na něj vyšle zvuk o 30 dB nad prahem bolesti (150 dB)
- **Způsobí** zvracení, nevolnost, nepřítele ochromuje, dezorientuje a lze jim simulovat palbu ze střelných zbraní a jiné zvuky
- Ve vzdálenosti menší než 300 m způsobí trvalé ohluchnutí
- **Za ústím zbraně** dosahuje hluk **jen 60 dB**

Nesmrtící akustická zbraň 2/2

- Armáda vyvíjí ještě sofistikovanější infrazvukové zbraně
- Ty vysílají **zvukové vlny na extrémně nízké frekvenci**
- Puška tak vyvolá silný tlak na vnitřní orgány, který **způsobí** mimo jiné **nedobrovolné** vyprázdnění střev



Nesmrtící mikrovlnná zbraň

- K regulaci davu v systému nazvaném Aktive Denial Technology (**technologie aktivního odmítnutí**)
- Používá vysílač vytvářející **energii na frekvenci 95 GHz**
- Součástí je anténa, která zacílí neviditelné vlny na konkrétní osoby
- Tyto vlny proniknou cca 0,4 mm pod kůži a **způsobují nesnesitelné pálení**, které přestává, když osoba uteče z prostoru chráněného tímto přístrojem
- 6 ks nasazeno v Iráku (výsledek neznámy)

Nesmrtící zbraň BOULE

- Proti davu jsou vyvinuty tzv. **psychotronická zbraň**
- **Šíří neviditelné elektromagnetické paprsky** ovlivňující náladu, chování a tělesné procesy zasažených osob
- **Vysílají v různých vlnových délkách** velmi dlouhých vln ULF v kombinaci, kdy jedny vlny jsou nositeli vln druhých, například radiových
- Vlny na 2 - 3 dny **otupují myšlení osob, působí depresi**, zmatenost, srdeční arytmie, pocit strachu, bolesti hlavy atd.
- Diskutuje se nezpůsobují sebevražedné akce velryb

Dračí vejce

- Po vhození do okna inkriminované budovy (váží 900 gramů), **umožní** policistům **rozhled o 360 stupních**
- Obraz je **přenášen bezdrátově** do okruhu 300 m díky čtyřem kamerám
- Kamery jsou obaleny hmotou, jež tlumí nárazy
- Při nalezení miniaturní kamery a pokusu o její zničení tento prostředek vypustí slzný plyn

Literatura 1/9

1. BOHÁČEK, P. (2005), *Systémy AFIS a rozpoznávání otisků prstů*, Brno: VÚT Brno - Fakulta Informačních technologií. Semestrální práce, 2005, 10s.
2. BOSH Security Systems [online]. *IP produkty – HW*, 2008 [cit. 21.8.2013]. Dostupný z: http://boschsecuritysystems.cz/produkty.php?sel_skup=178#
3. BROMBA, M. (2007), *BIOIDENTIFICATION* [online]. 2007 [cit. 23.8.2013]. Dostupný z: http://www.bromba.com
4. CONET [online]. *Přístupové systémy*. 2001[cit. 22.8.2013]. Dostupný z: http://www.conet.cz/pristupove_systemy.html

Literatura 2/9

5. ČSN EN 50131-1: *Poplachové systémy – Elektrické zabezpečovací systémy. Část 1: Všeobecné požadavky*, 1999, Změna Z7:2008, Český normalizační institut
6. ČSN EN 50133-1: *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Část 1: Systémové požadavky*, 2001, Změna A1:2003, Český normalizační institut.
7. ČSN P ENV 1627: *Okna, dveře, uzávěry – odolnosti proti násilnému vniknutí. Požadavky a klasifikace*, 2000. Český normalizační institut
8. FBI Biometric [online], *Center of Excellence*. 1995 [cit. 22.8.2013]. Dostupný z: http://www.fbibiospecs.org/fbibiometric/biospecs.html>.

Literatura 3/9

9. GALBAVÝ, M. (2006), *Vizualizace a vzdálené řízení v síti LonWorks*, Praha: České vysoké učení technické v Praze – Fakulta elektrotechnická. Bakalářská práce, 2006, 61s.
10. JABLOTRON [online]. *Detektory*. 2005 [cit. 23.8.2013]. Dostupný z: http://www.jablotron.cz/ezs.php?pid=products/ja-6op
11. JAIN, A., BOLLE, R., PANKANTI, S. (2002), *BIOMETRICS - Personal Identification in Networked Society*. London : Kluwer Academic Publisher, 2002. 422 s. ISBN 0-792-38345-1.
12. MUL-T-LOCK [online]. *Mechanické zabezpečovací systémy*. 2006 [cit. 23.8.2013]. Dostupný z: http://www.multlock.cz/cz/kategorie/produkty

Literatura 4/9

13. PETÍK, L. (2008), *Použití biometrické identifikace při zabezpečení objektu*, Ostrava: VŠB TU Ostrava - Fakulta bezpečnostního inženýrství, Bakalářská práce, 2008. 46 s.
14. SANDSTROM, M. (2004), *Liveness Detection in Fingerprint Recognition Systems*. Linkoping, 2004. 149 s.
15. SAPELI [online]. *Dveře a zárubně*. 2006 [cit. 22.8.2013]. Dostupný z: http://www.sapeli.cz/index.asp?obsah=15&amp
16. SOUMAR, C. (2002), *Biometric system security*. In *Secure*. 01/2002. s. 46-49.
17. ŠČUREK, R. (2007), *Přednášky z předmětu Ochrana objektů*, Ostrava: VŠB – TUO, Fakulta bezpečnostního inženýrství, 2007.

Literatura 5/9

18. UHLÁŘ, J. (2001), *Technická ochrana objektů, I. díl, Mechanické zábranné systémy.* Praha: Policejní akademie České republiky v Praze, 2001. ISBN 80-7251-172-6.
19. UHLÁŘ, J. (2001), *Technická ochrana objektů, II. díl, Elektrické zabezpečovací systémy.* Praha: Policejní akademie České republiky v Praze, 2001. ISBN 80-7251-076-2
20. VANĚK, R. (2007), *Technologie digitálního snímání prstů*. Zlín: Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky. Bakalářská práce, 2007, 37s.
21. CARR, J., BROWN M. (2000), *Introduction to biometrical Equipment Technology, Fourth Edition*. New Jersey: Prentice Hall, 2000. ISBN 0-13-010492-2.

Literatura 6/9

22. FUJITSU LABORATORIES LTD. Fujitsu Laboratories Develops Real-Time Pulse Monitor Using Facial Imaging. In: *FUJITSU*[online]. Kawasaki, 2013, 18.3.2013 [cit. 25.8.2013]. Dostupné z: http://www.fujitsu.com/global/news/pr/archives/month/2013/20130318-01.html
23. KARLSSON, M.(2012), *SAFE SECURITY MANAGEMENT SYSTEM: Situation awareness for enhanced security. In: SAAB* [online]. 2012 [cit. 25.8.2013]. Dostupné z: http://www.saabgroup.com/en/Civil-security/Prison-Security/Security-Management-Solutions/SAFE-Security-Management-System/

Literatura 7/9

24. POLIŠENSKÁ, V. (2013), *Profilování pachatelů trestných činů* [online]. 2013 [cit. 25.8.2013]. Dostupné z: http://www.mvcr.cz/clanek/profilovani-pachatelu-trestnych-cinu.aspx
25. ŠČUREK, R., MARŠÁLEK D. (2013). *Profilace cestujících jako bezpečnostní metoda na letištích* [online]. 2013 [cit. 25.8.2013]
26. WeCU Technologies Advances Airport Security [online]. *In: CARMON, Irin. Fast Company*. 2010 [cit. 26.8.2013]. Dostupné z: http://www.fastcompany.com/1659118/wecu-technologies-advances-airport-security
27. NEMESYSCO [online]. *Nemesysco: voice analysis technologies*. 2012 [cit. 26.8.2013]. Dostupné z: http://www.nemesysco.com/

Literatura 8/9

28. BEMOSA [online]. *Bemosa: Behaviour Mdelling for Security in Airports*. 2012 [cit.26.8.2013]. Dostupné z: http://www.bemosa.eu
29. VYTEJČKOVÁ. *Sledování a hodnocení fyziologických funkcí*. [online]. 2013 [cit. 25.8.2013]. Dostupné z: http://www.lf3.cuni.cz/opencms/export/sites/www.lf3.cuni.cz/cs/pracoviste/osetrovatelstvi/vyuka/studijni-materialy/CNSKOS1/studijni-materialy/Mxenx_a_hodnocenx_fyziologickxch_funkcx.pdf
30. AXIS COMMUNICATIONS [online]. *AXIS Communications*, 2013 [cit. 27.8.2013]. Dostupné z: http://www.axis.com/

Literatura 9/9

31. ANISHCHENKO, L.. D'YACHENKO,A.(2013), *The experiment "BIORASCAN": Remote measurements of breathing parameters* [online]. Mars500 [cit. 26.8.2013]. Dostupné z: http://mars500.imbp.ru/en/520_sci_experiments/520_bioraskan.html
32. HAZELTON, L.(2008), *MailOnline* [online]. 2008 [cit. 26.8.2013]. Dostupné z: http://www.dailymail.co.uk/sciencetech/article-1060972/The-airport-security-scanner-read-mind.html
33. CHUMCHAL T. (2013), *Zajištění bezpečnosti na letišti pomocí profilace a identifikace osob*, Ostrava: VŠB – TUO, Fakulta bezpečnostního inženýrství, Diplomová práce, 2013.