POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminalistiky

Biometrie v elektronických zabezpečovacích a přístupových systémech

Diplomová práce

Biometrics in Electronic Security and Access Systems

Diploma thesis

VEDOUCÍ PRÁCE

doc. Ing. Jiří JONÁK, Ph.D.

AUTOR PRÁCE

Bc. Martin ČERVENÝ

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Plzni, dne 3. 3. 2022

Bc. Martin ČERVENÝ

Poděkování

Děkuji svému vedoucímu diplomové práce doc. Ing. Jiřímu Jonákovi, Ph.D. za poskytnutou pomoc, odborné rady a věcné připomínky, které mi poskytl v průběhu psaní této práce. Také bych chtěl poděkovat své rodině za podporu po dobu celého studia.

ANOTACE

Diplomová práce se zabývá možnostmi využití biometrie v aplikacích zajišťujících přístup a zabezpečení budov. Součástí diplomové práce je také historický exkurz do vývoje biometrie a její užití na poli osobní identifikace a autentizace. Jednotlivé kapitoly teoretické části jsou věnovány konkrétním biometrikám se zaměřením na metody snímání a zpracování biometrických dat. U těchto, je vždy detailně popsána jejich funkce a fyzikální princip, který využívají pro svoji činnost. Součástí diplomové práce je též shrnutí aktuálních technických norem a zejména právního rámce upravujícího užití biometrických systémů. V praktické části této práce jsou prezentovány výsledky provedeného výzkumu, jež byl zaměřen na vnímání hlavních aspektů biometrické autentizace s následným zapracováním do modelového projektu.

KLÍČOVÁ SLOVA

biometrie * identifikace * verifikace * FRR * FAR * biometrická šablona * identifikátor * biometrika * autentizace *

ANNOTATION

The diploma thesis deals with the possibilities of using biometrics in applications providing access and security of buildings. The diploma thesis also includes a historical excursion into the development of biometrics and its use in the field of personal identification and authentication. The individual chapters of the theoretical part are devoted to specific biometrics with a focus on methods of scanning and processing biometric data. For these, their function and the physical principle they use for their activities are always described in detail. The diploma thesis also includes a summary of current technical standards and especially the legal framework governing the use of biometric systems. The practical part of this work presents the results of the research, which was focused on the perception of the main aspects of biometric authentication with subsequent incorporation into the model project.

KEYWORDS

biometrics * identification * verification * FRR * FAR * biometric template * identifier * biometry * authentication

ÚVOD

Již od nepaměti měli lidé potřebu chránit svůj majetek, pro tyto účely své cennosti a důležité dokumenty uchovávali takovým způsobem, aby k nim byl umožněn přístup pouze jim, nebo oprávněným osobám. Po celá staletí se pro tyto účely využívalo především mechanického způsobu zabezpečení, doplněného fyzickou ochranou, kde pro identifikaci byla zpravidla využívána pouze osobní znalost "oprávněné osoby" příslušným strážným vykonávajícím službu. Až poslední dekády vnesly do odvětví bezpečnostních systémů a možnosti identifikace jednotlivce značný posun díky širokému rozšíření elektroniky a počítačů. Fenoménem posledních několika let je identifikace a autentizace na základě využití biometrických identifikátorů.

Biometrický identifikátor lze definovat jako unikátní rys nebo rysy jedince, podle kterých je možné s větší či menší přesností (dle použité technologie) danou osobu odlišit od ostatních a tím ji identifikovat. Z toho je zřejmé, že pro využití biometrické identifikace je možné využít pouze ty markanty, které jsou v čase relativně neměnné a zároveň unikátní, jedinečné, charakteristické pro každého jedince. Důležitým požadavkem je též podmínka, že sledovaný biometrický údaj musí existovat u všech jedinců ve společnosti což v rámci biometrie představuje tzv. "univerzalita". Pro představu lze uvést biometriky jako je otisk prstu, obličej, DNA.

Biometrická identifikace zažívá v poslední dekádě obrovský rozmach, v současnosti je využívána od státních institucí až po jednotlivé soukromé osoby. Aplikace, které zpracovávají biometrické údaje najdeme ve státních institucích jako je kupříkladu policie, která biometrii využívá v kriminalistické a trestně právní rovině při odhalování a evidenci pachatelů trestné činnosti, popřípadě při kontrolách osob, které disponují pasy či občanskými průkazy s uloženými biometrickými údaji. Dále také v čistě komerčních aplikacích jako součást docházkových a přístupových systémů a systémů zabezpečení budov. V neposlední řadě je především biometrická verifikace hojně využívána pro čistě soukromé využití zejména při autorizaci přístupu do osobních počítačů a mobilních telefonů, popřípadě přístupu do jednotlivých aplikací jako

např. mobilní bankovnictví, trezor na hesla atp. Možnosti využití identifikace a autentizace pomocí biometrie jsou tak velmi široké a pro jednotlivé uživatele velmi přátelské. Důvod je zcela zřejmý, a tím je absence potřeby vymýšlení a pamatování si složitých hesel, případně držení a užívání jiného doplňujícího identifikátoru tzv. tokenu, kterým může být např. RF čip, nebo čipová karta umožňující přístup. Nehrozí ani nezanedbatelné riziko ztráty nebo poškození takového identifikátoru, které by uživateli znemožnilo autentizaci. Zkrátka biometrický identifikátor je vždy s uživatelem, je totiž jeho součástí.

Cílem této diplomové práce je v rámci teoretické části představení biometrické identifikace včetně její historie, detailní rozbor nejrozšířenějších druhů biometrik. Dále rozebrání jednotlivých technologií pracujících s biometrickou identifikací a verifikací se zaměřením na jejich případné výhody, nevýhody a možnosti jejich využití. V neposlední řadě také stručný souhrn právního rámce, který se problematiky biometrie a zpracování biometrických dat dotýká. Součástí práce je též zohlednění rizik spojených s biometrií, spolehlivost jednotlivých technologií, její měření a též možnosti a rizika zneužití biometrických identifikátorů.

Praktická část této diplomové práce je rozdělena do dvou částí, z nichž první představuje dotazníkové šetření. Cílem šetření bylo zjistit všeobecné povědomí o biometrii a společenské ochotě poskytnout svá biometrická data pro využití v rámci automatizovaných systémů. V druhé části jsou veškeré poznatky načerpané při zpracovávání této diplomové práce promítnuty do vlastního návrhu modelu zabezpečení budovy s maximálním využitím prvků pracujících na principech biometrické identifikace dle zadání diplomové práce. Přičemž byl též zohledněn výsledek provedeného dotazníkového šetření, který typ biometrického identifikátoru uživatelé spatřují jako uživatelsky nejpřívětivější a ve kterých aplikacích by upřednostnili použití biometrie namísto jiného identifikátoru.

Vzhledem k rozsahu práce však není možné provést zcela vyčerpávající popis veškerých dostupných prvků a technologií využívajících biometrii při zabezpečování budov a majetku. Z těchto důvodů jsem vybral pouze vhodné zástupce u jednotlivých technologií a systémů, na kterých jsem se pokusil demonstrovat jejich účel a vhodnost využití.

I TEORETICKÁ ČÁST

1 HISTORICKÝ VÝVOJ BIOMETRICKÉ IDENTIFIKACE

Samotný pojem biometrie vychází ze složení řeckých slov “bio“ (život) a “metrics“ (měřit). Biometrií tedy rozumíme vědu zabývající se měřitelnými charakteristikami člověka. Přestože moderní pojetí biometrie je úzce spjato s elektronickými systémy a počítači, její základní principy sahají do dávné minulosti. Již od pradávna se pro identifikaci mezi lidmi používá zejména vzhled tváře, případně tón a barva hlasu, nebo styl držení těla a lokomoce chůze. Avšak v tomto případě nelze hovořit o systému, ale pouze o jistých markantech, díky kterým lze vzájemně rozlišit jedince mezi sebou navzájem.

Mezi jedny z prvních uživatelů biometrické identifikace patřili staří Egypťané, kteří zejména při stavbách monumentálních stavebních děl, kterými byly např. pyramidy, potřebovali rozpoznat z ohromného množství pracovníků jednotlivé osoby z důvodů evidence vyplacené mzdy a zamezení jejímu vícenásobnému vyplacení. Pro tyto účely jim sloužily evidence, které obsahovaly detailní popsatelné a měřitelné vnější markanty jednotlivých pracovníků. Záznamy obsahovaly například jizvy po zranění, barvu očí a kůže, popřípadě velikost částí těla nebo hmotnost osoby.

Jiný druh biometrické identifikace, jejíž potenciál byl naplno objeven až o mnoho staletí později, používali Babyloňané, Peršané a též staří Číňané. Na těchto územích archeologické nálezy objevily předměty, které dokládají použití identifikace prostřednictvím otisků palce ruky či takových vtisků do hliněných destiček.

1.1 Identifikace podle měření částí těla – Bertillonáž

Exaktní základy, a především obrovský potenciál biometrické identifikace byl však postupně objevován teprve od druhé poloviny 19. stol. až do současnosti. Prvními průkopníky, kteří zasvětili svůj život výzkumu biometrické identifikace, byli lidé z lékařského, soudně-lékařského, a kriminalistického prostředí.

Mezi hlavní představitele průkopníků biometrické identifikace nepochybně patří Alphonse Bertillon, který se nesmazatelně zapsal do historie svojí antropometrií, která později vešla ve známost jako bertillonáž. Podstatou

bertillonáže bylo měření a evidence zprvu 14 a poté pouze 11 částí lidského těla, které se přibližně od dvacátého roku života dále v průběhu zbytku života u dospělého jedince nemění. Bertillonáž pracovala s teorií, že je vysoce nepravděpodobné, aby se u dvou či více osob naměřené hodnoty ve všech 14 resp. 11 parametrech shodovaly. V případě bertillonáže byla matematická pravděpodobnost shody vypočtena na 1:4.191.304.[1] Praktické využití našla bertillonáž zejména v kriminalistice při identifikaci recidivistů a později též při identifikaci neznámých mrtvol, u kterých se předpokládala kriminální minulost, a tudíž pravděpodobnost jejich předchozího zanesení do evidence.

1.2 Identifikace podle otisků prstů ruky – Daktyloskopie

Ač se bertillonáž v praxi osvědčila, její praktické využívání poměrně záhy ukončil na přelomu 19. a 20. století celosvětový nástup nové sofistikovanější metody biometrické identifikace, kterou byla daktyloskopie.

Daktyloskopie představuje výrazně propracovanější a násobně přesnější metodu biometrické identifikace, na kterou začátkem 20. století přešly postupně všechny země, které do té doby stále uznávaly a používaly bertillonáž. Na položení exaktních základů moderní daktyloskopie se výraznou měrou zasloužil český lékař J. E. Purkyně, který na základě svých výzkumů klasifikoval 9 základních vzorů obrazců papilárních linií. Přestože jeho výzkum byl primárně vědecko-medicínského charakteru, jeho výsledky byly nadále rozpracovány řadou vědců a učenců, kteří v otiscích papilárních linií spatřovali potenciál zejména na poli kriminalistické identifikace.

Nezávisle se problematikou možnosti identifikace podle otisků papilárních linií intenzivně zabýval také W. J. Herschel, který se v průběhu svého působení ve funkci guvernéra indické bengálské provincie potýkal s potřebou identifikace velkého množství osob, které neuměly číst ani psát, a navíc díky odlišné etnicitě byli pro Evropana mezi sebou vzájemně těžko rozeznatelní. Z toho důvodu pro stvrzení přijetí hotovosti při výplatě mezd a důchodů začal používat

[1] Kriminalistika.eu: Bertilone [online]. [cit. 24.09.2021]. Dostupné z: https://www.kriminalistika.eu/muzeumzla/bertilon/bertilon.html

jako identifikátor právě otisk prstu palce ruky, čímž vyloučil duplicitní výplaty mezd, případně výplaty důchodů již zesnulým osobám.

Léty shromažďovaný materiál W. J. Herschlem posloužil jako základ vystudovanému lékaři a antropologovi F. Galtonovi, který své čtyřleté bádání shrnul v díle *Fingerprints* a stanovil čtyři základní vzory otisků prstů.[2] V roce 1880 *Francis Galton a policejní inspektor Edward Henry položili základy praktického využívání daktyloskopie tím, že vytvořili třídící a registrační systémy využitelné v praxi.*[3]

Obrázek 1 – J. Vucetich – úplná sada otisků prstů [Zdroj: 37]

Ovšem samotný název daktyloskopie pro tuto identifikační metodu zavedl až Argentinec Juan Vucetich, který se též značnou měrou zasloužil o propagaci a praktické rozšíření daktyloskopické identifikace. J. Vucetich působil na pozici policejního úředníka na policejním úřadě zabývajícím se identifikací a statistikou v argentinském La Plata. Jeho hlavním inspirátorem se stal F. Galton a jeho výzkum, který J. Vucetich uvedl do praxe a postupně vytvořil funkční systém pro identifikaci pouze na základě tzv. úplné sady otisků prstů (pozn. Otisk všech 10 prstů) viz. (obr. 1), čímž zcela vyloučil nutnost identifikace pomocí složitého a časově náročného měření částí těla, kterou představovala bertillonáž. Na základě výsledků jeho výzkumu byl dokonce roku 1900 zaveden nový osobní

[2] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5, str. 159–161.
[3] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5, str. 91.

dokument pro občany Argentinské republiky, který obsahoval mimo do té doby běžných údajů, též otisk prstu.[4]

1.3 Identifikace podle oční duhovky

V průběhu následujících tří desetiletí se na poli biometrické identifikace nic převratného neudálo. Až v roce 1936 přichází s novým poznatkem oční lékař F. Burch. Burch při své práci oftalmologa zjistil, že pro identifikaci osob by bylo možné obdobně jako otisk prstu využít také oční duhovku, jejíž barva a struktura je u každého člověka též zcela unikátní. Avšak jeho zjištění zůstalo spíše pouhým konceptem. Jeho myšlenku rozvedli až oftalmologové L. Flam a A. Safir, kteří si svůj objev identifikace osob pomocí oční duhovky nechali v roce 1987 patentovat. Tato identifikační metoda biometrické identifikace patří v současnosti mezi nejpřesnější a výrazně předčí i identifikaci na základě otisků prstů.

Do praxe ji uvedli společně L. Flam, A. Safir a J. Daugman, který si v roce 1994 nechal patentovat algoritmus umožňující automatickou identifikaci prostřednictvím snímání oční duhovky. Následující rok byl dokončen první komerční identifikační systém pracující na skenu oční duhovky, který vznikl za spolupráce Defense Nuclear Agency a Iriscan. [5]

1.4 Identifikace podle obličeje

Nové možnosti v oblasti techniky, elektroniky a počítačovém zpracování informací umožnily od 60. let 20. století rychlý vývoj biometrické identifikace. Lídrem ve vývoji a jeho financování v oblasti biometrické identifikace se stávají USA. Na objednávku vlády USA v období mezi roky 1964–1966 W. W. Bledsoe a H. Chan vyvíjejí první poloautomatický systém na rozpoznání obličeje. Přestože systém byl funkční, do praktického využití měl ještě daleko. Jako největší úskalí se ukázala být značná variabilita tvaru hlavy, komplikace s úhlem jejího snímání a dále také úhel a intenzita dopadajícího světla, které značně

[4] Visible proofs: Forensic Views of the Body: Galleries: Biographies: Juan Vucetich (1858–1925) [online]. [cit. 24.09.2021]. Dostupné z: https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/vucetich.html
[5] Explainer: Iris Recognition | Biometric Update [cit. 25.09.2021]. Dostupné z: https://www.biometricupdate.com/201206/explainer-iris-recognition

komplikovali úspěšnost identifikace.[6] Na poznatky Bledsoova týmu navázali v 70. letech A. J. Goldstein, L. D. Harmon a A. B. Lesk, kteří pro umožnění automatizace zpracování stanovili 21 markerů (barva vlasů, velikost uší, velikost rtů atp.).

Značný pokrok a možnost identifikace v reálném čase pomocí automatické detekce obličeje přichází až v roce 1991 díky výzkumu M. Turka a A. Pentlanda, kteří za užití vlastních vektorů a kovariačních matic umožnili počítačové zpracování snímaného obrazu. Plně automatický systém byl v praxi poprvé použit při Super Bowl v Tampě 2001.[7]

1.5 Identifikace podle hlasu

Doposud všechny představené možnosti biometrické identifikace pracují s informacemi, které jsou nějakým způsobem pozorovatelné a hodnotitelné na základě viditelných stop. Změna v tomto ohledu přichází v roce 1960 s konceptem G. Fanta. Profesor Fant působící na Švédském královském institutu představil možnost identifikace osoby pouze podle hlasového projevu. Na možnosti identifikace mluvčího podle hlasového projevu v té době pracoval mimo jiných i český fonetik P. Janota, bohužel bez zásadního dopadu na odbornou veřejnost.

S využitím hlasu pro účely policejní identifikace jako první přišel v roce 1962 L. G. Kersta, který převedl hlas do grafické podoby tzv. sonagramu a tvrdil, že je možné díky specifickým charakteristikám hlasového projevu identifikovat osobu obdobně jako prostřednictvím otisků prstů. Proti sonagramu a jeho použití jako identifikačního důkazu narůstala na přelomu 60. a 70. let kritika, jejíž oprávněnost potvrdil experiment K. N. Stevense a kol., který dokázal, že chybovost v případě sluchového hodnocení byla pouhých 6 %, zatímco chybovost vyhodnocení sonagramu činila 21 %. Další výzkum ukázal vhodnost užití kombinace obou metod současně. Nicméně díky značné variabilitě faktorů ovlivňujících hlasový projev (fyzické změny, stárnutí, nemoci či psychické

[6] Woodrow Bledsoe Originates of Automated Facial Recognition: History of Information [online]. [cit. 25.09.2021]. Dostupné z: https://www.historyofinformation.com/detail.php?entryid=2495
[7] History of Biometrics | Biometric Update [online]. [cit. 25.09.2021]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

rozpoložení mluvčího) není prozatím možné získat absolutní jistotu v identifikaci konkrétní osoby prostřednictvím hlasové identifikace oproti např. otiskům prstů.[8]

2 BIOMETRICKÁ IDENTITA, IDENTIFIKACE A VERIFIKACE

2.1 Biometrická identita

Každý člověk vykazuje navenek určité, pro něj charakteristické rysy. Může se jednat o čistě vizuální statické charakteristiky, jako je výška, tvar postavy, délka vlasů, barva očí atp., nebo též specifické chování a projevy ve vnějším světě, mající určitou dynamiku. Jako příklad dynamického projevu ve vnějším světě lze uvést lokomoci chůze, dynamiku úhozů při psaní na počítačové klávesnici či dynamiku podpisu. Souhrn všech těchto specifických charakteristik tvoří dohromady biometrickou identitu jedince. Právě na základě těchto konkrétních odlišností, je možné díky biometrii odlišit „identifikovat" jedince mezi ostatními. Případně lze prostřednictvím biometrie potvrdit „verifikovat", že kupříkladu osoba vstupující do chráněného objektu, je osobou s patřičným právem vstupu.

2.2 Biometrická identifikace

Biometrická identifikace je v současné době velmi rychle se rozvíjející obor, který našel své uplatnění zejména po teroristických útocích na USA v roce 2001. Celosvětově nově zaváděná bezpečnostní opatření vyžadovala potřebu kontroly obrovského množství osob v krátkém čase a často též s požadavkem, aby toto bylo provedeno bez povědomí kontrolovaných osob.

Principem biometrické identifikace je porovnávání uložené biometrické identity (šablony) s množstvím všech ostatních identit (vzorků), které jsou snímány na vstupu. Vstup v takovém případě představuje technický prvek, který snímá biometrické údaje osob a posílá je k následnému vyhodnocení. Systém průběžně analyzuje data a při určité předem definované procentuální shodě šablony a vzorce vyhodnotí možnou shodu a tím identifikuje hledaného. Tento způsob lze využít např. na letištích, fotbalových stadionech, nákupních centrech a dalších místech s velkým počtem osob.

---

[8] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5, str. 455–459.

Pro umožnění automatického a efektivního nasazení biometrické identifikace je zcela klíčové, aby jednotlivé sledované charakteristiky vykazovaly:

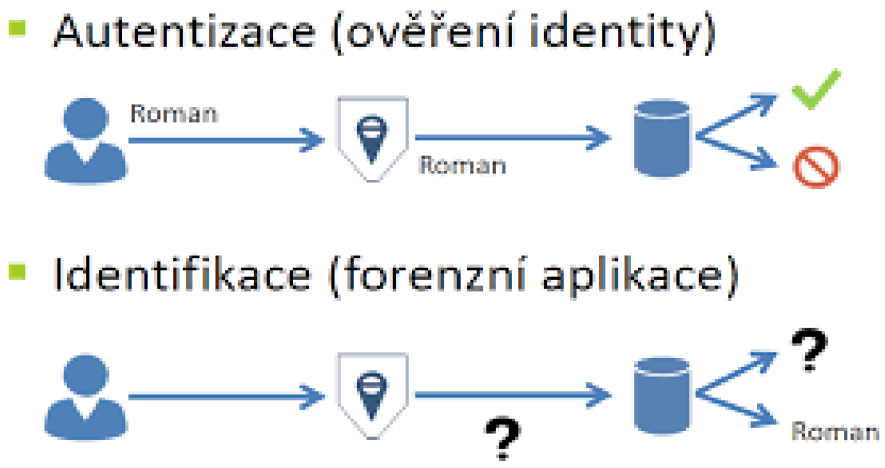
- **Univerzalitu** – charakteristika je obsažena u všech jedinců v populaci
- **Jedinečnost** – žádné dvě charakteristiky nejsou shodné či mezi sebou vzájemně zaměnitelné
- **Trvalost** – biometrická charakteristika musí být v čase neměnná nebo alespoň v hlavních rysech neměnná
- **Měřitelnost** – jednotlivé identifikační charakteristiky lze exaktně získat
- **Uchovatelnost** – získané charakteristiky lze bez ztráty informační hodnoty dále uchovat pro další zpracování
- **Akceptace** – existence společenského konsenzu na sběr a zpracování těchto biometrických charakteristik

2.3 Biometrická verifikace

Zatímco biometrickou identifikaci využívají především vládní agentury a státní bezpečnostní instituce, tak verifikace prostřednictvím biometrické identity je v současnosti doménou komerčních aplikací (obr. 2) a stala se v průběhu doslova pár let naprosto běžnou součástí našich každodenních životů.

Verifikace nebo též autentizace představuje proces, při kterém se porovnává shoda uložené biometrické identity (šablony) s jednou konkrétní snímanou identitou (vzorkem), který je zachycen snímačem na vstupu do systému. Kontroluje se míra podobnosti či shody snímaného vzorku s uloženou šablonou. V případě dosažení předdefinované podobnosti dochází ke kladné vazbě a tím zpřístupnění dalšího kroku nebo popř. umožnění vstupu atp.

V opačném případě, pokud se referenční vzorek se snímaným neshodují, je uživatel odmítnut.



Obrázek 2 – Identifikace vs. Autentizace [Zdroj: 22]

3 SPOLEHLIVOST A BEZPEČNOST BIOMETRIE

Biometrická identifikace a verifikace patří mezi nejbezpečnější identifikační metody. Ale, jak již bylo uvedeno, možností identifikace podle biometrických markantů je mnoho, a s tím souvisí i fakt, že ne všechny způsoby identifikace pomocí biometrie jsou stejně spolehlivé a přesné. Opak je pravdou, každá biometrická metoda ověření vykazuje odlišnou rozlišovací sílu tzv. "biometrickou entropii". Biometrická entropie nám určuje, jak velká by musela být populace, aby vznikla pravděpodobnost, že se v jeden okamžik vyskytnou dva vzorce nesoucí identickou biometrickou informaci. Vše je tedy odvislé od faktu, kolik jsme schopni jednotlivými metodami biometrie získat informací z konkrétního biometrického nosiče. Čím více dat získáme, tím je možnost identifikace přesnější a jsme schopni uplatnit tuto metodu na obrovské množství jedinců s vysokou mírou přesnosti. Pro představu lze uvést příklad nejpoužívanější metody biometrického ověření prostřednictvím otisku prstu, kde se reálná rozlišovací schopnost pohybuje v intervalu $5{,}3 \times 10^{36}$ – $1{,}9 \times 10^{53}$.[9] Při aktuálním počtu lidí

[9] PAVLÍK, Pavel. (2007), *Biometrie jako základ současné i budoucí identifikace a autentizace*. [online]. Kontakt, roč. 9, je 2, s. 427–430. [cit. 25.09.2021]. Dostupné z: https://kont.zsf.jcu.cz/pdfs/knt/2007/02/34.pdf

žijících na planetě cca $7,7x10^9$ je tedy tato metoda biometrické identifikace zcela dostačující pro praktické využití a spolehlivé určení konkrétního jednotlivce.

Mezi metody biometrické identifikace s nejvyšší mírou přesnosti patří například metoda identifikace pomocí DNA či identifikace pomocí oční duhovky. Co se týče DNA, jde o metodu velmi zdlouhavou a náročnou jak na použité prostředky, tak zejména vysoce erudovaný personál. Tato metoda biometrické identifikace má ovšem jistá úskalí, která představují případy, kde je zapotřebí identifikace jednovaječných dvojčat. V takových případech je metoda identifikace pomocí DNA neproveditelná. Z praktického hlediska se tedy v místech, kde je zapotřebí vysoká míra zabezpečení, jeví vhodnější metoda identifikace pomocí oční duhovky. Tato metoda biometrické identifikace je stejně rychlá a snadná jako kupříkladu metoda, kde je využíván otisk prstu, ovšem přináší nám ještě o poznání vyšší míru přesnosti. Díky její rozlišovací schopnosti, která se pohybuje na hranici těžko představitelných $3,2x10^{616}$, je případná záměna dvou jedinců vyloučena. Toto platí i u již zmíněných jednovaječných dvojčat.

Na druhém konci pomyslné škály přesnosti a spolehlivosti biometrické identifikace jsou metody identifikace podle hlasu, podpisu, nebo poměrně hojně využívané metody tzv. “Face ID“, tedy identifikace dle skenu obličeje. Jako příklad si můžeme uvést společnost Apple, která tuto technologii jako první zabudovala do svých mobilních telefonů a deklarovala u ní rozlišovací schopnost $1x10^6$.

V rámci biometrické identifikace je možné zpracovávat nejen statické nosiče biometrických dat, jako jsou otisk prstu, otisk dlaně, oční duhovka, oční sítnice, tvar ušního boltce, dentální obraz a další, ale také chování, představující tzv. “dynamické vzorce“. Dynamickým vzorcem rozumíme zachycení určitého pohybového stereotypu, pomocí kterého jsme schopni rozlišit osoby jednu od druhé. Mezi dynamické vzorce je možné zařadit dynamiku stisků kláves na počítačové klávesnici, obličejovou mimiku, bipedální lokomoci, hlas, dynamiku podpisu atd. Bližší představu o přesnosti a využitelnosti jednotlivých metod je možné vyčíst z přiložené tabulky č. 1.

Tabulka 1 – kritéria jednotlivých biometrik [Zdroj: 5]

biometrický prvek	univerzalita	jedinečnost	konstantnost	získatelnost	výkonnost	akceptace	bezpečnost	finance
obličej	vysoká	nízká	střední	vysoká	nízká	vysoká	nízká	nízké
otisk prstu	střední	vysoká	vysoká	střední	vysoká	střední	vysoká	nízké
geometrie ruky	střední	střední	střední	vysoká	střední	střední	střední	střední
žíly ruky	střední	střední	střední	střední	střední	střední	vysoká	střední
duhovka	vysoká	vysoká	vysoká	střední	vysoká	nízká	vysoká	vysoké
sítnice	vysoká	vysoká	střední	nízká	vysoká	nízká	vysoká	vysoké
podpis	nízká	nízká	nízká	vysoká	nízká	vysoká	nízká	nízké
hlas	střední	nízká	nízká	střední	nízká	vysoká	nízká	nízké
termogram	vysoká	vysoká	nízká	vysoká	střední	vysoká	vysoká	vysoké

Stupeň bezpečnosti a spolehlivosti je bez ohledu na použitý druh sledované biometriky závislý mimo jiné na předdefinovaném systémovém nastavení. Díky principu, na kterém je biometrická identifikace založena, je důležité, aby byla vstupní snímaná data konkrétní osoby v ideálním případě při každém načtení identická s uloženou šablonou tohoto uživatele. Tento požadavek však zpravidla není možné v praxi splnit. Avšak aby i za těchto objektivních podmínek bylo možné takový systém v praxi efektivně použít, je třeba již při projektování systému definovat práh citlivosti daného systému. Pro tento účel se do hodnocení výkonnosti biometrických systémů zavedly hodnoty FRR a FAR.

3.1 Pravděpodobnost chybného odmítnutí – FRR

Pravděpodobnost chybného odmítnutí (zkráceně FRR z anglického False Rejecting Rate), označovaná některou literaturou také jako chyba I. typu, definuje míru pravděpodobnosti, při které bude oprávněný uživatel chybně odmítnut. Přesto, že biometrická šablona je v systému řádně uložena, její shoda s načteným biometrickým nosičem oprávněného uživatele nepřekročila nastavenou mez pro úspěšné ověření. Důvodem pro takové odmítnutí může být mnoho faktorů. V případě nejpoužívanější metody biometrické identifikace dle otisků prstů může tato situace nastat vlivem přiložení pouze části prstu,

přiložením pod výrazně jiným úhlem, po úrazu nebo vlivem značného zašpinění kůže atp.

Z bezpečnostního hlediska se FRR nejeví jako problematické, spíše naopak. Ovšem zvýšené hodnoty FRR mohou zapříčinit značně nekomfortní uživatelské prostředí vlivem častého odmítání oprávněných uživatelů, kteří musí pro ověření své identity absolvovat více pokusů, popřípadě nejsou vůbec rozpoznáni. V praxi je tedy vhodné pro správně fungující a uživatelsky komfortní sytém mít hodnotu FRR na co nejnižší úrovni. Pravděpodobnost FRR můžeme definovat vzorcem:

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

kde:

N_{FR} *– Number of False Rejection (počet chybných odmítnutí)*

N_{EIA} *– Number of Enrolle Identification Attemps (počet pokusů oprávněných osob o odentifikaci)*

N_{EVA} *– Number of Enrolle Verification Attemps (počet pokusů oprávněných osob o verifikaci)*[10]

3.2 Pravděpodobnost chybného přijetí – FAR

Pravděpodobnost chybného přijetí (zkráceně FAR z anglického (False Acceptance Rate), někde též označována jako chyba II. typu, definuje pravděpodobnost toho, že bude systémem akceptován biometrický vzorek z nosiče, který není uložen jako šablona v systému. Tím hrozí riziko, že systém tzv. „selže“ a umožní přístup neoprávněné osobě. Pravděpodobnost chybného přijetí je na rozdíl od pravděpodobnosti chybného odmítnutí zcela zásadní pro vznik tzv. „bezpečnostního incidentu“ a ohrožení zájmů, informací, případně prostor, které má systém chránit. Z pohledu bezpečnosti je tedy zřejmé, že čím vyšší je hodnota FAR, tím je systém méně bezpečný pro možné náhodné,

[10] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5, str. 138

popřípadě záměrné zpřístupnění neoprávněné osobě. Pravděpodobnost FAR můžeme definovat vzorcem:

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

kde:

N_{FA} *– Number of False Acceptance (počet chybných přijetí)*

N_{IIA} *– Number of Impostor Identification Attemps (počet pokusů neoprávněných osob o odentifikaci)*

N_{IVA} *– Number of Impostor Verification Attemps (počet pokusů neoprávněných osob o verifikaci)*[11]

3.3 Vztah FRR x FAR

Z výše popsaného je zřejmé, že změny hodnot FRR a FAR mají zcela zásadní vliv na výslednou bezpečnost, spolehlivost a též uživatelskou přívětivost celého biometrického systému. V případě vyššího procenta metriky FRR bude systém stále bezpečný, ale již bude uživateli vnímán jako nespolehlivý, popř. obtěžující. Na druhou stranu, pokud bude systém vykazovat vyšší procento hodnoty FAR, stává se v podstatě nepoužitelným, neboť neplní řádně svoji funkci a představuje riziko bezpečnostní hrozby. Z toho vyplývá, že v ideálním případě by měly být obě metriky FRR i FAR na hodnotě 0, nebo se takové hodnotě co nejvíce přiblížit. Což ale bohužel není v reálné aplikaci realizovatelné.

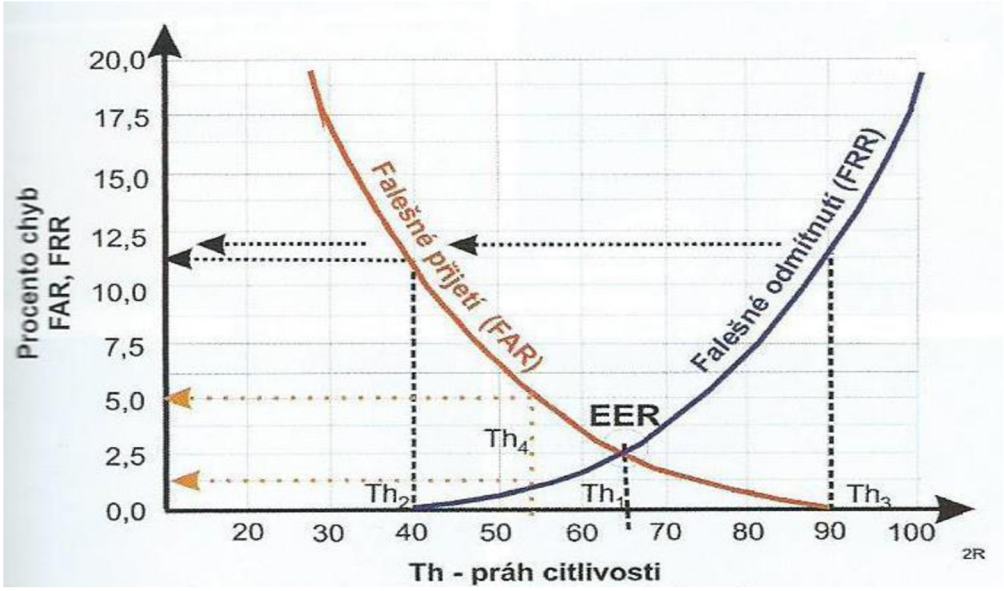
Navíc je zde vzájemná korelace obou hodnot a změna jedné hodnoty se projeví též na hodnotě druhé. To znamená, že bude-li požadavek na nižší hodnotu FAR z důvodu potřeby vyšší míry bezpečnosti, bude tím recipročně ovlivněna hodnota FRR, která v reakci na tento požadavek vzroste, čímž se oprávněným uživatelům zvýší pravděpodobnost, že budou systémem vyhodnoceni jako „neoprávněný uživatel“. Toto vzájemné působení lze znázornit na grafu

[11] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5, str. 139

prahové operační charakteristiky označované zkratkou ROC (z anglického Reciever Operating Characteristic), případně obdoby tzv. DET (z anglického Detection Error Trade – off) pomocí křivky. Mezi křivkami ROC a DET je rozdíl pouze v rozdílném zanesení bodů do grafu, jinak jsou obdobné.[12]

Případnou vhodnost, či vzájemné hodnocení dvou či více variant systémů lze určit z charakteru jednotlivých křivek zanesených do grafu. Pro vzájemné posouzení více variant je vhodné využít vymezení za pomoci tzv. ERR (z anglického Equal Error Rate).

ERR představuje průsečíkový bod na přímce procházející jednotlivými křivkami ROC, kde se FRR a FAR rovnají (nastane shoda chybné hodnoty). *V praxi se u FRR a FAR křivek jedná o diskrétní funkce, tj. přesné určení EER není možné.*[13] Bod EER představuje pouze vrchol množiny či hranici oblasti, kde budou míry FRR a FAR na shodné úrovni, tzn. nastavením prahu citlivosti na hodnotu EER zajistíme, že počet falešně přijatých uživatelů se bude rovnat počtu falešně omítnutých uživatelů. (obr. 3)



Obrázek 3 – graf závislosti FRR a FAR [Zdroj: 6]

[12] DRAHANSKÝ, Martin, ORSÁG, Filip. *Biometrie.* Brno: Computer Press, 2011, 294 s. ISBN 978-80-254-8979-6, str. 77–94
[13] DRAHANSKÝ, Martin, ORSÁG, Filip. *Biometrie.* Brno: Computer Press, 2011, 294 s. ISBN 978-80-254-8979-6, str. 87

Přesné nastavení prahu citlivosti pro jednotlivé aplikace je vysoce variabilní, závisí na hrozících rizicích, požadované míře bezpečnosti, uživatelské přívětivosti a obecném určení daného systému. Z uvedeného vyplývá, že např. požadavky kladené na biometrický systém, zajišťující kontrolu vstupu do komerčního objektu, budou diametrálně odlišné od požadavků a nastavení systému určeného k identifikaci hledaných osob na mezinárodním letišti.

3.4 Metriky IAR a SAR

Metriky IAR a SAR patří zejména do oblasti biometrických systémů určených pro verifikaci. Mimo výše popsaných FRR a FAR, které je nezbytné zohlednit u každého biometrického sytému, v posledních letech technologický gigant Google při vývoji operačního systému Android zavedl ještě IAR – Imposter Accept Rate, SAR – Spoof Accept Rate. Důvodem byla skutečnost, že žádná z metrik FRR a FAR při svém modelování nepočítá s možností cíleného útoku. Výsledné hodnoty FAR a FRR vycházejí pouze z modelu, který předpokládá ohrožení náhodným chybným přijetím či zamítnutím přístupu. Nově zavedené metriky tak mají sloužit k odhalení cíleného pokusu o napodobení biometrického vzorce oprávněného uživatele.

U metrik IAR a SAR je hodnota EER shodně nastavena na limit 7 % s možností budoucích úprav této hodnoty v závislosti na systémovém určení a zejména citlivosti senzorů. Avšak nejdůležitější je skutečnost, že po překročení této hranice je pro úspěšnou autentizaci požadován další autentizační prvek, kterým může být PIN, heslo, přiložení čipové karty aj. V závislosti na určení celého sytému je možné i zcela zablokovat uživatele a následné ověření přenést na fyzické potvrzení identity bezpečnostním administrátorem, který poté provede zpětnou aktivaci účtu uživatele. Obdobný požadavek je zpravidla systémy, které používají ověření pomocí biometrických identifikátorů, vyžadován v případech dlouhodobé neaktivity uživatele.[14]

[14] Android-developers.googleblog.com: *Better Biometrics in Android P.* [online]. [cit.2.10.2021]. Dostupné z: https://android-developers.googleblog.com/2018/06/better-biometrics-in-android-p.html

3.5 Ochrana identity

V případě biometrie je ochrana identity zcela klíčová, neboť na rozdíl od ostatních identifikátorů, které mohou představovat ID karty, tokeny, PIN apod. mají případné dopady při jejím odcizení dalekosáhlé až nevratné následky. Nespornou výhodou je skutečnost, že biometrický identifikátor nelze ztratit či zapomenout, neboť v případě biometrické identity představuje identifikátor sám sobě konkrétní jedinec. S tím souvisí skutečnost, že při odcizení biometrické identity není možné jednoduše zablokovat odcizený identifikátor a vystavit či vygenerovat uživateli jiný, jak by to bylo možné v případě jiného způsobu identifikace či spíše autentizace.

V případě ztráty, resp. odcizení, neboť ztráta biometrického identifikátoru je vyjma fatálních úrazů v podstatě nemožná, přichází uživatel ve své podstatě o své já a o možnost prokázat svoji existenci sebou samotným. Při hlubším zamyšlení je zjevné, že následky takové ztráty jsou nedozírné, neboť v jeden okamžik může takto napadená, resp. poškozená osoba přijít od velmi cenných osobních údajů přes finanční prostředky, kompletní přístup k digitalizované státní správě až po přístup do bytu v případě použitých biometrických zámků, které jsou zakomponovány do systému on-line chytré domácnosti. Je tedy zcela na místě věnovat zabezpečení a ochraně biometrické identity při jejím využití enormní pozornost.

Odcizení biometrické identity může být realizováno vícero způsoby, které představují v prvém případě fyzické napodobení biometrického identifikátoru uživatele. Vzhledem k vývoji na poli biometrických senzorů a systémů je stále obtížnější úspěšně aplikovat napodobeninu biometrického identifikátoru, např. fotkou či modelem ruky. Ovšem výrazně rizikovější a pro útočníky v mnohých aplikacích snazší je získání celých databází či zkopírování již digitalizovaných šablon biometrických identifikátorů z nedostatečně zabezpečených systémů či jednotlivých prvků těchto systémů. Pro názornost lze uvést obří únik z webové platformy BioStar 2, která představuje on-line rozhraní systému inteligentních zámků, pracujících na základě biometrické identifikace. Bezpečnostní audit u této společnosti odhalil volně dostupné databáze biometrických identifikátorů přibližně 27,8 milionu uživatelů z 5700

organizací, působících v 83 státech.[15] Databáze obsahovaly jak otisky prstů, tak záznamy pro identifikaci pomocí rozpoznání obličeje v originálu, namísto toho, aby byly zabezpečeny pomocí tzv. hashování (hash je matematický algoritmus pro převod vstupních dat do jakéhosi otisku v podobě krátké číselné řady).

3.6 Technické normy a standardy

Základem pro aplikaci každé nové technologie a její použití v praxi je zavedení určité normy, která stanoví technické a bezpečnostní standardy pro danou technologii. Zároveň je díky standardizaci umožněna případná vzájemná kompatibilita prvků různých výrobců mezi sebou v jednom systému bez nežádoucích komplikací, tzv. interoperabilita. Vzhledem k variabilitě biometrické identifikace a autentizace je zřejmé, že rozsah norem bude poměrně obsáhlý, neboť je třeba pokrýt širokou technologickou a právní škálu, které se problematika dotýká.

Dalším aspektem jsou rozdílná technická, právní a etická specifika, která si určují jednotlivé země při vytváření vlastních norem pro nové technologie. Mezi dvě hlavní mezinárodní organizace, zabývající se standardy, patří ISO/IEC a ANSI/INCITS, kde druhá zmíněná určuje normy především pro oblasti severní Ameriky.

Zde uvádím pouze stěžejní normy, které vycházejí ze standardů ISO/IEC, a které jsou aplikovány na území EU. Jejich aplikace je realizována buď přímo v rámci směrnic a nařízení vydávaných unijními orgány, nebo prostřednictvím zapracování (inkorporace) do norem vydávaných jednotlivými zeměmi na národní úrovni. Pro oblast informačních technologií byla ISO/IEC zřízena komise JTC 1 (Join Technical Committee), která má řadu podkomisí označených SC (Sub-Committee), přičemž oblast standardů pro biometrii zpracovává konkrétně podkomise označená SC 37 *Biometrics.*

[15] SystemOnLine.cz: S přehledem ve světě informačních technologií [online]. [cit.10.10.2021]. Dostupné z: https://m.systemonline.cz/it-security/je-zpracovavani-biometrickych-dat-bezpecne.htm

Normy převzaté ISO/IEC a aplikované v ČR:

- ČSN ISO/IEC 2382-37 *Informační technologie – Slovník – Část 37: Biometrika*
- ČSN ISO/IEC 19785-2 *Informační technologie – Společný rámec formátů biometrické výměny – Část 2: Postupy pro činnost biometrické registrační autority*
- ČSN ISO/IEC 19785-4 *Informační technologie – Společný rámec formátů biometrické výměny – Část 4: Specifikace formátu bezpečnostního bloku*
- ČSN ISO/IEC 19794 *Informační technologie – Formáty výměny biometrických dat* (zahrnuje 14 samostatných norem)
- ČSN ISO/IEC 19795 *Informační technologie – Testování a hodnocení biometrik* (zahrnuje 5 samostatných norem na testování biometrik)
- ČSN ISO/IEC 30107 *Informační technologie – Detekce biometrického prezentačního útoku* (zahrnuje 3 samostatné normy)

3.7 Právní aspekty biometrické identifikace

Biometrické systémy, jak již bylo částečně nastíněno v první kapitole, v posledních letech doznaly značného rozmachu a lze konstatovat, že do jisté míry předběhly platnou legislativu. Vzhledem ke skutečnosti, že biometrické údaje jsou považovány za citlivé osobní údaje, dochází při jejich pořizování, uchovávání a zpracování neodmyslitelně k zásahům do základních lidských práv. Z uvedeného vyplývá, že právní rámec upravující problematiku biometrické identifikace se dotýká mimo jiné i právních předpisů nejvyšší právní síly, neboť základní lidská práva a jejich ochrana jsou zakotveny v základních právních předpisech jak na evropské, tak na národní úrovni.

V České republice ochrana základních lidských práv vychází primárně z ústavního pořádku České republiky a díky našemu členství v EU také z právních předpisů EU spadajících do tzv. Evropského acquis. Stěžejním právním předpisem v případě ochrany základních práv a svobod je zákon č. 2/1993 Sb., Listina základních práv a svobod. Ochrana osobnosti je v Listině upravena

zejména v čl. 7 odst. 1 a čl. 10 odst. 2 a 3, které dále provádí řada zákonů, mimo jiné zákon č. 89/2012 Sb., Občanský zákoník (NOZ) a v případě problematiky související s biometrií též zákon č. 110/2019 Sb., O zpracování osobních údajů.

V minulosti byla ochrana osobních údajů upravena přímo zákonem č. 101/2000 Sb., O ochraně osobních údajů a o změně některých zákonů, který byl 25. května 2018 nahrazen Nařízením Evropského parlamentu a Rady (EU) 2016/679 O ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů nebo též známé pod zkratkou GDPR) ze dne 27. dubna 2016 (dále jen Nařízení). Toto nařízení vzniklo na základě potřeby dohnat již zmíněný technologický náskok a nutnosti sjednotit, regulovat a minimalizovat zásahy do základních práv a svobod občanů EU.

Nařízení představuje zcela klíčový a převratný dokument, upravující získávání, zpracování a předávání osobních údajů, který staví na obecných principech a tzv. technologické neutralitě, a tím stanovuje režim a pravidla pro současné, ale i potencionálně v budoucnu vznikající technologie. Dále přináší přesné vymezení některých pojmů, které dosud byly různými subjekty vykládány odlišně, často dle vlastních potřeb a sledovaného cíle. Jako příklad přesného vymezení pojmů si můžeme uvést definici biometrického údaje, který je upraven v čl. 4 odst. 14 Nařízení. *„Biometrickými údaji“ jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování určité osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.*[16] Nařízení též zařadilo dle čl. 9 odst. 1 biometrické údaje do kategorie zvláštních osobních údajů, které je dokonce zakázáno zpracovávat. Avšak tento zákaz není absolutní. Za dodržení podmínek uvedených v čl. 9 odst. 2 Nařízení je možné oprávněně zpracovávat i tato data spadající do zvláštní kategorie osobních údajů. Mimo uvedených podmínek je však též nutné dodržet tzv. princip proporcionality.

[16] NPP. (2016). Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. [online]. [cit.2.10.2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679

Princip proporcionality v tomto případě představuje posouzení zásahu práva jednoho subjektu do práv druhého či ostatních subjektů. Proporcionality nebo též přiměřenosti bude dosaženo v případech, kdy buď nelze sledovaného cíle dosáhnout jinak, nebo přínos ze zásahu do práv jednoho subjektu bude vyšší, než případný zásah či omezení práv subjektu druhého.

Mezi režimy zpracování osobních údajů, které upravuje čl. 5 Nařízení, který stanovuje režim zpracování v obecném rámci a čl. 9 Nařízení, kde je upraveno zpracování tzv. zvláštní kategorie osobních údajů, kam mimo jiné spadá i biometrie, je poměrně zásadní rozdíl a je na první pohled zjevné, jakou důležitost zákonodárci dávají biometrickým údajům.

Zpracování osobních údajů dle čl. 5 Nařízení musí být:

- Korektní, zákonné a prováděné transparentním způsobem
- V souladu s výslovně vyjádřenými a legitimními účely
- Přiměřené rozsahu, který je nezbytný k účelu použití (tzv. minimalizace údajů)
- Provedené způsobem zajišťujícím přesnost údajů a jejich aktualitu
- Za podmínky jejich uložení nejdéle po dobu, po kterou slouží k účelu použití (tzv. omezené uložení)
- Prováděno vhodným způsobem tak, aby nedošlo k neoprávněnému či nezákonnému zneužití či ztrátě
- Odpovědnost za řádné zpracování nese správce systému

Zpracování osobních údajů dle čl. 9 odst. 2 Nařízení je možné:

- Po udělení výslovného souhlasu subjektu údajů k jednomu či více účelům.
- Jsou-li tyto údaje nezbytné pro účely plnění zvláštních práv a povinností v oblasti pracovního práva a oblasti sociálního zabezpečení a sociální ochrany.

- Za účelem ochrany životně důležitých zájmů subjektu práv, či jiné fyzické osoby v případech fyzické či právní nezpůsobilosti udělit souhlas.
- Při dodržení vhodných záruk lze zpracovávat údaje svých současných nebo bývalých členů nadace, sdružení, nebo jiného neziskového subjektu za účelem politických, náboženských, filozofických nebo odborových cílů a za podmínek, že údaje nejsou bez souhlasu zpřístupněny nikomu mimo tuto organizaci.
- Za předpokladu, že dotčené údaje zveřejnil subjekt údajů o sobě samém.
- V rámci soudních procesů pro určení, výkon či obhajobu právních nároků.
- Z důvodu významného veřejného zájmu, který je přiměřený sledovaným cílům a v souladu s legislativou EU či členského státu.
- V případě požadavku na lékařský posudek v rámci prevence, popřípadě posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky a sociální péče (odpovědná osoba navíc musí být vázána služebním tajemstvím).
- Ve veřejném zájmu z důvodu přeshraniční ochrany před zdravotními hrozbami a bezpečnosti zdravotní péče a kvality léčiv.
- V rámci vědeckých, historických a statistických výzkumů, kde veřejný zájem převyšuje právo na ochranu údajů.
- Zpracování biometrických, genetických a zdravotních údajů lze navíc nad tento rámec omezit příslušnou legislativou na národní úrovni jednotlivých členských států.

Z uvedeného je zřejmé, že aplikace biometrických systémů zejména v komerční sféře způsobem, který by byl bezezbytku v souladu s legislativou, není nikterak snadná. Případná instalace bude též v průběhu následujících let provozu poměrně náročná na vysokou odbornou kvalifikaci provozovatele a zejména jejího správce, který nese plnou odpovědnost za zákonnost, korektnost a transparentnost biometrického systému.

4 METODY BIOMETRICKÉ IDENTIFIKACE

Následující kapitola podrobně představí vybrané nejpoužívanější technologie biometrické identifikace, které jsou v současnosti aplikovány v systémech využívajících biometrii. Především principy, na kterých jednotlivé technologie pracují, jejich benefity a případná úskalí, které s sebou přináší.

4.1 Identifikace podle otisků prstů – DAKTYLOSKOPIE

Metoda identifikace prostřednictvím otisků prstů je, jak již bylo zmíněno v 1. kapitole, jednou z nejstarších skutečně důkladně vědecky zmapovaných způsobů biometrické identifikace. Počátky vědecky podložené identifikace podle otisků prstů jsou více než 100 let staré, a přesto nebo možná právě proto je tato identifikační metoda i v současné době nejrozšířenější metodou pracující s biometrikou. Primární využití našla tato metoda v kriminalistické daktyloskopii a též její hlavní rozvoj probíhal po desetiletí výhradně v souladu s požadavky kriminalistiky a potřebami forenzních věd. Komerční využití daktyloskopie jako biometrické identifikace a rozšíření mezi širokou laickou veřejnost umožnil až technologický vývoj posledních let.

Základním principem této identifikační metody je vědecky podložený fakt, že každý člověk má dlaně, bříška prstů, ale též plosky nohou pokryté specifickou strukturou čar a rýh, tzv. papilárních linií. (obr. 4) K tomu je nutné poznamenat, že sousloví „každý člověk“ není zcela definitivní. Papilární linie a jejich případné zpracování mohou být ovlivněny úrazy, kožními nemocemi, vrozenými či vývojovými vadami apod. V takových případech nemusí být použití této biometriky k identifikaci či verifikaci vůbec možné. Struktura papilárních linií se utváří již v prenatálním vývoji plodu v zárodečné kožní vrstvě a je po celý život daného jedince neměnná. Současně je u každého člověka tak specifická, že za aktuálního stavu žijící populace, tzv. biometrické entropii je v podstatě vyloučené, aby se objevili dva jedinci, kteří by měli identickou kresbu těchto papilárních linií a tím zanechali při doteku stejný otisk.

Obrázek 4 – detail struktury papilárních linií [Zdroj: 29]

Míru pravděpodobnosti případné shody se poprvé pokusil stanovit již jeden ze zakladatelů daktyloskopie F. Galton, který svým výpočtem došel k hodnotě $1{:}64x10^{9}$.[17] Tato hodnota však vycházela z možností, které před více než stoletím F. Galton měl. Současné možnosti komplexního zpracování otisků prstů Galtonův odhad výrazně překonávají. Např. P. Pavlík v roce 2007 uvedl v článku pro magazín JČU Kontakt hodnoty pro reálnou biometrickou entropii dokonce v intervalu $5{,}3x10^{36}$ – $1{,}9x10^{53}$.[18], což představuje násobně nižší míru pravděpodobnosti výskytu shodného obrazce papilárních linií, než deklaroval F. Galton ve své studii.

Přestože tato metoda biometrické identifikace má, jak již bylo nastíněno, své základy zejména v kriminalistice, pro rozsah této práce bude pozornost zaměřena výhradně na automatizované zpracování tzv. bezprostředně sejmutých

[17] EVANS, David & PARISH, Siobhan. (2015) *Predicting the First Recorded Set of Identical Fingerprints.* [online]. Journal of Interdisciplinary Science. Topic. 4. [cit.2.10.2021]. Dostupné z: https://www.researchgate.net/publication/274250949_Predicting_the_First_Recorded_Set_of_Identical_Fingerprints

[18] PAVLÍK, Pavel. (2007), *Biometrie jako základ současné i budoucí identifikace a autentizace*. [online]. Kontakt, roč. 9, je 2, s. 427 – 430. [cit. 25.09.2021]. Dostupné z: https://kont.zsf.jcu.cz/pdfs/knt/2007/02/34.pdf

otisků prstů a možnosti jejich využití v rámci systémů zajišťujících zabezpečení a přístup do objektů.

4.1.1 Rozdělení senzorů

Pro zpracování vstupních informací z otisků prstů jednotlivých uživatelů v rámci aplikace automatických systémů slouží elektronické snímače, které lze primárně rozdělit do dvou základních kategorií na KONTAKTNÍ a BEZKONTAKTNÍ. Tyto lze následně dělit dle použité technologie snímání na:

- **KONTAKTNÍ**
  - OPTICKÉ
  - ELETRONICKÉ
  - OPTO – ELEKTRONICKÉ
  - KAPACITNÍ
  - TEPLOTNÍ
  - TLAKOVÉ

- **BEZKONTAKTNÍ**
  - OPTICKÉ
  - ULTRAZVUKOVÉ

Z uvedeného přehledu lze vyčíst, že pro sken bezprostředního otisku prstů je možné použít různé fyzikální vlastnosti lidské kůže, které mohou představovat vodivost, teplotní a tlakové diference či pouhý specificky zvrásněný reliéf. Také je důležité zmínit, zejména s ohledem na současný celosvětový pandemický stav, možnost instalace bezkontaktních senzorů, které splňují nejen bezpečnostní, ale též čím dál více zohledňované požadavky hygienické.

V závislosti na použité technologii snímače se liší i míra schopnosti snímače odhalit případný neoprávněný pokus o verifikaci prostřednictvím přiložené kopie otisku prstu. Nejnižší odolnost v tomto ohledu mají technologicky nejstarší optické kontaktní senzory, které pracují pouze s dvourozměrným obrazem. V případě statického způsobu snímání je dokonce možné, že na skle senzoru zůstane otisk oprávněné osoby, který bude senzorem následně opakovaně zpracován a umožněn přístup v době, kdy tento uživatel již není fyzicky

přítomen. Vyšší odolnost vykazují senzory tlakové či elektro-optické, u kterých musí být zajištěna plasticita a trojrozměrnost snímaného objektu, ovšem i tyto lze v jistých případech překonat např. přiložením silikonového modelu otisku prstu.

Na opačnou škálu pomyslné bezpečnostní stupnice lze zařadit termické a zejména ultrazvukové snímače. V případě ultrazvukového snímání jsou prostřednictvím miniaturního sonaru emitovány vysokofrekvenční zvukové pulsy proti snímanému vzorku prstu. Následný odraz těchto pulsů je tím samým zařízením přijímán a z rozdílů vyslaných a přijatých vln je snímač schopen vytvořit detailní obraz skenovaného prstu či celé dlaně ve velmi vysoké kvalitě. Tato technologie je velmi přesná, a navíc díky částečnému průniku zvukových vln pod povrch kůže je takový snímač schopen současně ověřit i tzv. živost snímaného objektu.

4.1.2 Detekce živosti

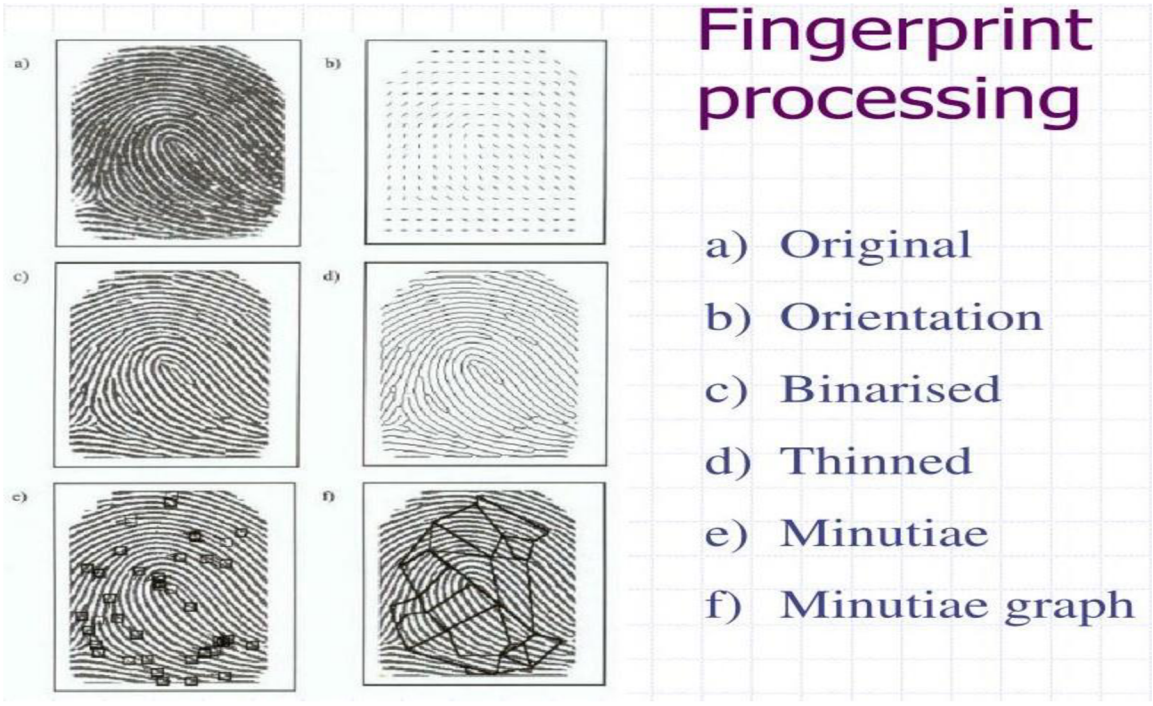
Vzhledem k výše uvedeným rizikům, spojeným ve zvýšené míře zejména s některými typy snímačů otisků prstů a relativní jednoduchosti vytvoření kopie otisku prstu, bylo nutné z bezpečnostního hlediska doplnit tyto snímače o další funkci, kterou představuje tzv. detekce živosti. Detekce živosti spočívá ve schopnosti snímače vyhodnotit, zda snímaný objekt je skutečným pravým živým biometrickým nosičem, nebo zda se jedná o falzifikát, který pouze vykazuje shodné obrazce papilárních linií, avšak bez dalších vlastností živého organismu. Tato sledovaná specifika živého organismu mohou být v závislosti na výrobci a druhu snímače různá, např.:

- Detekce přítomnosti potu
- Detekce pomocí multispektrálního světelného emitoru polarizovaným světlem
- Detekce ultrazvukovými vlnami
- Detekce fyziologických změn povrchu kůže při jejím stlačení
- Detekce srdeční aktivity
- Detekce přítomnosti okysličené krve

4.1.3 Zpracování otisků

Aby bylo umožněno automatizované použití otisků prstů, které bude dostatečně rychlé, přesné, a především bezpečné proti zneužití a ztrátě dat, je zapotřebí vstupní data nasnímaná senzorem nejprve zpracovat a bezpečně uložit. Při zadávání nového uživatele do systému, resp. registraci jeho biometrického nosiče, je zpravidla nutné vícenásobné sejmutí daného otisku. Tento postup je nezbytný z důvodu nasnímání biometrického nosiče z různých úhlů a pod rozdílným tlakem, který zapříčiní odlišnou deformaci obrazců papilárních linií, což následně zajistí eliminaci nežádoucích chyb při ověřování uživatele. Při běžném používání není totiž možné zabezpečit identickou sílu doteku ani orientaci přikládaného prstu.

Takto získaná data jsou následně zpracována dle předem nastavených algoritmů, jejichž cílem je odfiltrování nežádoucích šumů a nadbytečných informací, které by negativně ovlivňovali přesnost a čas zpracování. Konkrétní algoritmus či případná kombinace více algoritmů závisí na aplikaci jednotlivých výrobců hardwaru, ale pro názornost lze uvést nejběžnější typ takového algoritmu, který vytváří tzv. markantograf.



Obrázek 5 – postup zpracování otisku prstu [Zdroj: 13]

Při vytváření markantografu je původní otisk prstu postupně zpracován v několika fázích, které z něj extrahují směr orientace papilárních linií. Ty jsou následně počítačově zobrazeny tzv. binarizací, a dále ještě co nejvíce zeslabeny. Následuje nalezení markantů, které představují zejména smyčky, víry a oblouky, ze kterých se nadále vytvoří specifický obrazec zvaný markantograf, který je poté uložen do paměti zařízení. (obr. 5) Tímto způsobem je znemožněna zpětná extrakce originálního otisku a zároveň značně snížen požadavek na výpočetní výkon z důvodu minimalizace zpracovávaných dat.

4.2 Identifikace podle geometrie ruky

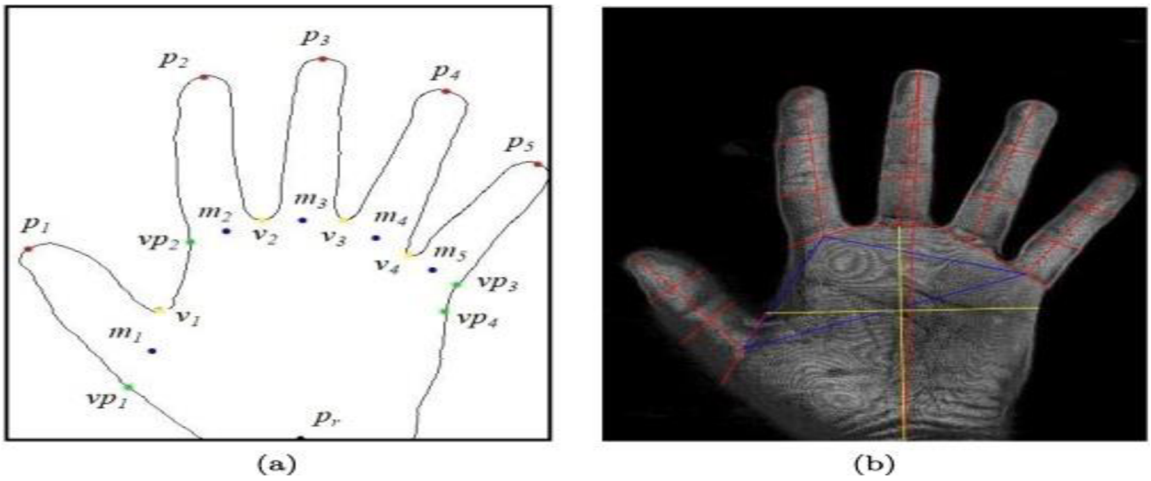
Metoda identifikace prostřednictvím geometrie ruky patří mezi první komerčně využívanou biometrickou identifikaci. Základy této metody položil v 70. letech 20. století Robert P. Miller svým patentem na zařízení zvané Identimat. Toto zařízení pracovalo na principu mechanického měření délek všech pěti prstů jedné ruky a jejich vzájemných rozdílů.

Podstatou této metody je identifikace osob na základě specifických markantů ve tvaru a velikosti částí ruky od zápěstí po konečky prstů. Na rozdíl od předchozí metody identifikace uvedené v kapitole 4.1 nejsou v rámci identifikace prostřednictvím geometrie ruky nikterak zohledněny nebo snímány obrazce papilárních linií. Pracuje se pouze se specifiky, které představuje tvar, proporce ruky a velikost jednotlivých prstů. V souvislosti se sledovanými markanty jsou u této technologie relativně nízké požadavky na použitý hardware oproti jiným technologiím. A to jak v oblasti požadovaného rozlišení pořizovaných snímků v případě použití nejběžnějšího optického CCD/CMOS snímače, tak také potřebné velikosti úložiště pro uložené šablony. Vzhledem k relativně nízké informační hodnotě této biometriky se velikost šablony geometrie ruky pohybuje okolo nízkých desítek bytů, na rozdíl např. od šablony otisku prstu, jehož datový objem se v závislosti na kvalitě pohybuje v intervalu 250–1000 bytů. V souvislosti s nízkým informačním obsahem této biometriky je vhodné její využití spíše pro biometrickou verifikaci než identifikaci. Své využití velmi úspěšně nachází v rámci aplikací v menších relativně uzavřených skupinách, kde může být jistou výhodou též poměrně nízká míra hodnot FRR. V některých moderních aplikacích jsou pro přesnější a rychlejší vyhodnocení snímaných vzorků efektivně využívány

i tzv. neuronové sítě.[19] Navíc je tato metoda společensky výrazně lépe akceptována než např. otisky prstů, a to z důvodu nižšího zásahu do práv osobnosti. Neboť jak již bylo nastíněno, geometrie ruky v sobě nenese dostatečný objem informací pro možnost přesné identifikace, s čímž souvisí obavy z jejího zneužití při potenciálním úniku uložených dat. Pro vyšší míru bezpečnosti je v případě použití technologie založené na geometrii ruky, vhodné paralelně použít doplňující způsob identifikace dalším identifikátorem v podobě PIN, ID karty, RFID čipu nebo RF karty. Takto navržený systém je poté vysoce efektivní a přesný. Důvodem je skutečnost, že systém již nevyhledává v celé databázi uložených šablon režimem 1:N, ale pouze ověřuje shodu v režimu 1:1 mezi uloženou šablonou evidovanou u konkrétního uživatelského účtu s právě přiloženým biometrickým nosičem.

4.2.1 Metody snímání

Metody snímání jsou v případě geometrie ruky nejčastěji na optické bázi a ve dvourozměrném zobrazení. Avšak technologický vývoj zejména v posledních letech umožnil zavedení výrazně přesnějšího trojrozměrného snímání (obr. 6), které umožnila jednak zařízení pracující na bázi optické triangulace, tak také snímače pracující na principu ultrazvukového sonaru obdobně jak již bylo popsáno v kapitole 4.1.1.

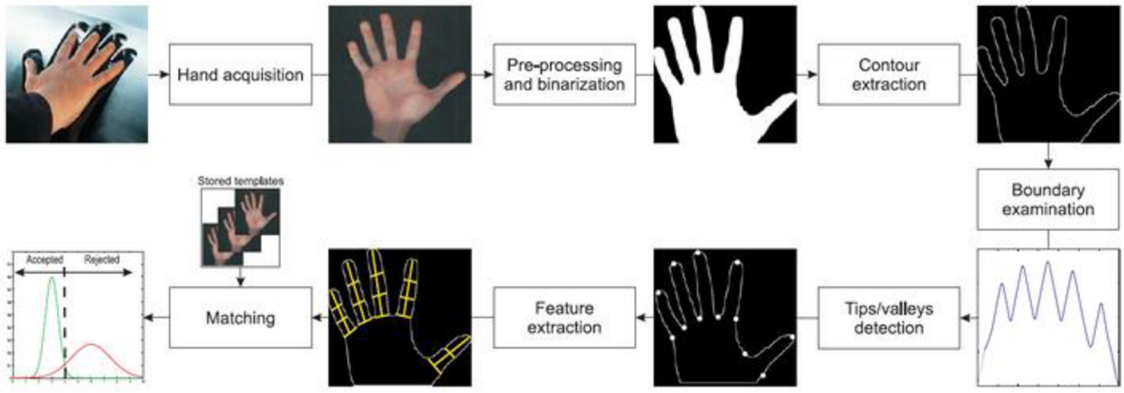


Obrázek 6 – snímek ruky pořízený 3D ultrazvukovým skenerem [Zdroj: 18]

[19] MOHAMED, Hesham Hashim et al (2021), *J. Phys.: Conf. Ser.* 1804 012144. [online]. [cit.26.10.2021]. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/1804/1/012144/pdf

Samotná verifikace spočívá v přiložení ruky přesně daným způsobem na zpravidla skleněnou podložku, kde je ruka fixována. Její fixaci v identické poloze zajišťují v podložce pevně zabudované kolíčky, o které se jednotlivé části ruky při přiložení opřou. Následně je pořízen záznam obrysu ruky a fixační body jsou počítačově odstraněny. (obr. 7) Výsledný snímek je dále zpracován dle nastavených algoritmů, které zajistí odfiltrování nežádoucích a nadbytečných informací a umožní maximální redukci dat pro uložení šablony. V závislosti na typu zařízení a výrobci zařízení uživatele verifikují na základě:

- Vzdálenosti přesně definovaných bodů
- Komparaci obrysu snímku šablony se snímkem vzorku
- Měření síly jednotlivých prstů
- Kombinací promítnutí a měření
- Trojrozměrného modelování celé ruky



Obrázek 7 – grafické znázornění celého procesu [Zdroj: 23]

4.3 Identifikace podle krevního řečiště

Metoda umožňující biometrickou identifikaci osob prostřednictvím unikátního větvení žilního systému uvnitř ruky se poprvé objevila v první polovině 90. let minulého století. Již v té době vykazovala značný potenciál pro budoucí využití, který spočívá zejména ve vysoké míře bezpečnosti dané skutečností, že se jedná o na první pohled skrytou biometriku, díky čemuž je téměř nemožné vytvořit její kopii. Jedinečnost a možnost využití této biometriky pro identifikaci byla potvrzena mimo jiné také komparací žilních obrazů jednovaječných dvojčat.

Dokonce ani jednovaječná dvojčata nevykazovala podobnost či shodu ve větvení žilního sytému. Dalším benefitem této metody je skutečnost, že při jejím využití dochází automaticky k ověření živosti snímaného vzorku, neboť bez přítomnosti okysličeného hemoglobinu se žilní struktura vůbec nezobrazí.[20] V neposlední řadě je důležité zmínit její velmi dobrou uživatelskou akceptaci mimo jiné z důvodu neinvazivního snímání a možnosti použití bez nutnosti fyzického kontaktu se snímačem.

Princip biometrického snímače, který zpracovává krevní řečiště ruky, spočívá v prosvícení ruky světlem o vlnové délce 700–940 nm v takzvaném NIR (near infra red) spektru. To umožní kontrastní zobrazení žilního systému vůči okolním tkáním. Tento jev je zapříčiněn skutečností, že žíly obsahující krevní hemoglobin pohlcují tento druh světelného vlnění více než okolní tkáň a tím se jejich struktura promítne jako výrazně tmavší vůči okolní tkáni. V případě použití NIR o vlnové délce 850 nm je kontrast nejmarkantnější a odhadovaný optický průnik takového vlnění do tkáně činí 3,57mm.[21] Pro sken krevního řečiště je možné využít jak hřbetní, tak dlaňovou část ruky. Avšak vždy pouze tu stranu, která byla použita při registraci uživatele do systému.

4.3.1 Metody snímání

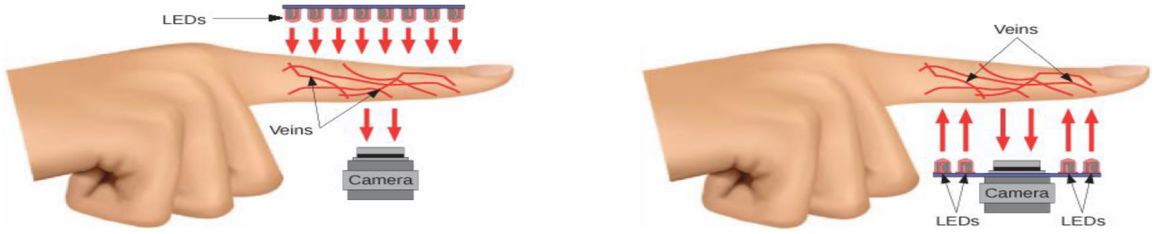
Pro vykreslení krevního řečiště potřebného pro kontrastní zobrazení je nejčastěji použito LED osvětlení o vlnových délkách v blízkém infračerveném záření. Ovšem je nutné poznamenat, že řada výrobců již používá i kombinace několika světelných paprsků o odlišných vlnových délkách pro lepší výsledné zobrazení. Záznam je zajištěn prostřednictvím monochromatického CCD snímače s vysokým rozlišením, který je schopen zaznamenat výsledný promítnutý obraz ve škále odstínů šedi. Důvodem pro použití CCD čipů je skutečnost, že mají vysokou citlivost zejména v používaném NIR spektru přibližně do vlnové

[20] WU, W., ELLIOTT, S.J., LIN, S., SUN, S. and TANG, Y. (2020), *Review of palm vein recognition* [online]. IET Biom., 9: 1-10. [cit.4.11.2021]. DOI: https://doi.org/10.1049/iet-bmt.2019.0034

[21] ZHOU, Y., KUMAR, A. (2011), *Human identification using palm-vein images* [online]. IEEE Trans. Inf. Forensics Sec., **6**, (4), pp. 1259–1274. [cit.4.11.2021]. Dostupné z: http://www4.comp.polyu.edu.hk/~csajaykr/myhome/papers/TIFS2011_PalmVein.pdf

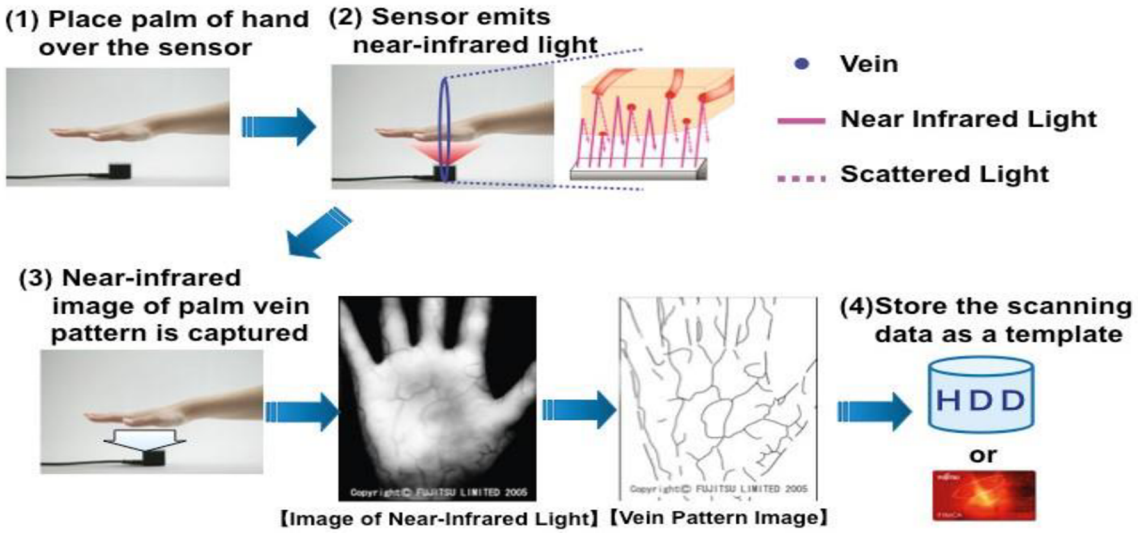
délky 1100nm. V případě použití optické technologie je možné výsledný žilní obraz získat dvěma metodami snímání. (obr. 8)

- Reflexivní metodou – snímač vyhodnocuje zpět odražený světelný paprsek
- Transmisivní metodou – za použití světelného paprsku vysoké intenzity, který prochází skrz tkáň ruky a je následně zachycen na její druhé straně



Obrázek 8 – zobrazení komparace transmisivní a reflexivní metody [Zdroj: 21]

Zachycený obraz krevního řečiště je zapotřebí obdobně jako u jiných typů biometrik zpracovat. V případě, že je použit bezkontaktní senzor, je nutné nejprve vymezit snímanou oblast tzv. ROI (z anglického Region of Interest), která bude snímána a následně použita ke zpracování. Důvod je ten, že zde není přesná fixace orientace ruky, jako např. u senzorů pracujících s geometrií ruky, kde je k tomuto účelu použito fixačních kolíčků. Po nasnímání zájmové plochy prochází snímek řetězcem úprav, které jsou nezbytné pro vytvoření šablony. (obr. 9)



Obrázek 9 – znázornění celého procesu zpracování žilního obrazu [Zdroj: 32]

4.4 Identifikace podle oční duhovky

Metoda identifikace prostřednictvím oční duhovky patří v současné době mezi nejpřesnější biometrickou metodu vůbec. Její přesnost je přibližně 1050krát větší než v případě otisků prstů.[22] Možnost využít oční duhovku pro identifikaci v rámci automatizovaných systémů umožnil až v poměrně nedávné době učiněný objev Dr. J. Daugmana a jeho týmu. Na základě tzv. Daugmanových algoritmů, které jsou od roku 1994 chráněny patentem, je možné zpracovat obraz oční duhovky a jejích specifik do bitového kódu, který je následně uložen v systému jako šablona a lze ji použít pro identifikaci či verifikaci obdobně jako např. otisk prstu.

Tato biometrická identifikační metoda je založena na obdobném principu, jako např. daktyloskopie, která zpracovává individuální kresbu papilárních linií. V případě využití biometriky oční duhovky je obdobou papilárních linií řada specifických markantů, které jsou součástí duhovky a vytvářejí na jejím povrchu unikátní charakteristický reliéf. Tyto markanty, mezi které řadíme např. krypty, radiální rýhy, hřebeny, dutinky, prstence, korony, pigmentové skvrny a další vymezil, Dr. J. Daugman do cca 250 jednotlivých charakteristik.[23] Tato specifická struktura duhovky se formuje již v průběhu prenatálního vývoje plodu mezi cca 3–8 měsícem jeho vývoje. Díky skutečnosti, že se nachází uvnitř oka a je tedy chráněna vůči vnějším vlivům, zůstává její struktura v průběhu života neměnná.

V případě využití části oka jako biometrického identifikátoru je patřičné zmínit, že duhovka není jedinou možností, které lze využít. Pro identifikaci je možné velmi úspěšně využít též oční sítnice. Dokonce oční sítnice byla jako biometrika objevena o desítky let dříve. Ovšem její praktické uplatnění se vyjma některých ozbrojených složek a vládních agentur USA příliš nerozšířilo. Důvodem byla vysoká cena zařízení a také poměrně nekomfortní a relativně komplikovaný proces snímání. Ani v současné době není tato metoda

[22] Biometricke-ctecky.cz: Biometrie – Oko [online]. [cit. 18.11.2021]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

[23] DRAHANSKÝ, Martin, ORSÁG, Filip. *Biometrie.* Brno: Computer Press, 2011, 294 s. ISBN 978-80-254-8979-6, str. 179–188

biometrického ověření v praxi příliš využívána, z toho důvodu se jí nebudu v práci dále výrazněji zabývat.

4.4.1 Oční duhovka

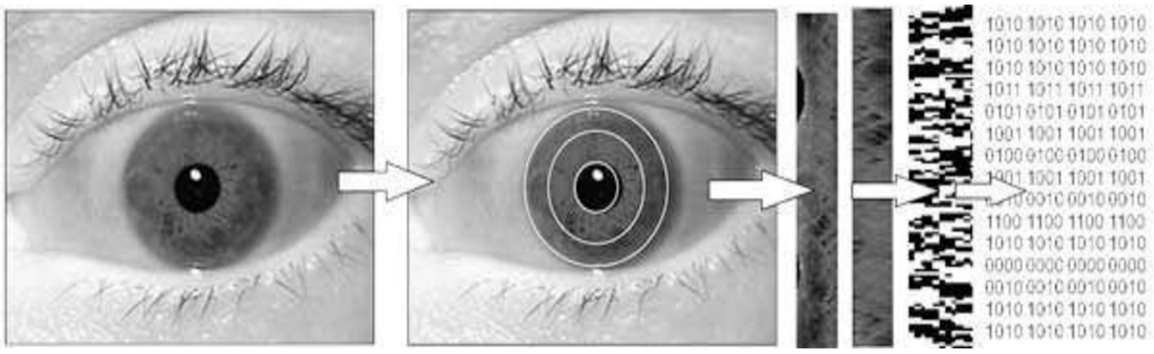
Duhovka (anglicky iris) principiálně funguje jako clona a umožňuje změnou své dilatace regulovat vstupující světlo, které prochází panenkou dále do oka. Samotná duhovka, představuje vnitřní část oka o velikosti cca 11 mm, kterou lze dobře pozorovat pouhým okem zvenčí i díky jejímu specifickému zabarvení. Její zabarvení je částečně geneticky závislé a finální odstín je dosažen cca kolem druhého roku života jedince. Od této doby zůstává individuální charakteristická struktura i barevný odstín v průběhu života konzistentní a je možné ji využít jako biometrického identifikátoru s vysokou přesností.

4.4.2 Metody snímání

Vzhledem ke skutečnosti, že je duhovka vnitřní součástí oka, kterou lze dobře pozorovat z vnějšího prostředí, je pro její snímání použito výhradně optických neinvazivních metod. Některé výraznější rysy struktury duhovky jsou viditelné i za běžného osvětlení, ovšem pro detailní záznam snímaného obrazu je zapotřebí kamery s monochromatickým CCD čipem o vysokém rozlišení, neboť obdobně jako u předchozí biometriky uvedené v kapitole 4.3 je i zde použito NIR záření pro zvýraznění markantů na povrchu duhovky a zobrazení její detailní struktury. Pro sken oční duhovky je zpravidla použito zařízení, které má dvě kamery, z nichž jedna snímá celý objekt (obličej, hlavu) a software ze snímaného obrazu určí prostor oka. Následně se na předdefinovanou oblast ve snímaném obrazu zaostří monochromatická kamera, software vyhodnotí přítomnost duhovky a během cca 2 vteřin pořídí detailní záznam. Pro finální extrakci a vyhodnocení dat z detailního snímku oka, resp. duhovky je nutné snímek podrobit několika matematickým postprocesům, mezi než patří Gaborův wavelet, Prostorový filtr, Waveletové protnutí nuly, Místní odchylky, Lokální texturové vzory – LTP.[24] Po aplikaci výše uvedených

[24] MUTHANA, H.H. (2019), Optimized biometric system based iris-signature for human identification. *International Journal of Advances in Intelligent Informatics* [online]. Baghdad: Mustansiriyah University, 2019, 273-284 [cit.20.11.2021]. ISSN 2442-6571 Dostupné z: https://core.ac.uk/download/pdf/268127039.pdf

demodulací je duhovka znázorněna v tzv. fázorovém diagramu, který obsahuje informace o pozici, četnosti a orientaci jednotlivých markantů.[25] Takto získaný diagram je v podstatě bitovým kódem nasnímané duhovky, který následně slouží systému pro vytvoření biometrické šablony, popř. ověření snímaného vzoru s šablonou daného uživatele. (obr. 10)



Obrázek 10 – proces vyhledání a následné zpracování duhovky [Zdroj:26]

4.4.3 Detekce živosti

Vzhledem ke skutečnosti, že se duhovka nachází uvnitř oka, a navíc vykazuje tak značnou biometrickou entropii, je velmi nepravděpodobné, že by se ji podařilo nahradit a úspěšně systémem ověřit. Nicméně pro případné pokusy použít k identifikaci plagiát či snad delaborované oko mrtvého uživatele je i v těchto aplikacích implementován test ověření živosti.

Živost je možné ověřit hned několika způsoby. V první řadě lze monitorovat pohyb oka a popř. pohyb očního víčka. Sofistikovanější metodou je monitoring reakce, resp. dilatace duhovky v závislosti na změně intenzity světla, popř. jejích drobných reflexivních pohybů (tzv. hippus). Další metodou ověření živosti je sledování průtoku krve za pomoci NIR záření, obdobně jako bylo popsáno v kapitole 4.3.

4.5 Identifikace podle obličeje

Obličej slouží v lidské společnosti jako hlavní biometrický identifikátor tisíce, resp. desetitisíce let. Aniž bychom si to jakkoli uvědomovali, přirozeně

[25] ŠČUREK, Radomír. *Biometrické technologie – technické prostředky bezpečnostních služeb.* Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2015, 115 s. ISBN 978-80-248-3786-4, str. 36–37

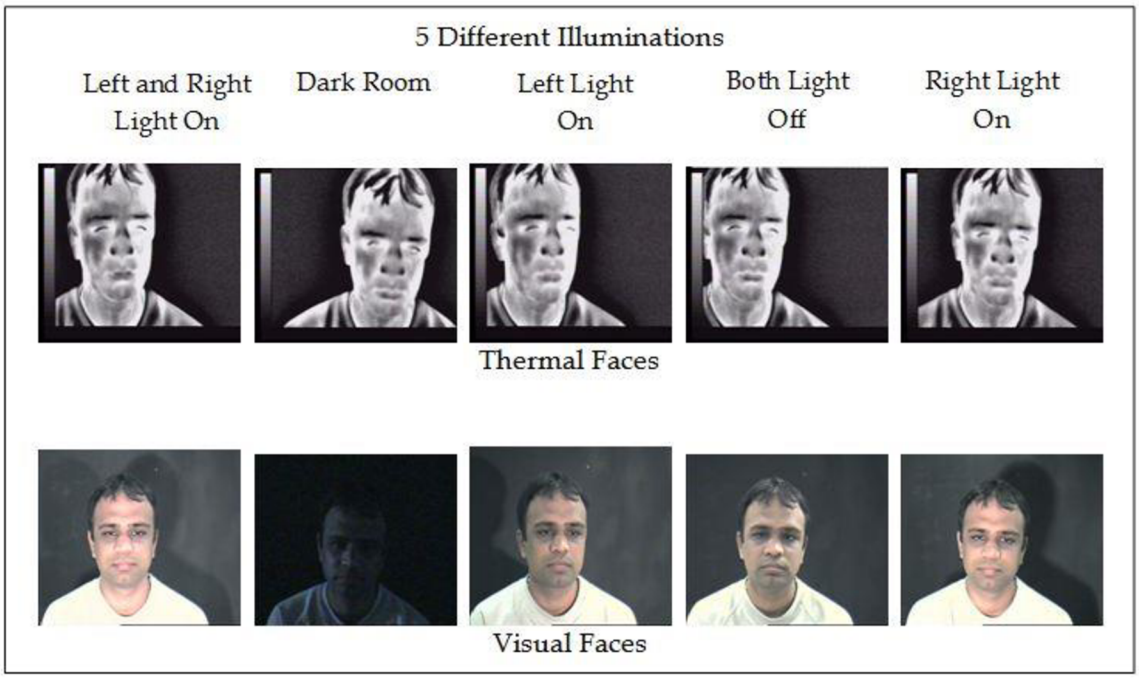
rozeznáváme osoby jednu od druhé mimo dalších charakteristických prvků podle jejich obličeje. Z obličeje je díky velkému množství drobných mimických svalů dokonce možné vyčíst vnitřní psychické rozpoložení osoby či konkrétní emoce jako je radost, vztek, údiv, popř. bolest. Vzhledem k této "přirozenosti" a také relativní jednoduchosti získání biometrických dat, často i bez vědomí samotné osoby, bylo nasnadě implementovat tuto biometriku do automatických identifikačních systémů. Možnost skryté biometrické identifikace, kterou tato metoda jako jedna z mála poskytuje, našla své uplatnění zejména po událostech 11. září 2001. Od této doby nabral vývoj a též praktické nasazení této biometriky značnou dynamiku.

V případě tzv. "Face ID" jak je také někdy tato biometrická identifikační metoda označována, není dosaženo tak vysokých hodnot biometrické entropie jako např. v případě některých jiných biometrik, kterými jsou otisky prstů, oční duhovka či sítnice. Navíc je zde komplikace v podobě značné vnitrotřídní variability, která je zapříčiněna hned několika faktory. Mezi tyto faktory lze zařadit vliv činnosti již zmíněných mimických obličejových svalů, dále změny v úpravě vousů a vlasů, změny vyvolané stárnutím, popř. nošením brýlí, pokrývek hlavy apod. Zohlednit je zapotřebí také charakteristické odlišnosti dané etnicitou a pohlavím. Dalším faktorem, který má významný vliv, je měnící se míra intenzity a úhel dopadajícího světla, díky čemuž mohou některé obličejové markanty splynout nebo naopak působit výrazněji, než ve skutečnosti jsou. Nicméně i přes tato úskalí je technologie identifikace prostřednictvím obličeje v současné době na vzestupu a obličej jako biometrika je celosvětově široce používán v různých aplikacích napříč společností.

4.5.1 Metody snímání

Metody umožňující identifikaci osob podle obličejových rysů jsou založené na optické bázi, neboť hlava a obličejové rysy osoby jsou až na výjimky (nošení burky, kukly, masky atp.) dobře zaznamenatelné bez potřeby speciálních senzorů. Ve většině případů lze nasnímat tvář osoby při běžném osvětlení, avšak sofistikovanější zařízení zpravidla používají NIR přísvit nebo jsou dokonce konstruována jako duální a běžný obraz ve viditelném spektru doplňují

např. termosnímkem. (obr. 11) V takovém případě je zároveň ověřována živost snímaného vzorku a výrazně narůstá i přesnost identifikace.



Obrázek 11 – porovnání stejné osoby nasnímané termokamerou a běžnou kamerou za rozdílných světelných podmínek [Zdroj:36]

Dalším dělícím hlediskem při pořizování snímku obličeje může být skutečnost, zda je záznam pořizován jako pouhý dvourozměrný obraz "fotka" nebo je tvář a její charakteristické rysy zaznamenány jako trojrozměrný objekt "model", případně zda je pořizován snímek statický či je nutné extrahovat data z dynamického záběru. Ve všech případech má zcela zásadní úlohu softwarové zpracování a vyhodnocení snímaného obrazu. Pro tzv. normalizaci snímku, díky které je možné následné zpracování obrazu, je důležitá i fáze nazývaná pre-procesing, která pomocí nastavených algoritmů umožňuje např. promítnutí pod úhlem snímaného obličeje do podoby jako by byla osoba zabírána přímo z čelního pohledu.[26] (obr. 12)

[26] TAMILSELVI, M. a S. KARTHIKEYAN. *An ingenious face recognition system based on HRPSM_CNN under unrestrained environmental condition* [online]. Chennai, India: Sathyabama Institute of Science and Technology, 2021 [cit. 2021-11-29]. ISSN 1110-0168. DOI: https://doi.org/10.1016/j.aej.2021.09.043

V zásadě je možné celý proces rozčlenit do tří kroků, kterými jsou:

- Detekce obličeje v záběru – k tomuto účelu slouží především tzv. eye-trackery, které zaznamenají charakteristický pohyb očních víček. V některých aplikacích je k tomuto účelu využito termální stopy obličeje.
- Extrakce rysů z detekovaného obličeje – aplikování příslušného algoritmu, popř. kombinace několika algoritmů. (viz. demonstrativní výčet)
    - PCA – Principal Component Analysis označováno i jako eigenfaces
    - LDA – Linear Discriminative Analysis
    - DBC – Directional Binary Code
    - LBP – Local Binary Patettern
    - SIFT – Scale-Invariant Feature Transform
    - Multi SVM – Multi Support Vector Machine
    - HRPSM CNN – Hybrid Robust Point Set Maching Convolutional Neural Network
- Rozpoznávání tváře – porovnání výsledků extrahovaných dat s tvářemi v příslušné databázi. Dle určení systému v režimu identifikace/autentizace.

Lze konstatovat, že různé druhy technologií odlišným způsobem mapují hlavní obličejové markanty, které představují oči, nos, ústa a tvar, resp. obrys obličejové části hlavy. Měření jejich velikosti, vzájemné vzdálenosti a celkové geometrie obličeje slouží po zpracování k vytvoření jedinečné biometrické šablony.

Obrázek 12 – a) vstupní obraz, b) výstup zpracovaný metodou HRPSM CNN [Zdroj:12]

4.6 Identifikace podle chůze

Bipedální lokomoce, jak je někdy v odborné literatuře nazývána člověku naprosto přirozená pohybová aktivita představující chůzi či běh, v sobě skrývá řadu specifických pohybových markantů, které lze použít v rámci tzv. behaviorální biometrie. V závislosti na vzájemné interakci celého souboru specifik, jakými jsou výška, hmotnost, délka končetin, kloubní rozsah, případné vývojové vady, popř. prodělané nemoci či úrazy, je chůze každého člověka velmi individuální. Dalším aspektem umožňujícím využití chůze jako biometrického identifikátoru je skutečnost, že rytmus chůze zůstává za běžných podmínek po většinu života neměnný. Tato skutečnost může být využita ve forenzní praxi v rámci vyšetřování závažnější kriminality, při které byl pořízen kamerový záznam, ale není dostatečně kvalitní, či je pořízen z úhlu nebo větší vzdálenosti, kdy není možné identifikovat osobu podle obličeje atp. Další uplatnění je možné najít např. v případech zabezpečovacích systémů, kdy je žádoucí informování osoby vykonávající dohled o tom, že byl zaznamenám charakteristický pohyb člověka ve sledovaném perimetru.

Potenciál a budoucí širší možnosti uplatnění této biometriky odhalil mimo jiné nedávný výzkum společného týmu akademických pracovníků University of Manchester a Universidad Autonoma de Madrid, kteří za využití pokročilé umělé inteligence dosáhli hodnoty ERR méně než 1 %, konkrétně 0,7 %, což oproti předchozím výsledkům této biometriky představuje zlepšení o propastných 371 %. V tomto případě nebylo pro získání vstupních informací použito kamerového systému, ale záznam pohybu osob byl pořízen tlakovými senzory zabudovanými v podlaze.[27] Výsledky uvedeného výzkumu umožňují použití dynamiky chůze jako velmi přesného biometrického identifikátoru pro verifikaci konkrétní osoby s mimořádně vysokou mírou přesnosti. Samozřejmě není reálné použít tento druh biometriky pro čistě identifikační systémy obdobně jako např. otisk prstu či sken oční duhovky. Nicméně lze předpokládat úspěšné a efektivní nasazení takového

[27] REYES, O.C., R.V. RODRIGUES, P. SCULLY a K.B. OZANYAN. *Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks* [online]. 2. Vol. 41. IEEE: Transactions on Pattern Analysis and Machine Intelligence, 2019, 285-296 [cit. 2021-12-01]. DOI: 10.1109/TPAMI.2018.2799847

systému v rámci menších relativně uzavřených kolektivů, obdobným způsobem jako systémy založené na biometrice geometrie ruky.

4.6.1 Metody snímání

Základní a nejrozšířenější metodou pro záznam lokomoce chůze je nepochybně prostřednictvím video záznamu. V závislosti na určení systému lze zaznamenat použití jak standardní videotechniky, tak také použití technologie pracující se záznamem pořízeným s NIR přísvitem, popř. i infrakamerou. Optický záznam je možné pořizovat také jako dvourozměrný nebo za pomoci souboru několika kamer jako trojrozměrný. Relativně novým trendem je použití podlahových senzorů, které zaznamenávají frekvenci, tlak, vzdálenost a intenzitu jednotlivých kroků. Tento trend čerpá poznatky z oblasti medicíny, konkrétně tzv. baropodometrie (měření tlaku nohy na podložku za stoje, chůze či běhu) a aplikuje je v rámci behaviorální biometrie. Ostatně obdobný vývojový proces lze najít u většiny biometrik.

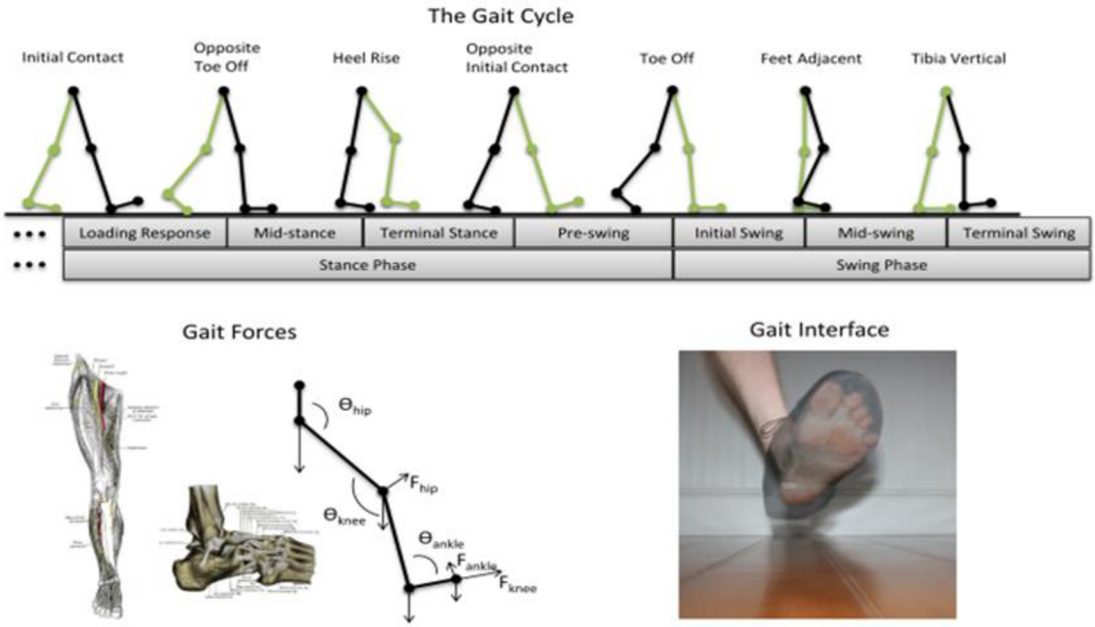
Základní jednotkou pro zisk informací je stále se opakující tzv. krokový cyklus, resp. dvojkrok. *Pro potřeby identifikace osob podle chůze je důležitá fáze kroku, kdy obě nohy spočívají na zemi (dvojí opora) a fáze, kdy tělo spočívá na jedné končetině a druhá osciluje (jednostranná opora).*[28] Tyto dvě fáze lze dále rozčlenit do dalších 7 úseků. (obr. 13)

Příkladem jednotlivých sledovaných markantů, které v sobě krokový cyklus nese, jsou:

- Rytmus a pravidelnost
- Délka kroku
- Pohyb těžiště
- Postavení nohy a její odrážení od podložky
- Stabilita při chůzi
- Současný pohyb horních končetin a trupu

[28] SULOVSKÁ, Kateřina. *Výzkum biometrických systémů z hlediska jejich důvěryhodnosti a integrity: Analýza změn ve vzorcích chůze*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 76 s. ISBN 978-80-7454-799-7. Dostupné také z: http://hdl.handle.net/10563/43763. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav automatizace a řídicí techniky.

- Osové postavení nohy vůči podložce
- Svalová aktivita



Obrázek 13 – fáze krokové cyklu a hlavní silové vektory [Zdroj:17]

Výstupem měření jsou charakteristické křivky, které opisují jednotlivé části těla, zejména oblasti kloubních spojení kostí. A také graf znázorňující dynamický stereotyp, který představuje frekvenci opakujících se krokových cyklů v čase.

II PRAKTICKÁ ČÁST A
(DOTAZNÍKOVÉ ŠETŘENÍ)

5 VYHODNOCENÍ DOTAZNÍKOVÉHO ŠETŘENÍ

5.1 Cíle výzkumu

Cílem provedeného výzkumu bylo zjistit, jaké je povědomí široké veřejnosti o biometrii a biometrické identifikaci. Jakým způsobem se společnost staví k aplikacím využívajícím různé druhy biometrik, mimo jiné, zda by respondenti upřednostnili využití biometrických prvků v systémech zajišťujících přístup a zabezpečení budov před klasickými čtečkami využívajícími tokeny. Které druhy biometrické identifikace jsou preferovány a oproti tomu, které z biometrických identifikátorů by osoby subjektivně vnímaly jako neakceptovatelné. Jaký druh osobního identifikátoru by respondenti upřednostnili v případě možnosti volby v rámci docházkového a zabezpečovacího systému svého zaměstnavatele, a zda by vůbec byli ochotni poskytnout své biometrické údaje zaměstnavateli. Jaká kritéria jsou v rámci hodnocení biometrických systémů pro respondenty nejdůležitější, a zda jsou zařízení pracující na bázi biometrické identifikace společností vnímána jako bezpečná či vzbuzují spíše nedůvěru a obavy.

5.2 Sběr dat

Sběr dat byl uskutečněn pouze v prostředí internetu, a to především z důvodů snadného šíření dotazníku mezi respondenty, úspory času a také možnosti okamžitého zpracování dat bez dalších komplikací spojených s jinými formami sběru dat. Pro tvorbu a následné zpracování celého dotazníku jsem vybral společnost Survio, která se zabývá problematikou online dotazníků.

Odkaz na dotazník jsem rozšířil mezi okruh nejbližších přátel a kolegů v zaměstnání s žádostí o následné sdílení mezi jejich přátele a známé. Tím byla dosažena velmi pestrá struktura respondentů, což bylo mimo jiné mým cílem, aby výsledky šetření pokrývaly co možná nejširší společenské spektrum a výsledek měl skutečně vypovídající hodnotu.

Dotazník byl přístupný prostřednictvím odkazu po dobu tří týdnů a dle statistiky dosáhl za tuto dobu 216 zobrazení, ze kterých bylo řádně vyplněno

a do výsledků započteno 114 dotazníků. Mým cílem bylo získat alespoň 100 platně vyplněných dotazníků. Množstevní cíl pro zajištění objektivity byl tímto splněn.

5.3 Využití získaných dat

Výsledky vyplývající z provedeného výzkumu poslouží jako kritérium při výběru nejvhodnějších biometrických prvků, které budou následně instalovány v rámci modelového objektu, který bude představen v Praktické části B. Celý systém zabezpečení bude vhodně doplněn biometrickými prvky takovým způsobem, aby i nadále odpovídal svému účelu, ale zároveň byl pro firmu efektivnější a současně byl vnímán jednotlivými uživateli jako přínosný a komfortní upgrade usnadňující každodenní rutinu.

5.4 Soubor použitých otázek

Kompletní souhrnný písemný report celého dotazníkového šetření je součástí této práce ve formě přílohy, nicméně z důvodu přehlednosti a lepší orientace v následujících kapitolách uvádím soubor použitých otázek i zde.

Otázka č. 1

Jste muž/žena?

Otázka č. 2

Jaký je Váš věk?

Otázka č. 3

Jaké je Vaše nejvyšší dosažené vzdělání?

Otázka č. 4

Víte, co je biometrická identifikace?

Otázka č. 5

Už jste se setkal/a se systémem/zařízením, které využívalo nějaký druh biometrie?

Otázka č. 6

Znáte nebo aktivně používáte některý z uvedených druhů biometrických identifikátorů?

Otázka č. 7

Domníváte se, že je využití biometrie bezpečné?

Otázka č. 8

Pokud byste měl/a na výběr, kterou metodu/formu ověření své osoby byste zvolil/a?

Otázka č. 9

Který z uvedených biometrických identifikátorů byste preferoval/a v případě použití ve vašem zaměstnání?

Otázka č. 10

Jakou měrou Vás při volbě mezi jednotlivými druhy biometrie ovlivňují uvedená hlediska?

Otázka č. 11

Je některý z níže uvedených biometrických identifikátorů pro Vás neakceptovatelný?

Otázka č. 12

Byl/a byste ochoten/na poskytnout svá biometrická data zaměstnavateli za účelem jejich využití v docházkovém a přístupovém systému, popř. pro automatické ovládání systému zabezpečení objektu/ů?

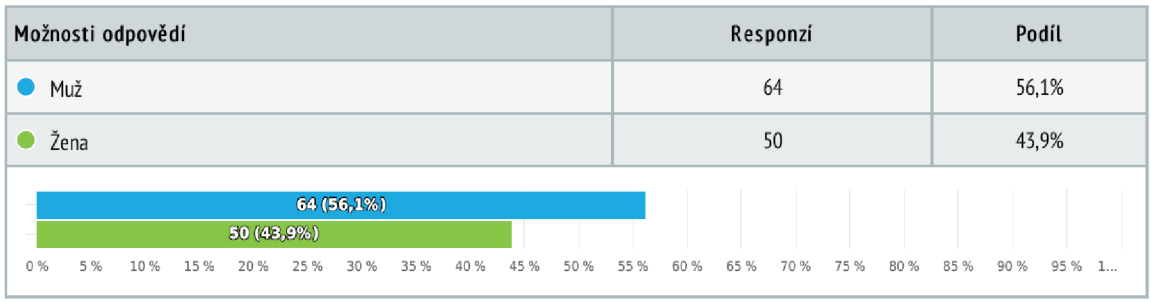
Otázka č. 13

Pokud by Váš zaměstnavatel nainstaloval biometrický systém v rámci automatizované správy zabezpečení budov, vnímal byste to jako?

6 VYHODNOCENÍ DOTAZNÍKU

6.1 Respondenti

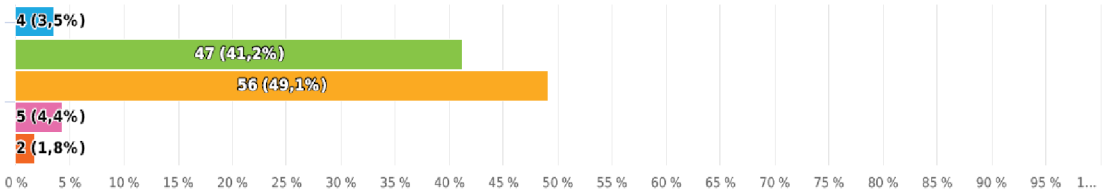
Charakteristika respondentů vychází z otázek č. 1–3, kde jsou požadovány informace o pohlaví, věku a nejvyšším dosaženém vzdělání. Co se týče zastoupení obou pohlaví, tak je vzájemný poměr relativně vyrovnaný, 56,1 % mužů proti 43,9 % žen, jak je vidět na následujícím obrázku č. 14.



Obrázek 14 – charakteristika respondentů podle pohlaví [Zdroj: Autor]

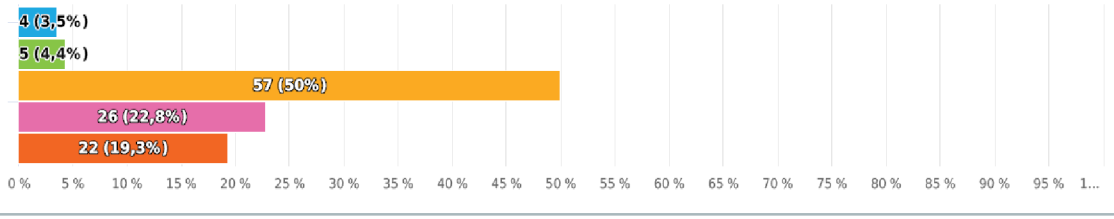
Věkový rozsah je velice široký a pokrývá všechny skupiny od 15 let po osoby ve věku 70 let a více. Největší zastoupení však představují dvě skupiny osob v aktivním věku, pokrývající interval 26–55 let. Tyto skupiny čítají dohromady 103 respondentů, jak je vidět i na přiloženém obrázku č. 15. Taktéž lze hodnotit i míru nejvyššího dosaženého vzdělání respondentů. Zde je nejvyšší zastoupení středoškoláků s maturitou v počtu 57 osob, kteří tvoří celých 50 % všech respondentů. Druhou nejvýznamnější skupinu tvoří součet obou skupin vysokoškolsky vzdělaných respondentů, která čítá 26 absolventů bakalářských studijních programů, resp. 22 absolventů magisterského a vyššího studia, což představuje 42,1 % všech respondentů, jak je možné vyčíst z obrázku č. 16. Osoby se základním vzděláním a středoškoláci bez maturity představují pouhých 7,9 % ze všech respondentů. V tomto ohledu lze konstatovat, že cíl byl také splněn, neboť je pokryta široká škála osob a zároveň nejvyšší zastoupení má věková skupina aktivních pracujících.

Možnosti odpovědí	Responzí	Podíl
15-25 let	4	3,5%
26 - 40 let	47	41,2%
41 - 55 let	56	49,1%
56 - 70 let	5	4,4%
70 a více let	2	1,8%



Obrázek 15 – charakteristika respondentů podle věku [Zdroj: Autor]

Možnosti odpovědí	Responzí	Podíl
Základní	4	3,5%
Středoškolské bez maturity	5	4,4%
Středoškolské s maturitou	57	50,0%
VŠ - bakalářské	26	22,8%
VŠ - magisterské a vyšší	22	19,3%



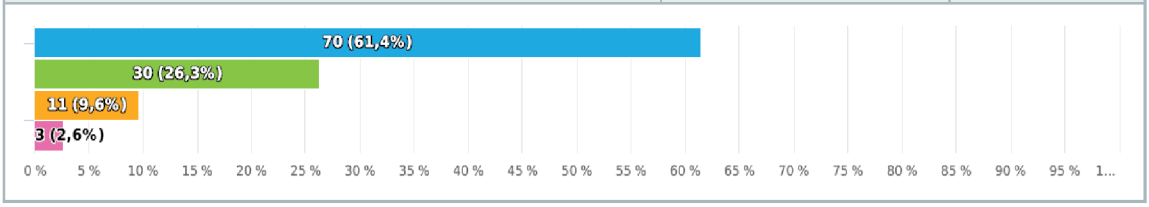
Obrázek 16 – charakteristika respondentů podle vzdělání [Zdroj: Autor]

6.2 Obecné povědomí o biometrické identifikaci

Na zjištění o obecném povědomí společnosti v oblasti biometrické identifikace cílily otázky č. 4–6. Z čehož v nejobecnější rovině byla položena otázka č. 4, zda respondenti vědí, co si představit pod souslovím biometrická identifikace. Z přiloženého obrázku č. 17 vyplývá, že 61,4 % respondentů

ví přesně a dalších 26,3 % se domnívá, že ví, co v sobě sousloví biometrická identifikace zahrnuje. Jen 9,6 % ze všech respondentů neví, co si představit pod biometrickou identifikací, a další pouhé 3 osoby o biometrické identifikaci nikdy ani neslyšely.

Možnosti odpovědi	Responzí	Podíl
Ano, vím	70	61,4%
Domnívám se, že vím	30	26,3%
Nevím	11	9,6%
Nikdy jsem to neslyšel	3	2,6%



Obrázek 17 – obecné povědomí o biometrické identifikaci [Zdroj: Autor]

V tomto ohledu je také zajímavé promítnutí některých údajů do kontingenční tabulky. V tabulce č. 2 jsou znázorněny údaje z odpovědí porovnávající pohlaví respondentů a obecné povědomí o biometrické identifikaci.

Tabulka 2 – kontingenční tabulka otázek č. 1 a č. 4 dotazníku [Zdroj: Autor]

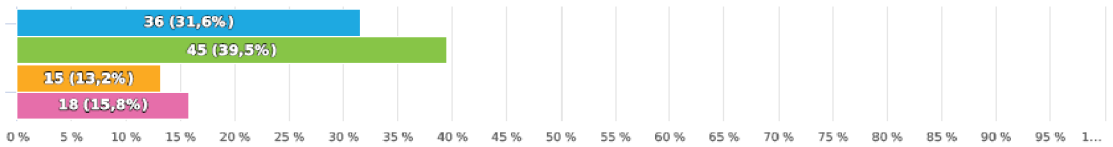
	Muž	Žena	Celkem
Ano, vím	47	23	70
Domnívám se, že vím	13	17	30
Nevím	3	8	11
Nikdy jsem to neslyšel	1	2	3
Celkem	64	50	114

Z údajů je možné vyčíst, že představu či povědomí o biometrické identifikaci mají ve větší míře muži než ženy, a to v poměru 52,6 % ku 35,1 % ze všech respondentů. Toto zjištění lze potvrdit také z výsledků odpovědí o nevědomosti či neznalosti biometrické identifikace, které vychází v opačném poměru mužů a žen. V tomto ohledu neví nebo nikdy o biometrické identifikaci neslyšelo 3,5 % mužů a 8,8 % žen.

Následující otázka č. 5 směřovala ke zjištění, zda respondenti mají osobní zkušenosti se zařízením nebo systémem, který by při své činnosti využíval nějaký druh biometrie. Z přiloženého obrázku č. 18 je patrné, že nějakou zkušenost s použitím svého těla jako identifikátoru má celkem 96 osob, což představuje 84,2 % všech respondentů. Pouze 15,8 % respondentů doposud nemělo příležitost v průběhu svého života vyzkoušet zařízení, popř. systém umožňující využití biometrické identifikace.

Je patrné, že největší využití biometrie je zatím v rámci soukromého života, což lze velmi pravděpodobně přisuzovat používání mobilních telefonů se zabudovanou čtečkou otisků prstů, která je v současnosti instalována téměř v každém zařízení. Ovšem nezanedbatelná část respondentů se již setkala nebo dokonce pravidelně aktivně využívá nějaký druh biometrie také ve svém zaměstnání. V případě osob pravidelně aktivně využívajících biometrickou identifikaci v soukromém i profesním životě, je tato skupina zastoupena 31,6 % ze všech respondentů. Z uvedených dat je zřejmé, že biometrické prvky jsou společností poměrně dobře přijímány a jsou již hojně zastoupeny v rámci identifikačních a autentizačních aplikací, jak v soukromém, tak také v profesním životě.

Možnosti odpovědí	Responzí	Podíl
Ano, aktivně pravidelně používám biometrickou identifikaci v zaměstnání i v soukromí.	36	31,6%
Ano, ale pouze v soukromí.	45	39,5%
Ano, ale pouze v zaměstnání.	15	13,2%
Ne, takové zařízení jsem ještě nevyzkoušel.	18	15,8%

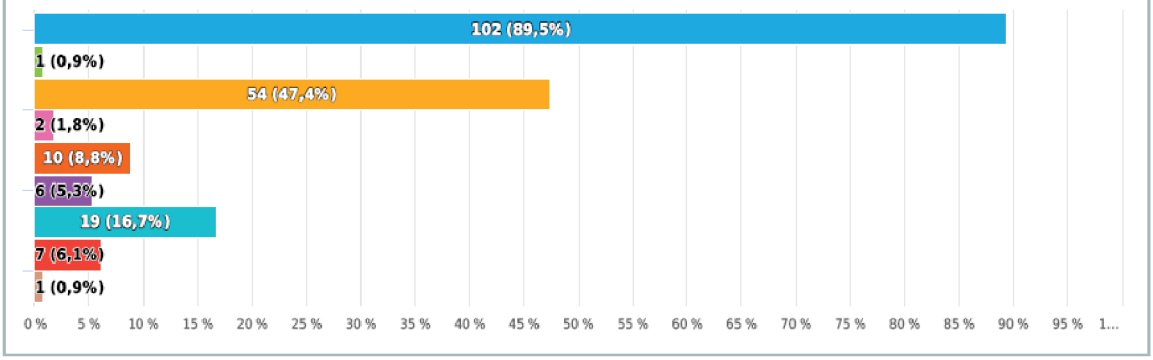


Obrázek 18 – osobní zkušenost se zařízením nebo systémem využívajícím biometrii [Zdroj: Autor]

V případě otázky č. 6, která cílila na to, které konkrétní druhy biometrik jsou respondentům známy, popř. jaké z uvedených druhů respondenti aktivně využívají, zcela dominantně převládl otisk prstu. V tomto případě bylo možné zvolit více než jednu možnost odpovědi, z toho důvodu pak absolutní hodnoty,

i procentní zastoupení jednotlivých druhů biometrik překračují v součtu celkový počet respondentů, resp. hodnotu 100 %. Dle hodnot znázorněných na obrázku č. 19 je s drtivou převahou na prvním místě zastoupený již zmíněný otisk prstu s poměrem 89,5 % hlasů, na pomyslné druhé pozici se 47,4 % hlasů biometrika obličeje a třetí nejvyšší zastoupení s 16,7 % zaujímá hlas jako biometrický identifikátor. Ostatní druhy biometrik ještě snad s výjimkou oka, zastoupeného v úhrnu 14,1 % hlasů, z čehož připadá 8,8 % pro oční duhovku, resp. 5,3 % pro oční sítnici, jsou mezi širokou veřejností spíše neznámé.

Možnosti odpovědí	Responzí	Podíl
Otisk prstu	102	89,5%
Geometrii ruky	1	0,9%
Obličej	54	47,4%
Žilní obraz dlaně/prstu	2	1,8%
Oční duhovku	10	8,8%
Oční sítnici	6	5,3%
Hlas	19	16,7%
Dynamiku chůze	7	6,1%
Jiný...	1	0,9%



Obrázek 19 – povědomí o jednotlivých druzích biometrických identifikátorů [Zdroj: Autor]

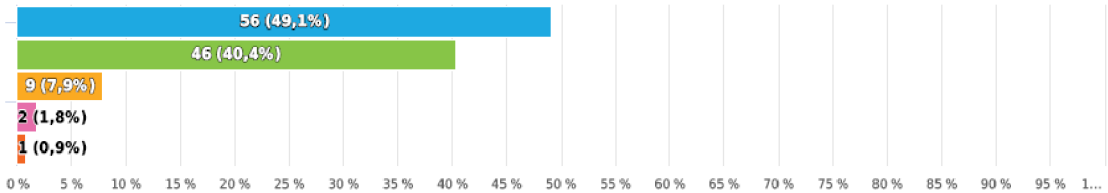
6.3 Bezpečnost a subjektivní vnímání jednotlivých biometrik

Na oblast subjektivního vnímání biometrických technologií byly zaměřeny otázky č. 10 a 11, které jsou doplněny ještě otázkou č. 7, jejímž cílem bylo zjistit,

jak společnost vnímá hledisko bezpečnosti biometrie. Odpověď na otázku, zda respondenti vnímají biometrii jako bezpečnou technologii nám poskytuje obrázek č. 20.

Ze získaných dat je patrné, že naprostá většina představující v souhrnu 89,5 % všech respondentů vnímá technologii založenou na biometrické identifikaci buďto jako zcela bezpečnou 49,1 %, nebo spíše bezpečnou 40,4 %. Pouze 3 respondenti představující zanedbatelné 2,7 % nepovažují využití biometrie za bezpečné. Ucelený názor, zda je či není biometrie bezpečná, nemá 7,9 % respondentů, kteří zvolili možnost „Nevím“. Z uvedených dat je možné konstatovat, že je biometrie a její použití v rámci identifikačních a autentizačních aplikací společností vnímána převážně pozitivně jako bezpečná technologie.

Možnosti odpovědí	Responzí	Podíl
Ano	56	49,1%
Spíše ano	46	40,4%
Nevím	9	7,9%
Spíše ne	2	1,8%
Ne	1	0,9%

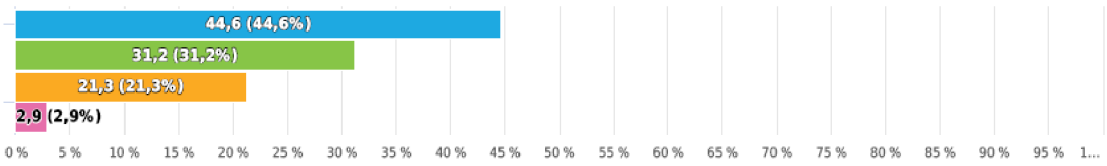


Obrázek 20 – obecné vnímání bezpečnosti biometrie [Zdroj: Autor]

Odpovědi na následující otázku č. 10 poskytují informace, jaké priority, resp. jaká hlediska by byla pro respondenty nejpodstatnější při výběru biometrické technologie. V tomto případě byla respondentům poskytnuta možnost rozdělení přidělených 100 bodů mezi nabízené čtyři varianty v závislosti na tom, které hledisko je pro ně nejpodstatnější a které méně podstatné. Z následujícího obrázku č. 21 je možné vypozorovat, že pro respondenty je na prvním místě uživatelský komfort, který získal v průměru 44,6 % bodu. Druhé nejvýznamnější hledisko je zastoupeno průměrnou hodnotou 31,2 % bodu, a je jím rychlost a přesnost zařízení při samotném ověření. Poněkud překvapivě až na pomyslné

třetí příčce je s 21,3 % bodu zastoupena bezpečnost. Z tohoto výsledku lze usuzovat, že nemalé procento respondentů má tendenci podceňovat bezpečnost biometrických dat. Popřípadě si plně neuvědomují rizika spojená s případnou ztrátou či zneužitím svých biometrických dat. Částečně však lze vypozorovat souvislost mezi tímto třetím místem a výsledky odpovědí na předchozí otázku č. 7, která cílila na obecné vnímání bezpečnosti biometrie, kdy téměř 90 % respondentů odpovědělo, že vnímá biometrii jako bezpečnou.

Odpověď	Průměr	Podíl
Uživatelský komfort	44,6	44,6%
Rychlost a přesnost ověření	31,2	31,2%
Bezpečnost zpracovávaných dat	21,3	21,3%
Možnost osobního vyzkoušení nové technologie.	2,9	2,9%



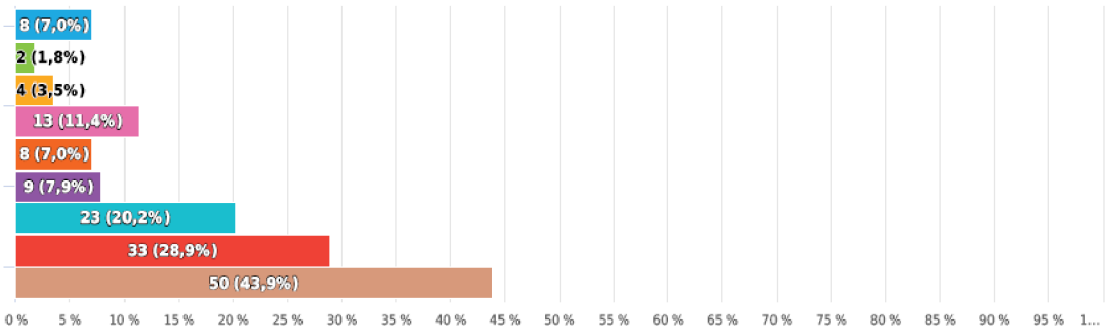
Obrázek 21 – subjektivní míra důležitosti uvedených hledisek při výběru biometrické technologie [Zdroj: Autor]

Následující otázka č. 11 měla za cíl zjistit, zda je některý z osmi nabídnutých nejběžnějších druhů biometrik používaných v rámci identifikačních a autentizačních prvků instalovaných v biometrických aplikacích pro respondenty přímo neakceptovatelný. Respondenti měli obdobně jako v případě otázky č. 6 možnost zvolit více než jednu variantu odpovědi, z toho důvodu pak absolutní hodnoty, i procentní zastoupení jednotlivých nabízených biometrik překračují v součtu celkový počet respondentů, resp. hodnotu 100 %. Tyto varianty jsem ještě doplnil o odpověď, která vyjádřila bezproblémové akceptování všech předložených druhů nejběžnějších biometrik. Jak je patrné z obrázku č. 22 tak tato možnost získala nejvyšší počet hlasů. Celkem tedy 50 respondentů by plně akceptovalo jakoukoli z osmi nabídnutých biometrik.

Na druhé straně plných 64 respondentů vnímá alespoň jednu z nabízených variant běžně užívaných biometrik jako subjektivně neakceptovatelnou. Poněkud překvapivě se jako nejméně přijatelná pro tyto respondenty jeví behaviorální

biometrická metoda dynamiky chůze, která získala 28,9 % hlasů. Za druhý nejméně akceptovatelný druh biometriky označili respondenti hlas, který získal 20,2 % hlasů. Třetí nejvyšší procentní podíl hlasů získala s 11,4 % biometrika žilního obrazu dlaně/prstu. Je otázkou, z jakého důvodu tomu tak je? Možná panuje obava z vysoké chybovosti či falešného přijetí neoprávněné osoby, popř. neznalosti možností jednotlivých technologií. V každém případě by pro konkrétnější závěr bylo zapotřebí provést další výzkum zaměřený podrobněji na tuto problematiku.

Možnosti odpovědí	Responzí	Podíl
Otisk prstu	8	7,0%
Geometrie ruky	2	1,8%
Obličej	4	3,5%
Žilní obraz dlaně/prstu	13	11,4%
Oční duhovka	8	7,0%
Oční sítnice	9	7,9%
Hlas	23	20,2%
Dynamika chůze	33	28,9%
Všechny uvedené biometriky vnímám jako akceptovatelné.	50	43,9%



Obrázek 22 – biometrické identifikátory vnímané jako neakceptovatelné [Zdroj: Autor]

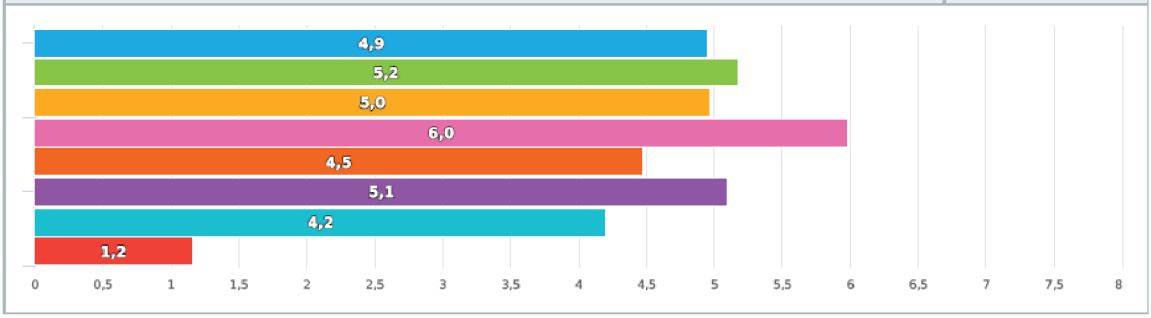
6.4 Vnímání biometrie v kontextu profesního života

Soubor zbývajících čtyř otázek, které představují otázky č. 8–9 a otázky č. 12–13, je zaměřen na vnímání užití biometrie v rámci aplikací dotýkajících se především profesního života respondentů. Z odpovědí je možné si vytvořit názor, jakým způsobem by pravděpodobně bylo rozhodnutí o instalaci biometrického

systému přijato ze strany zaměstnanců, do jaké míry je pravděpodobné, že by byli zaměstnanci ochotni poskytnout své biometrické údaje zaměstnavateli ke zpracování a také, které druhy biometrické identifikace se z pohledu zaměstnanců jeví jako nejpřijatelnější.

Obecnou rovinu, jakým způsobem by v případě možnosti volby chtěli být respondenti v rámci vnitropodnikové mobility ověřováni, je možné vyčíst z odpovědí na otázku č. 8, které jsou zobrazeny níže na obrázku č. 23. V tomto případě bylo respondentům nabídnuto celkem osm možných variant ověření své identity v rámci běžné každodenní vnitropodnikové autentizace. Jednotlivé varianty měli respondenti seřadit od subjektivně nejvhodnějšího po nejméně vhodný způsob ověřování.

Odpověď	Důležitost
Průkaz s fotografií předkládaný vrátnému/ostraze.	4,9
Čipovou kartu/čip	5,2
PIN - zadávání osobního číselného kódu	5,0
Biometrický identifikátor	6,0
Kombinaci čipové karty/čipu + PIN	4,5
Kombinaci biometrického identifikátoru + PIN	5,1
Kombinaci biometrického identifikátoru + čipové karty/čipu	4,2
Jinou zde neuvedenou.	1,2

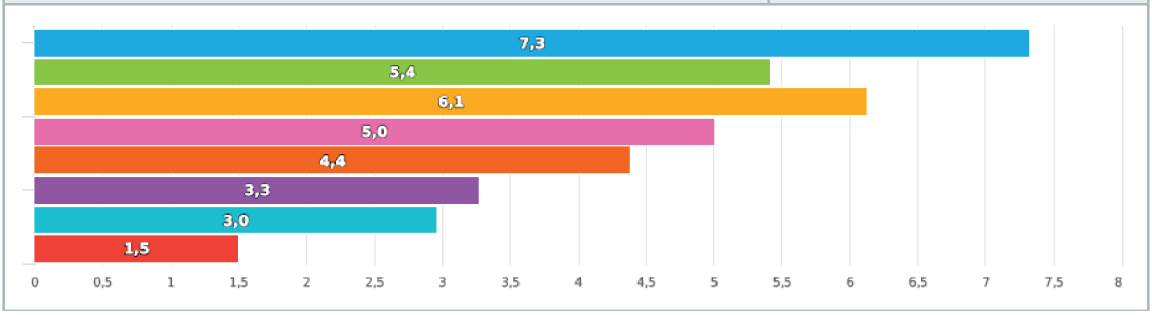


Obrázek 23 – výběr nejvhodnější formy vnitropodnikové autentizace [Zdroj: Autor]

Výsledky odpovědí na otázku č. 8 však bohužel nepřinášejí bližší informace o konkrétním preferovaném způsobu ověřování, byť lze pozorovat mírnou inklinaci k biometrii, popř. kombinaci biometrie s některým z dalších způsobů ověření. Z výsledků je nicméně patrná značná, až překvapující variabilita vnímání ideálního prostředku či způsobu ověření své osoby v rámci rutinní profesní mobility.

Následující otázka č. 9 představovala pomyslnou nadstavbu předešlé otázky č. 8 s tím, že však cílila pouze na výběr konkrétní biometriky, kterou by respondenti upřednostnili pro své ověření v rámci použití ve svém zaměstnání. Také u této otázky měli respondenti seřadit jednotlivé možnosti dle subjektivního vnímání, obdobně jako u předchozí otázky č. 8. V tomto případě, jak je také možné vyčíst z obrázku č. 24, je mezi odpověďmi nejvíce zastoupena hodnotou 7,3 bodu z osmi možných biometrická metoda ověření prostřednictvím otisku prstu. Druhou nejpreferovanější biometriku se ziskem 6,1 bodu představuje obličej. Také geometrie ruky 5,4 bodu a oční duhovka 5,0 bodů jsou biometriky, které společnost vnímá relativně pozitivně. Naproti tomu, zcela opačně jsou respondenty vnímány biometriky hlas a dynamika chůze, které v tomto případě získaly pouhé 3 body, resp. 1,5 bodu.

Odpověď	Důležitost
Otisk prstu	7,3
Geometrie ruky	5,4
Obličej	6,1
Oční duhovku	5,0
Oční sítnici	4,4
Žilní obraz dlaně/prstu	3,3
Hlas	3,0
Dynamiku chůze	1,5

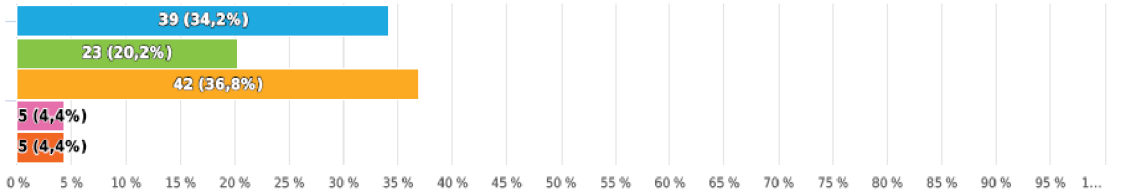


Obrázek 24 – výběr nejvhodnější biometriky [Zdroj: Autor]

Otázka č. 12 cílila na problematiku ochoty poskytnout svá biometrická data a udělení souhlasu s jejich zpracováním zaměstnavateli za účelem jejich využití v docházkovém a přístupovém systému, popř. pro automatické ovládání zabezpečení budov. Z obrázku č. 25 lze vyčíst, že nadpoloviční většina tvořící v součtu 54,4 % by s poskytnutím svých biometrických dat zaměstnavateli neměla

buď žádný problém 34,2 %, nebo by tento souhlas ochotně poskytla výměnou za vyšší uživatelský komfort 20,2 %. Značná část respondentů 36,8 % by pro své rozhodnutí poskytnout biometrická data a udělit souhlas s jejich zpracováním potřebovala znát podrobnější informace a okolnosti využití těchto dat. Z uvedeného je zřejmé, že více než třetina respondentů si skutečně uvědomuje značnou citlivost svých biometrických dat a před jejich poskytnutím a udělením souhlasu se zpracováním by vyžadovala bližší informace o účelu využití, popř. míře zabezpečení poskytnutých dat. Navzdory tomu však pouze necelá desetina ze všech respondentů již dopředu ví, že by své biometrické údaje neposkytla svému zaměstnavateli vůbec 4,4 %, nebo že by je spíše neposkytla, a to z důvodu toho, že v tyto technologie nemá dostatečnou důvěru 4,4 %.

Možnosti odpovědí	Responzí	Podíl
Ano, nemám s tím problém.	39	34,2%
Spíše ano, za ten komfort mi to stojí.	23	20,2%
Nevím, záleželo by na okolnostech.	42	36,8%
Spíše ne, nemám v tyto technologie důvěru.	5	4,4%
Ne	5	4,4%



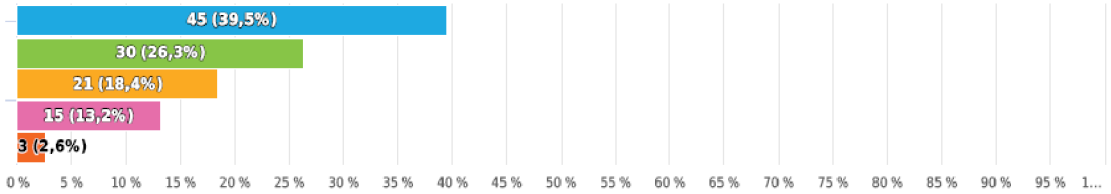
Obrázek 25 – ochota poskytnout biometrická data zaměstnavateli [Zdroj: Autor]

Otázka č. 13, která uzavírala celý dotazník, měla zjistit, jakým způsobem by respondenti vnímali zavedení biometrického systému pro automatickou správu a zabezpečení budov ve svém zaměstnání. Pro své odpovědi měli na výběr pět možností, ze kterých bylo možné vybrat pouze jednu nejvhodnější variantu. Jak je patrné z obrázku č. 26, tak výrazně nadpoloviční většina respondentů 65,8 % by zavedení systému, který by byl založen na biometrické autentizaci, vnímala pozitivně. Z čehož větší část zastoupená 39,5 % by takovou změnu vnímala jako krok správným směrem a praktické využití moderní technologie v praxi. Zbývající 26,3 % by takovou změnu kvitovala z důvodu usnadnění běžné rutiny, která je spojena s vnitropodnikovou mobilitou, zejména absenci nutnosti

nošení a používání některého z běžných typů identifikátorů (identifikační průkaz, čipová karta, RF čip).

Necelá pětina respondentů 18,4 % uvedla, že by je taková změna zásadněji nezasáhla a bylo by jim to jedno. Skupina, která by zavedení biometrického systému vnímala negativně a s nelibostí, představuje spíše menšinu a je zastoupena 15,8 %. Pouze pro 3 respondenty by instalace biometrického systému byla absolutně nepřijatelná do takové míry, že by zvažovali odchod a změnu zaměstnavatele.

Možnosti odpovědí	Responzí	Podíl
Krok správným směrem, je třeba jít s dobou a využívat moderní technologie.	45	39,5%
Kvitoval bych, že nemusím neustále nosit/hledat zaměstnaneckou kartu.	30	26,3%
Bylo by mi to jedno.	21	18,4%
Takovou změnu bych pociťoval spíše negativně a s nelibostí.	15	13,2%
Bylo by to pro mě absolutně nepřijatelné a zvažoval bych změnu zaměstnavatele.	3	2,6%



Obrázek 26 – vnímání instalace biometrického systému v zaměstnání [Zdroj: Autor]

6.5 Resumé

Z výsledků provedeného dotazníkového šetření, které je přílohou této diplomové práce, vyplývá, že biometrická identifikace a autentizace je vnímána ve společnosti vesměs pozitivně. Zcela nepochybně na tom, jak společnost relativně dobře využití biometrie vnímá, má skutečnost, že použití sebe sama jako klíče či autentizačního prvku je velice komfortní a svým způsobem návykové. Je příjemným překvapením, v jakém rozsahu je biometrie využívána i ze strany zaměstnavatelů, ať již v rámci evidence docházky či řízení přístupu a zabezpečení majetku. Provedený výzkum jasně ukazuje, že některé druhy biometrik nejsou společnosti prozatím příliš známy a jejich širší použití pravděpodobně teprve v budoucnu přijde. Například respondenty poměrně

zatracovaná technologie autentizace prostřednictvím dynamiky chůze se dle posledních výzkumů a nasazení v pilotních projektech na letištích ukazuje jako velice vhodná a efektivní, s velmi nízkými hodnotami FAR a FRR. Naopak je patrné, že například nejčastěji používané biometriky, představující otisk prstu či obličej, jsou již široce rozšířeny a hojně využívány napříč společností.

Z provedeného výzkumu je také zjevné, že ne všichni uživatelé systémů a zařízení umožňující zejména biometrickou autentizaci si jsou vědomi případných rizik spojených se ztrátou či zneužitím poskytnutých biometrických dat. Biometrie je v drtivé většině případů vnímána společností jako bezpečná technologie, což je dobře pro její další úspěšné rozšíření. Ovšem i přesto je vždy nutné se zajímat o důvody a účel využití poskytovaných biometrických identifikátorů, neboť jejich zneužití či ztráta mohou způsobit osobě značné škody a komplikace, popř. mohou navždy znemožnit další bezpečné použití odcizeného identifikátoru. Jak již bylo naznačeno v kapitole 3.5, při odcizení např. biometrické šablony otisku prstu nikomu nový prst nenaroste, popř. si poškozený nedokáže změnit strukturu papilárních linií pro budoucí opětovné bezpečné používání dotčené biometriky.

V případě použití biometrické autentizace v aplikacích, které se dotýkají profesního života respondentů, lze konstatovat, že pokud bude zaměstnavatelem použití biometrického systému dostatečně odůvodněno a bude zajištěna bezpečnost poskytnutých biometrických dat, bude takový krok zaměstnanci vnímán vesměs pozitivně. A díky vyšší míře komfortu a efektivitě budou z takového kroku profitovat obě strany současně.

III PRAKTICKÁ ČÁST B
(návrh biometrického systému)

7 PŘEDSTAVENÍ PROJEKTU

Vlastní návrh systému pracujícího na základě biometrické identifikace a autentizace bude zakomponován do projektu komplexního zabezpečení objektu střední velikosti, který představuje sídlo a zázemí bezpečnostní agentury Červ Security, který jsem v minulosti zpracoval pro účely praktické části své bakalářské práce. Cílem této části diplomové práce je doplnění, resp. upgrade systémů PZTS, EKV a CCTV, při kterém bude realizována výměna některých koncových, ovládacích a snímacích prvků za prvky umožňující primárně biometrickou autentizaci. Při návrhu biometrického systému, volbě jednotlivých prvků a technologií bude přihlédnuto k výsledkům provedeného dotazníkového šetření tak, aby výsledná realizace stále odpovídala původnímu účelu, ale současně se zvýšila efektivita celého systému, uživatelský komfort a bylo zajištěno dobré akceptování ze strany dotčených uživatelů, resp. zaměstnanců.

Návrh biometrického systému bude postaven na aktuálně dostupných technologiích, bez ohledu na jejich finanční náročnost. Komerční realizace samozřejmě podobný přístup nedovoluje a je vždy nutné na samém počátku projektování jakéhokoli systému stanovit jak požadavky zákazníka na zabezpečení a funkcionalitu, tak provést podrobnou analýzu rizik, a především zajistit odpovídající objem finančních prostředků potřebných pro realizaci celého projektu.

Úvodní pasáž bude věnována popisu celého objektu a aktuálně použitým prvkům, které jsou zahrnuty v původním zpracovaném projektu. Následně budou vybrána nejvhodnější místa a komponenty, které by bylo vhodné nahradit biometrickými prvky. Současně bude zvolena vhodná biometrická technologie pro dané umístění a také výběr konkrétního nově instalovaného komponentu.

8 CHARAKTERISTIKA SOUČASNÉHO STAVU OBJEKTU

8.1 Popis objektu

Objekt bezpečnostní agentury Červ Security je složen ze dvou samostatně stojících panelových budov – jednopodlažní (obr. 27, 28) a dvoupodlažní (obr. 29, 30), které mezi sebou mají asfaltovou plochu, jenž je z části využívána pro parkování vozidel (obr. 31). Jednopodlažní budova (dále jen budova 1), která přímo sousedí s okolo vedoucí pozemní komunikací, má ve svém středu umístěná sekční vrata, jež slouží jako jediný vjezd do objektu (obr. 27). Součástí průjezdu je i vrátnice s nepřetržitou obsluhou a instalovaným dohledovým poplachovým přijímacím centrem – DPPC, kde jsou přijímány veškeré informace ze všech instalovaných systémů PZTS, EKV, CCTV a EPS (obr. 27, 31). Zbylé prostory budovy 1 jsou využívány jako skladové prostory, které jsou přístupné pouze z vnitřní strany objektu. Jednotlivé prostory jsou uzavřené plechovými vraty a jejich střežení je zajištěno prostředky PZTS, které je možné ovládat instalovanými RF čtečkami s klávesnicí, umístěnými na plášti budovy (obr. 28, 31). Druhá, protilehlá dvoupodlažní budova (dále jen budova 2) je ve své přízemní části využívána pro parkování vozidel, umístění PHM a dalších technických zařízení firmy. Také tyto prostory jsou zajištěny prvky sytému PZTS a k jejich aktivaci a deaktivaci jsou použity identické RF čtečky s klávesnicí, instalované na plášti budovy mezi jednotlivými garážemi (obr. 29, 30, 31). V celém 1. patře téže budovy se nachází kancelářské prostory, zbrojní sklad a také místnost pro práci s finanční hotovostí včetně trezoru pro její ukládání. Tyto prostory jsou střeženy řadou prvků systémů PZTS a CCTV (viz obr. 29, 30, 32). Ovládání a nepřetržitý dohled je realizován z prostor DPPC umístěného ve vrátnici (obr. 31). Možnost aktivace a deaktivace systému PZTS poskytuje též ovládací klávesnice umístěná na schodišti u vstupní mříže do 1. patra (obr. 32). Celý objekt je též monitorován prostřednictvím souboru kamer systému CCTV. Obě budovy jsou mezi sebou vzájemně propojeny pod úrovní terénu malým kolektorem, který je účelně využit pro skrytou a chráněnou instalaci potřebné kabeláže. (obr. 31). Veškeré instalované prvky systémů, které budou úpravou dotčeny (PZTS, CCTV, EKV),

jsou přehledně rozepsány i s jejich konkrétním umístěním v následujících tabulkách 8.2, 8.3, 8.4.

8.2 Aktuálně instalované prostředky PZTS

Tabulka 3 – soupis prvků PZTS [Zdroj: Autor]

UMÍSTĚNÍ	POPIS PRVKU	Bezpečnostní stupeň	Počet kusů
Budova 1 vrátnice	Ústředna celé instalace PARADOX DIGIPLEX EVO 192.	3	1
Budova 1 vrátnice	Dotykový ovládací panel ústředny s grafickým zobrazením stavu celého systému a jednotlivých zón PARADOX TM70. Lze zobrazit až 32 půdorysů s osazenými prvky a jejich stavem, historii událostí a detaily konkrétní události.	3	1
Budova 1 vrátnice	PIR čidlo PARADOX NV75MX se 2x zdvojeným senzorem, aktivním IR antimaskingem a tamperem proti sejmutí ze zdi, které využívá technologii kombinující lomené zrcadlo a Fresnelovu čočku. Dosah až 16 m/90°.	3	1
Budova 1 vrátnice	Výklopný tísňový hlásič SENTROL S 3045.	X	1
Budova 1 vrátnice	Magnetický polarizovaný okenní kontakt VAR-TEC 3G-SM-60 čtyřvodičový s tamperem.	3	2
Budova 1 vrátnice	Elektromechanický zámek s monitorováním stavu VAR-TEC DZS-12VDC.	3	1
Budova 1	Bezdotyková čtečka s klávesnicí PARADOX R915 s audio-optickou signalizací (led/bzučák).	3	2
Budova 1 vrátnice	Dveřní magnetický kontakt pro průmyslové využití VAR-TEC MET – 300T s pancéřovou chráničkou na kabely.	2	1

Tabulka 3 – soupis prvků PZTS (pokračování)

Budova 1 vjezd	Vratový magnetický přejezdový kontakt VAR-TEC 3G-SM-85MET s tamperem a pancéřovou chráničkou na kabely.	3	1
Budova 1	Signalizační dioda JUMBO LED.	X	1
Budova 2 přízemí	Vratový magnetický přejezdový kontakt VAR-TEC 3G-SM-85MET s tamperem a pancéřovou chráničkou na kabely.	3	4
Budova 2 přízemí	Stropní PIR čidlo TEXECOM Premier Elite AM360QD s quad senzorem a aktivním IR antimaskingem. Čidlo má dvojitý tamper (ochrana proti otevření a sejmutí ze stropu).	3	4
Budova 2 přízemí	Bezdotyková čtečka s klávesnicí PARADOX R915 s audio-optickou signalizací (led/bzučák).	3	2
Budova 2 přízemí vchod	Elektromechanický zámek s monitorováním stavu VAR-TEC DZS-12VDC.	3	1
Budova 2 1. patro mříž	Magnetický polarizovaný dveřní kontakt VAR-TEC 3G-SM-70MET s tamperem a pancéřovou chráničkou na kabely.	3	1
Budova 2 1. patro mříž	Elektromechanický zámek s monitorováním stavu VAR-TEC DZS-12VDC.	3	1
Budova 2 1. patro/perim.	Dvousměrné PIR čidlo PARADOX NV780MX s aktivním IR antimaskingem obsahující 4 dvojité PIR snímače, vytvářející buď záclonu, nebo paprsek na každou stranu. Dosah 12 m.	3	2/2
Budova 2 1. patro	Duální PIR+MW čidlo MAXIMUM SECURITY GUARD s dvojitým PIR senzorem, aktivním IR antimaskingem a tamperem. Možnost nastavení citlivosti PIR a MW zvlášť. Dosah 12 m/110°.	3	6

Tabulka 3 – soupis prvků PZTS (pokračování)

Budova 2 1. patro	Magnetický polarizovaný okenní kontakt VAR-TEC 3G-SM-60 čtyřvodičový s tamperem.	3	7
Budova 2 1. patro finance/SZ	Digitální audio detektor tříštění skla PARADOX DG457 analyzující prolomení tabule skla a následné tříštění skla. Dvě úrovně citlivosti.	2	2
Budova 2 1. patro finance	Výklopný tísňový hlásič SENTROL S 3045.	X	1
Budova 2 1. patro trezor	Trezorový seismický detektor ALARMTECH VD500 s všesměrovou vibrační, termickou a piezootřesovou detekcí.	3	1
Budova 2 1. patro mříž	Ovládací klávesnice PARADOX K641+ s dvouřadým displejem pro zobrazení stavu zón.	3	1
Budova 2 1. patro schodiště	PIR čidlo RISCO iWISE RK800Q-G3 se 2x zdvojeným senzorem, aktivním IR antimaskingem a dvojitým tamperem (ochrana proti otevření a sejmutí ze stěny). Dosah až 15 m/100°.	3	1
Budova 2 1. patro	Signalizační dioda JUMBO LED.	X	7
Budova 2 1. patro fasáda	Signalizační venkovní siréna BELL-TEC MINI zálohovaná s akusticko-optickou signalizací a tamperem.	X	1

8.3 Aktuálně instalované prostředky EKV

Tabulka 4 – soupis prvků EKV [Zdroj: Autor]

UMÍSTĚNÍ	POPIS PRVKU	Bezpečnostní stupeň	kusů
Budova 1 vjezd	Čtečka karet a přívěsků SEBURY R3 pracující s komunikátory na frekvenci 125 kHz. Možnost zapojení do ústředny DIGIPLEX EVO.	x	2
Budova 2 přízemí	Bezdotyková čtečka s klávesnicí PARADOX R915 s audio-optickou signalizací (led/bzučák).	3	1

8.4 Aktuálně instalované prostředky CCTV

Tabulka 5 – soupis prvků CCTV [Zdroj: Autor]

UMÍSTĚNÍ	POPIS PRVKU	kusů
Budova 1 perimetr	Venkovní 4Mpix IP kamera DAHUA IPC-HFW3441E-AS - 3,6 mm s fixním objektivem, IR přísvitem do 50 m, IP67, napájení PoE, možnost detekce pohybu.	4
Budova 1 vrata vjezd	Venkovní 2Mpix IP kamera DAHUA IPC-HFW5241T-ASE BLACK - 2,8 mm s širokoúhlým fixním objektivem, IR přísvitem 80 m, inteligentní funkcí detekce osob, vozidel a obličejů, dále s funkcí počítání osob, přidání a odebrání předmětu.	1
Budova 1 vrátnice	Videomatice DAHUA M70-D-H pro zpracování obrazu 16x full HD, 4x poplachový vstup/výstup, funkce zoom/sloučení/přesouvání/překrytí obrazu, záznam na HDD.	1
Budova 1 vrátnice	Zobrazovací monitor DAHUA DHL32" LCD 24/7, full HD obraz, určeno pro nepřetržitý provoz.	2
Budova 1 vrátnice	Ovládací klávesnice HIKVISION DS-1005KI k NVR, možnost zapojení přímo do USB, joystick pro ovládání PTZ kamery s rotací pro zoom, 15 tlačítek pro předvolbu.	1

Tabulka 5 – soupis prvků CCTV (pokračování)

Budova 2 perimetr	Venkovní 4Mpix IP kamera DAHUA IPC-HFW3441E-AS - 3,6 s fixním objektivem, IR přísvitem do 50 m, IP67, s možností detekce pohybu.	1
Budova 2 1. patro chodba	Vnitřní 2Mpix IP kamera DAHUA IPC-HFW5241T-ASE - 2,8 mm s širokoúhlým fixním objektivem, IR přísvitem 80 m, s inteligentní funkcí detekce osob, rozpoznání obličejů, dále počítání osob, přidání/odebrání předmětu, detekcí průchodu a vstupu do vyznačeného prostoru.	1
Budova 2 1. patro finance/SZ	Vnitřní dome 2Mpix IP kamera DAHUA IPC-HDBW5241R-ASE - 2,8 mm s širokoúhlým fixním objektivem, IR přísvitem 50 m, s inteligentní funkcí detekce osob, rozpoznání obličejů, dále počítání osob, přidání/odebrání předmětu, detekcí průchodu a vstupu do vyznačeného prostoru.	2
Budova 2 střecha	Venkovní PTZ 2Mpix IP kamera DAHUA SD49225T-HN s motorickým objektivem a až 25x zoom, IR přísvitem 100 m, IP 66, s detekcí přidání/odebrání předmětu, průchodu a vstupu do vyznačeného prostoru.	1

9 NÁVRH ÚPRAV JEDNOTLIVÝCH SYSTÉMŮ

Veškeré zvolené biometrické prvky jsou vybrány s ohledem na kompatibilitu s původní instalací, aby zamýšlený upgrade mohl být případně realizován v co nejkratším časovém horizontu a také s minimálními technickými úpravami. Navrhované řešení, použité prvky a zvolené technologie však nepředstavují jediný možný způsob přechodu na systémy využívající biometrii, ale pouze jednu z možných variant takové úpravy. V následujících kapitolách 9.1, 9.2, 9.3 jsou představeny zamýšlené biometrické prvky po jednotlivých systémech a vždy na konci každé kapitoly věnované konkrétnímu systému je uvedena přehledová tabulka použitých prvků s popisem a umístěním. Následně je pro ucelený přehled v kapitole 9.4 přiloženo grafické zobrazení celého komplexu budov s veškerými instalovanými technologiemi.

9.1 Biometrické prvky PZTS

Budova 1

Aktivace a deaktivace střežení jednotlivých skladových prostor bude zajištěna prostřednictvím dvou kombinovaných čteček otisků prstů ZKTeco MA300, které nahradí v současné době instalované ovládací klávesnice PARADOX R915 (obr. 28, 31), každá pro obsluhu jednoho páru vrat v dané polovině budovy.

Budova 2

V přízemí budovy 2 bude obdobně mezi každým párem sekčních garážových vrat instalována kombinovaná čtečka otisků prstů ZKTeco MA300. Nahradí tak původní ovládací klávesnice PARADOX R915, které sloužily k aktivaci a deaktivaci systému PZTS v garážích (obr. 29, 31).

V 1. patře bude aktivace a deaktivace systému PZTS v jednotlivých místnostech, ale i skladu zbraní a místnosti pro práci s finanční hotovostí, zajištěna prostřednictvím společného biometrického snímače oční duhovky Iris ID iCAM 7101, který bude umístěn v chodbě vedle dveří do skladu zbraní (obr. 32). Aktuálně provozovaná ovládací klávesnice PARADOX K641+, umístěná na stěně před vstupní mříží, (obr. 32) bude ponechána jako záložní.

Tabulka 6 – soupis biometrických prvků PZTS [Zdroj: Autor]

UMÍSTĚNÍ	POPIS PRVKU	Bezpečnostní stupeň	kusů
Budova 1	Kombinovaná čtečka otisků prstů a čipových karet 125 kHz ZKTeco MA300 s kapacitou až 1500 otisků/karet s releovým výstupem a tamperem	3	2
Budova 2 přízemí	Kombinovaná čtečka otisků prstů a čipových karet 125 kHz ZKTeco MA300 s kapacitou až 1500 otisků/karet s releovým výstupem a tamperem	3	2

Tabulka 6 – soupis biometrických prvků PZTS (pokračování)

Budova 2 1. patro	Kombinovaný skener oční duhovky Iris ID iCAM 7101 umožňující sken obou očí ze vzdálenosti 31-35 cm. Integrovaná čtečka čipových karet a možnost použití PIN kódu na virtuální klávesnici. Zajištění správy zabezpečených oblastí, ale i evidenci docházky. Komunikace ethernet (LAN, WAN), RS 232 pouze vstup, RS 422 pouze výstup	3	1

9.2 Biometrické prvky CCTV

Součástí biometrického sytému bude též kamera DAHUA IPC-HFW5241T-ASE-2,8 mm snímající prostory schodiště, resp. oblast vstupní mříže oddělující schodiště od zabezpečené oblasti 1. patra (obr. 32), která umožní autentizaci příchozích osob. Následně prostřednictvím propojení s ústřednou PARADOX DIGIPLEX EVO 192 bude zajišťovat deaktivaci prvků PZTS ve společné chodbě v 1. patře a současně bude ovládat elektromechanický zámek VAR-TEC DZS-12VDC vstupní mříže. Díky skutečnosti, že pro původní realizaci byl zvolen vhodný typ kamer, bude možné požadovanou kameru využít v rámci biometrického systému bez nutnosti její výměny. Pro tento účel bude zapotřebí pouze doinstalace softwarového balíčku, který zpřístupní požadované funkce.

Tabulka 7 – soupis biometrických prvků CCTV [Zdroj: Autor]

UMÍSTĚNÍ	POPIS PRVKU	kusů
Budova 1 vrátnice	Softwarový balíček	1

9.3 Biometrické prvky EKV

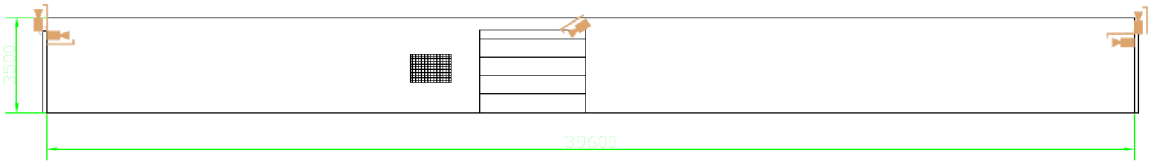
Vstup do prostor vrátnice bude nyní realizován prostřednictvím kombinované čtečky otisků prstů ZKTeco MA300, která bude umístěna vedle vstupních dveří vrátnice a zajistí ovládání elektromechanického zámku VAR-TEC DZS-12VDC, který je osazen na dveřích vrátnice (obr. 31). Ovládání identického zámku, který je i součástí vstupních dveří budovy 2, bude taktéž zajištěno prostřednictvím kombinované čtečky otisků prstů ZKTeco MA300, která nahradí v současné době instalovanou ovládací klávesnici PARADOX R915. Součástí systému EKV bude i snímač oční duhovky Iris ID iCAM 7101, který mimo svůj hlavní úkol v systému PZTS zajistí také kompletní elektronickou evidenci docházky zaměstnanců (obr. 29, 31).

Tabulka 8 – soupis biometrických prvků EKV [Zdroj: Autor]

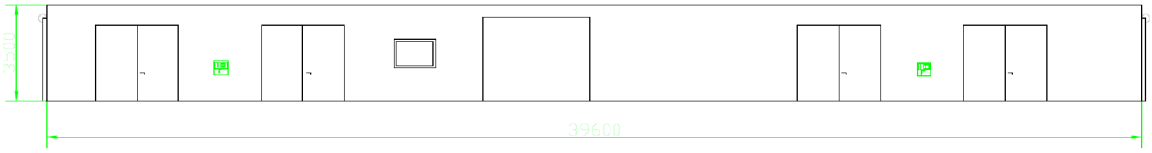
UMÍSTĚNÍ	POPIS PRVKU	Bezpečnostní stupeň	kusů
Budova 1 vrátnice	Kombinovaná čtečka otisků prstů a čipových karet 125 kHz ZKTeco MA300 s kapacitou až 1500 otisků/karet s releovým výstupem a tamperem	3	1
Budova 2 vchod	Kombinovaná čtečka otisků prstů a čipových karet 125 kHz ZKTeco MA300 s kapacitou až 1500 otisků/karet s releovým výstupem a tamperem	3	1

9.4 Zobrazení všech prvků v projektu

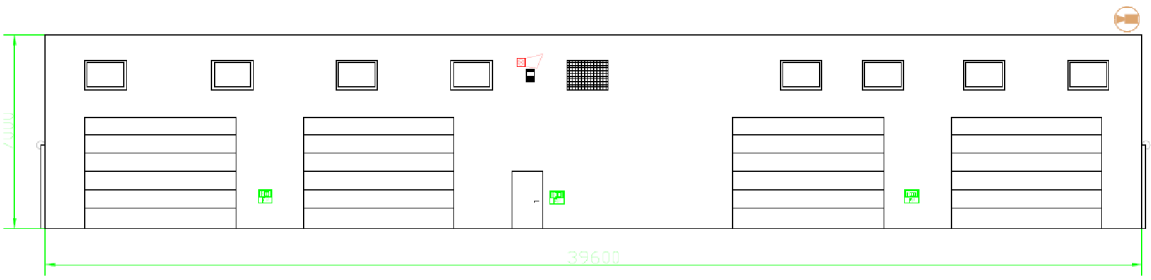
Následující grafické zobrazení vytvořené v programu AutoCAD, není zcela vyčerpávající, nicméně poskytuje přesný přehled umístění veškerých instalovaných prvků. Nezbytná instalace kompletní kabeláže, propojovací expandéry a záložní zdroje některých prvků nejsou z důvodu přehlednosti zakresleny. Primárně jsou prvky zobrazeny v půdorysech budovy, ostatní pohledy jsou víceméně přehledové pro ucelenou představu o velikosti, vzájemné poloze budov a dále poskytují detailnější přehled o umístění kamer CCTV a prvků ochrany perimetru. Součástí komplexního grafického zpracování je také stávající a neměněná instalace systému EPS.



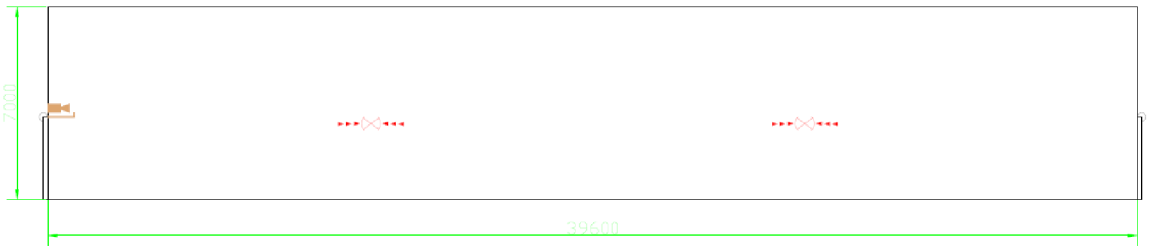
Obrázek 27 – budova 1 pohled z ulice [Zdroj: Autor]



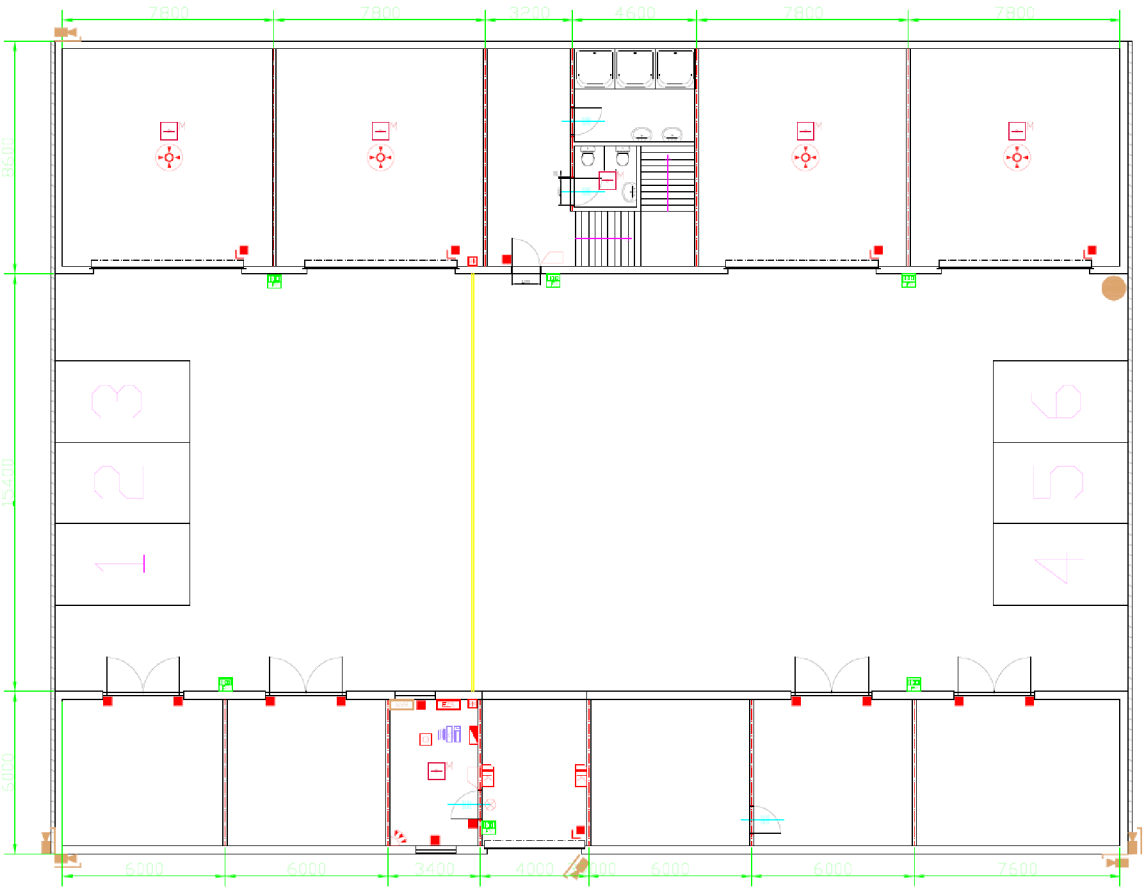
Obrázek 28 – budova 1 pohled z vnitrobloku [Zdroj: Autor]



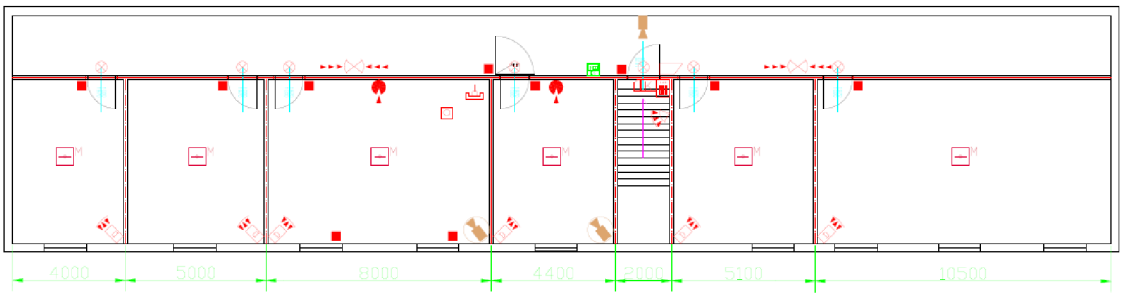
Obrázek 29 – budova 2 pohled z vnitrobloku [Zdroj: Autor]



Obrázek 30 – budova 2 pohled ze zadní strany [Zdroj: Autor]



Obrázek 31 – půdorys celý objekt přízemí [Zdroj: Autor]



Obrázek 32 – půdorys budova 2 1. patro [Zdroj: Autor]

Tabulka 9 – legenda k obrázkům 27–32 [Zdroj: Autor]

LEGENDA ZNAČEK EZS/EPS/ACCES/CCTV

EZS	ÚSTŘEDNA EZS		SIRÉNA S OPTICKOU SIGNALIZACÍ		MAGNETICKÝ KONTAKT		KÓDOVÁ KLÁVESNICE
	OVLÁDACÍ KLÁVESNICE EZS		OPTICKÁ SIGNALIZACE EZS		MAGNETICKÝ KONTAKT VRATOVÝ		ROZVODNÁ KRABIČKA
	INFRAPASIVNÍ DETEKTOR S ANTIMASKINGEM		TLAČÍTKOVÝ TÍSŇOVÝ HLÁSIČ		VENKOVNÍ DVOUSMĚR. PIR S ANTIMASKINGEM	M	MULTISENZOROVÝ HLÁSIČ EPS
	INFRAPASIVNÍ DETEKTOR STROPNÍ S ANTIM.		OTŘESOVÉ ČIDLO		KAMERA PEVNÁ VNITŘNÍ		DOOME KAMERA
D	DUÁLNÍ DETEKTOR PIR+MW S ANTIMASKINGEM	K	BEZDOTYKOVÁ ČTEČKA		KAMERA PEVNÁ VENKOVNÍ		DOOME KAMERA ANTIVANDAL
	AUDIO DETEKTOR TŘÍŠTĚNÍ SKLA		ELEKTRICKÝ DVEŘNÍ ZÁMEK	NVR	NVR ZÁZNAMOVÉ ZAŘÍZENÍ		PC
BIO FP	BIOMETRICKÁ ČTEČKA OTISKŮ PRSTŮ	BIO IC	BIOMETRICKÁ ČTEČKA OČNÍ DUHOVKY				

ZÁVĚR

Tato diplomová práce je zaměřena na využití biometrie v rámci komerční praxe. Zejména její využití v rámci systémů zajišťujících automatizovanou správu a zabezpečení budov. Práci jsem se rozhodl rozčlenit do tří postupně navazujících částí.

První teoretická část diplomové práce podává přehled o historii a postupném vývoji na poli biometrické identifikace. V této souvislosti jsem se zaměřil na nejvýznamnější milníky, které jsou spojené s identifikací člověka prostřednictvím jeho fyziologických markantů. Součástí teoretické části je vysvětlení základních pojmů, objasnění podmínek hodnocení a měření spolehlivosti biometrických prvků. V rámci teoretické části jsem se zaměřil také na důležité hledisko bezpečnosti biometrie a s tím související technické a právní normy, které upravují problematiku využití biometrie. Následně jsem vybral nejčastěji používané druhy biometrik, které byly blíže představeny v jednotlivých kapitolách. Zohledněny byly zejména faktory biometrické entropie a s tím spojená přesnost a spolehlivost, metody snímání a také metody následného zpracování získaných biometrických dat.

Druhou část diplomové práce představuje provedený výzkum, jenž byl realizován formou dotazníkového šetření v on-line prostředí. Dotazník, který je součástí této práce jako příloha, cílí svými 13 otázkami na 3 pomyslné okruhy zájmu. Prvním zájmovým okruhem je obecné povědomí respondentů o biometrii a jejich praktické zkušenosti s biometrickou identifikací. Druhý okruh přináší odpovědi na otázky jak společnost, resp. zúčastnění respondenti vnímají biometrii z hlediska bezpečnosti a uživatelské přívětivosti jednotlivých technologií. Třetí zájmový okruh je zaměřen na problematiku spojenou s využitím biometrie v rámci profesních aplikací, představující zejména ovládání koncových prvků přístupových a zabezpečovacích systémů. Získané výsledky byly využity pro výběr nejvhodnějších technologií v rámci úpravy bezpečnostního a přístupového systému modelového objektu.

Třetí část, resp. druhá polovina praktické části diplomové práce, spočívá ve vhodném zapracování biometrických prvků do jednotlivých systémů komplexně

zabezpečeného modelového objektu bezpečnostní agentury Červ Security, jež jsou v současné době založené na běžné identifikaci tokenem. Tato úprava byla provedena způsobem, který v maximální míře zohlednil výsledky vzešlé z provedeného šetření, při současném zachování původního účelu všech dotčených systémů. Cílem bylo zajistit modernizaci stávajících systémů a současně zvýšit jejich uživatelskou přívětivost, komfort a efektivitu.

Biometrie je v posledních letech skutečným fenoménem na poli bezpečnostních technologií a domnívám se, že v blízké budoucnosti se s aplikacemi, kde bude použit nějaký biometrický prvek, budeme setkávat čím dál častěji. Tento fakt byl také hlavním motivem při výběru tématu diplomové práce a jsem velmi rád, že jsem si jej mohl zvolit. Poznatky nabyté při zpracování této diplomové práce výrazně rozšířily mé znalosti o biometrii. Pevně věřím, že pro případné čtenáře mé diplomové práce budou zde prezentované informace užitečné a přínosné.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7

[2] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management II.* 1. vyd. Zlín: VeRBuM, 2012, 387 s. ISBN 978-80-87500-19-4

[3] DIEM, Walter. *Bezpečnostní zařízení.* Praha: Ikar, 2000, 111 s. ISBN 80-7202-604-6

[4] BASTIAN, Hans Werner. *Bezpečný dům a byt – Ochrana před vloupáním, požárem a škodami způsobenými vodou.* Praha: BETA, 2004, 80 s. ISBN 80-7306-171-6

[5] DRAHANSKÝ, Martin, ORSÁG, Filip. *Biometrie.* Brno: Computer Press, 2011, 294 s. ISBN 978-80-254-8979-6

[6] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: GRADA, 2008, 664 s. ISBN 978-80-247-2365-5

[7] ŠČUREK, Radomír. *Biometrické technologie – technické prostředky bezpečnostních služeb.* Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2015, 115 s. ISBN 978-80-248-3786-4

[8] UHLÁŘ, Jan. *Technická ochrana objektů – III. díl ostatní zabezpečovací systémy.* Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8

[9] ČESKÝ NORMALIZAČNÍ INSTITUT. *ČSN EN 50131-1 – Poplachové systémy – Elektrické zabezpečovací systémy – Část 1: Všeobecné požadavky*. Praha: ČNI, 1999, 53574

[10] ČESKÝ NORMALIZAČNÍ INSTITUT. *ČSN EN 50131-1 ed. 2 – Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky.* Praha ČNI, 2007, 78248

Elektronické zdroje:

[11] REYES, O.C., R.V. RODRIGUES, P. SCULLY a K.B. OZANYAN. *Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks* [online]. 2. Vol. 41. IEEE: Transactions on Pattern Analysis and Machine Intelligence, 2019, 285-296 [cit. 2021-12-01]. DOI: 10.1109/TPAMI.2018.2799847

[12] TAMILSELVI, M. a S. KARTHIKEYAN. *An ingenious face recognition system based on HRPSM_CNN under unrestrained environmental condition* [online]. Chennai, India: Sathyabama Institute of Science and Technology, 2021 [cit. 2021-11-29]. ISSN 1110-0168. DOI: https://doi.org/10.1016/j.aej.2021.09.043

[13] *www.slideserve.com: PPT – An Overview of Biometrics PowerPoint Presentation, free download – ID:1367072* [online]. [cit.17.11.2021]. Dostupné z: https://www.slideserve.com/vanessa/an-overview-of-biometrics-1367072

[14] *Kriminalistika.eu: Bertilone* [online]. [cit. 24.09.2021]. Dostupné z: https://www.kriminalistika.eu/muzeumzla/bertilon/bertilon.html

[15] Android-developers.googleblog.com: *Better Biometrics in Android P.* [online]. [cit.2.10.2021]. Dostupné z: https://android-developers.googleblog.com/2018/06/better-biometrics-in-android-p.html

[16] Recfaces.com: Biometric Authentication & Biometric Identification: Explained With Examples | RecFaces [online]. [cit.16.10.2021]. Dostupné z: https://recfaces.com/articles/biometric-authentication-identification#1

[17] CONNOR, P. a A. ROSS. *Biometric recognition by gait: A survey of modalities and features, Computer Vision and Image Understanding* [online]. 2018. Elsevier, 2018, 1-27 [cit. 2021-12-02]. Vol. 167. ISSN 1077-3142. DOI: https://doi.org/10.1016/j.cviu.2018.01.007

[18] IULA, A. *Biometric recognition through 3D ultrasound hand geometry* [online]. Vol. 111. Potenza, Italy: University of Basilicata, 2020 [cit. 2021-11-30]. ISSN 0041-624X. DOI: https://doi.org/10.1016/j.ultras.2020.106326

[19] Biometricke-ctecky.cz: Biometrie – Oko [online]. [cit. 18.11.2021]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

[20] PAVLÍK, Pavel. (2007), *Biometrie jako základ současné i budoucí identifikace a autentizace*. [online]. Kontakt, roč. 9, je 2, s. 427–430. [cit. 25.09.2021]. Dostupné z: https://kont.zsf.jcu.cz/pdfs/knt/2007/02/34.pdf

[21] SIERRO, A., P. FERREZ a P. RODUIT. UNIVERSITY OF APPLIED SCIENCES WESTERN SWITZERLAND. *Contact-less Palm/Finger Vein Biometrics* [online]. Sion, Switzerland: University of Applied Sciences Western Switzerland, 2015 [cit. 2021-11-30]. ISBN 978-3-8857-9639-8. DOI: 10.1109/BIOSIG.2015.7314596

[22] *www.law.muni.cz*: *Co všechno lze falsifikovat v digitálním světě aneb důkazy nejsou vždy důkazy* [online]. [cit.16.10.2021]. Dostupné z: https://www.law.muni.cz/dokumenty/40736

[23] BURGUÉS, J., J. FIERREZ, D. RAMOS, M. PUERTAS a J.O. GARCIA. Detecting Invalid Samples in Hand Geometry Verification Through Geometric Measurements. *2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics* [online]. Madrid, Spain: Univ. Autonoma de Madrid, 2010, 2010, **2010**(11), 1-6 [cit. 2021-11-30]. Dostupné z: https://www.javierburgues.com/publication/burgues-2010-detecting/

[24] ZHOU, Y., KUMAR, A. (2011), *Human identification using palm-vein images* [online]. IEEE Trans. Inf. Forensics Sec., **6**, (4), pp. 1259–1274. [cit.4.11.2021]. Dostupné z: http://www4.comp.polyu.edu.hk/~csajaykr/myhome/papers/TIFS2011_PalmVein.pdf

[25] History of Biometrics | Biometric Update [online]. [cit. 25.09.2021]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

[26] KOŽNER, P. Identifikace skenem duhovky: Sci-fi, nebo realita? *Vesmír* [online]. 2011, 10.2.2011, **2011**(90), 79-80 [cit. 2021-11-30]. Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/2011/cislo-2/identifikace-skenem-duhovky.html

[27] Explainer: Iris Recognition | Biometric Update [cit. 25.09.2021]. Dostupné z: https://www.biometricupdate.com/201206/explainer-iris-recognition

[28] MOHAMED, Hesham Hashim et al (2021), *J. Phys.: Conf. Ser.* 1804 012144. [online]. [cit.26.10.2021]. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/1804/1/012144/pdf

[29] *www.PBS.org: New iPhone May Have Fingerprint Authenticetion – Could It Be Hacked? | NOVA | PBS* [online]. [cit.17.11.2021]. Dostupné z: https://www.pbs.org/wgbh/nova/article/new-iphone-may-have-fingerprint-authentication-can-it-be-hacked/

[30] NPP. (2016). Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. [online]. [cit.2.10.2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679

[31] MUTHANA, H.H. (2019), Optimized biometric system based iris-signature for human identification. *International Journal of Advances in Intelligent Informatics* [online]. Baghdad: Mustansiriyah University, 2019, 273-284 [cit.20.11.2021]. ISSN 2442-6571 Dostupné z: https://core.ac.uk/download/pdf/268127039.pdf

[32] *platform.keesingtechnologies.com:* Palm vein authentication systems and its applications – Keesing Platform [online]. [cit.16.11.2021]. Dostupné z: https://platform.keesingtechnologies.com/palm-vein-authentication-systems-and-its-applications/

[33] EVANS, David & PARISH, Siobhan. (2015) *Predicting the First Recorded Set of Identical Fingerprints.* [online]. Journal of Interdisciplinary Science. Topic. 4. [cit.2.10.2021]. Dostupné z: https://www.researchgate.net/publication/274250949_Predicting_the_First_Recorded_Set_of_Identical_Fingerprints

[34] WU, W., ELLIOTT, S.J., LIN, S., SUN, S. and TANG, Y. (2020), *Review of palm vein recognition* [online]. IET Biom., 9: 1-10. [cit.4.11.2021]. DOI: https://doi.org/10.1049/iet-bmt.2019.0034

[35] SystemOnLine.cz: S přehledem ve světě informačních technologií [online]. [cit.10.10.2021]. Dostupné z: https://m.systemonline.cz/it-security/je-zpracovavani-biometrickych-dat-bezpecne.htm

[36] BHOWMIK, M.K., K. SAHA, S. MAJUMDER, et al. *Thermal Infrared Face Recognition: A Biometric Identification Technique for Robust Security system* [online]. India: 1Tripura University, 2011 [cit. 2021-11-30]. DOI: 10.5772/18986

[37] *Visible proofs: Forensic Views of the Body: Galleries: Biographies: Juan Vucetich (1858 – 1925)* [online]. [cit. 24.09.2021]. Dostupné z: https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/vucetich.html

[38] SULOVSKÁ, Kateřina. *Výzkum biometrických systémů z hlediska jejich důvěryhodnosti a integrity: Analýza změn ve vzorcích chůze*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 76 s. ISBN 978-80-7454-799-7. Dostupné také z: http://hdl.handle.net/10563/43763 Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav automatizace a řídicí techniky.

[39] Woodrow Bledsoe Originates of Automated Facial Recognition: History of Information [online]. [cit. 25.09.2021]. Dostupné z: https://www.historyofinformation.com/detail.php?entryid=2495

SEZNAM POUŽITÝCH ZKRATEK

CCD – Charged Coupled Device (obrazový snímač s vysokou světelnou citlivostí)

CCTV – Closed Circuit Television (uzavřený televizní okruh)

CMOS – Complementary Metal Oxide Semiconductor (obrazový snímač s nízkou spotřebou a levnější výrobou oproti CCD)

ČSN – Česká Státní Norma

DPPC – Dohledové Poplachové Přijímací Centrum

DET – Detection Error Trade-off (křivka/graf znázorňující vztah FARxFRR)

EER – Equal Error Rate (stejná míry chybovosti)

EKV – Elektronická Kontrola Vstupu

EU – Europe Union (Evropská unie)

FAR – False Acceptance Rate (pravděpodobnost chybného přijetí)

FRR – False Rejecting Rate (pravděpodobnost chybného odmítnutí)

GDPR – General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)

HDD – Hard Disc Drive (pevný počítačový disk)

IAR – Imposter Accept Rate (pravděpodobnost podvodného přijetí)

ID karta – Identity Document (identifikační průkaz)

IEC – International Electrotechnical Commission (Mezinárodní elektrotechnická komise)

IP – Internet Protocol (protokol používaný v počítačových sítích)

IR – Infra Red (ifra červené světlo)

ISO – International Organization for Standardization (Mezinárodní organizace pro normalizaci)

JČU – Jihočeská univerzita

JTC 1 – Join Technical Committee (společná technická komise)

LAN – Local Area Network (místní síť)

LED – Light Emitting Diode (dioda vyzařující světlo)

LTP – Local Texture Patterns (Lokální texturové vzory)

NEIA – Number of Enrolle Identification Attemps (počet oprávněných identifikačních pokusů)

NEVA – Number of Enrolle Verification Attemps (počet oprávněných verifikačních pokusů)

NFR – Number of False Rejection (počet chybných odmítnutí)

NIR – Near Infra Red (blízké červené spektrum)

NOZ – Nový Občanský Z8koník

NVR – Network Video Recorder (síťový videorekordér)

Mpix – Megapixel (jednotka digitálního zobrazení – 1mil. obrazových bodů)

PHM – Pohonné Hmoty a Maziva

PIN – Personal Identification Number (osobní identifikační číslo)

PIR – Passive Infra Red (pasivní infračervené čidlo)

PoE – Power over Ethernet (systém napájení IP kamer)

PTZ – Pan, Tilt, Zoom (kamery pohyblivé horizontálně, vertikálně s přiblížením)

PZTS – Poplachový Zabezpečovací a Tísňový Systém

RFID – Radio Frequency Identification (identifikace prostřednictvím rádiové frekvence)

RF karta – Radio Frequency karta (identifikační karta komunikující na rádiové frekvenci)

ROC – Reciever Operating Characteristic (operační charteristika přijímače – křivka)

ROI – Region of Interest (zájmová oblast)

RZ – Registrační Značka

SAR – Spoof Acceptance Rate (pravděpodobnost přijetí repliovaného vzorku)

SC – Sub-Committee (pod-komise zřízená v rámci JTC 1)

SKV – Systém Kontroly Vstupu

SZ – Sklad Zbraní

TB – Terabyte (jednotka digitální informace)

TVI – Transport Video Interface (přenosové video rozhraní)

US – Ultra Sonic (ultrazvukové čidlo)

USA – United States of America (Spojené státy americké)

VMS – Video Management Systém (prostředí pro práci a zobrazení videosignálů z kamer uzavřeného kamerového okruhu)

WAN – Wide Area Network (rozlehlá síť, např. internet)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Přílohy

Biometrie

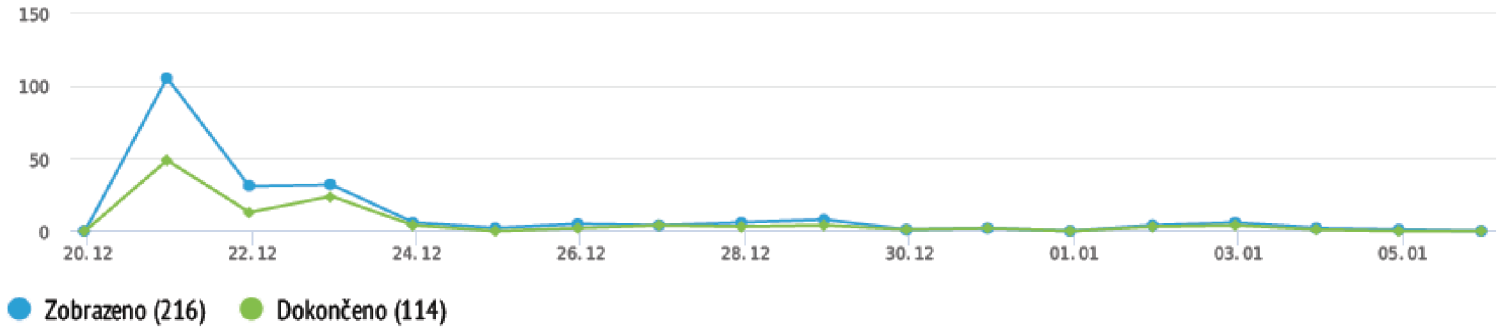
Základní údaje

Název výzkumu	Biometrie
Autor	
Jazyk dotazníku	Čeština
Veřejná adresa dotazníku	https://www.survio.com/survey/d/U6A7L1N3M3F3P5K9S
První odpověď	21. 12. 2021
Poslední odpověď	04. 01. 2022
Doba trvání	15 dnů

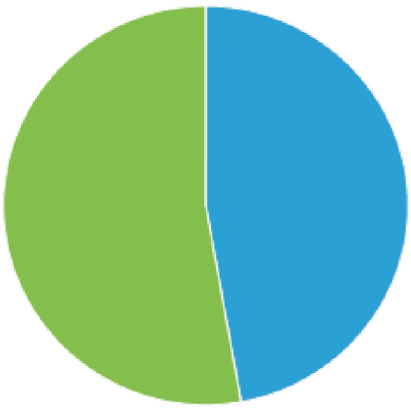
Statistika respondentů

216	114	0	102	52,8 %
Počet návštěv	Počet dokončených	Počet nedokončených	Pouze zobrazení	Celková úspěšnost vyplnění dotazníku

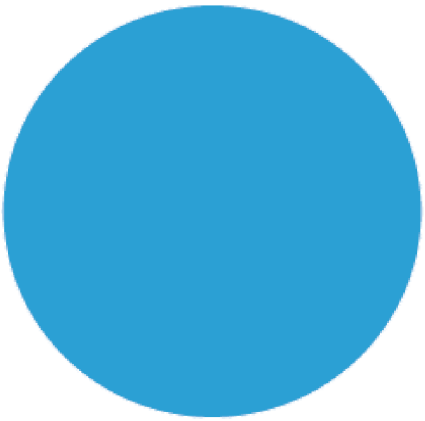
Historie návštěv (21. 12. 2021 – 04. 01. 2022)



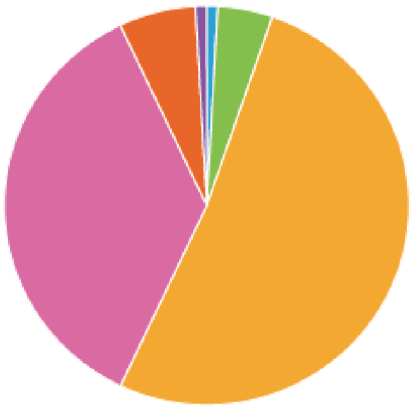
Celkem návštěv

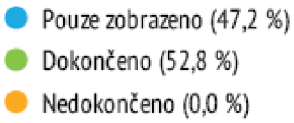


Zdroje návštěv



Čas vyplňování dotazníku




Pouze zobrazeno (47,2 %)
Dokončeno (52,8 %)
Nedokončeno (0,0 %)


Přímý odkaz (100,0 %)

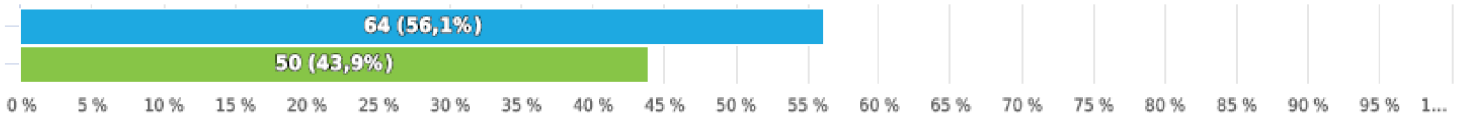

<1 min. (0,9 %)
1-2 min. (4,4 %)
2-5 min. (51,8 %)
5-10 min. (36,0 %)
10-30 min. (6,1 %)
30-60 min. (0,9 %)

Výsledky

1 Jste?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

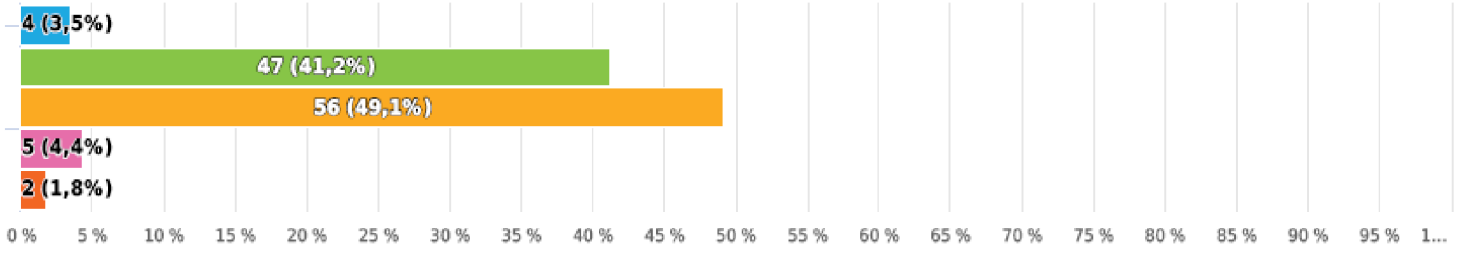
Možnosti odpovědí	Responzí	Podíl
Muž	64	56,1%
Žena	50	43,9%



2 Jaký je váš věk?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

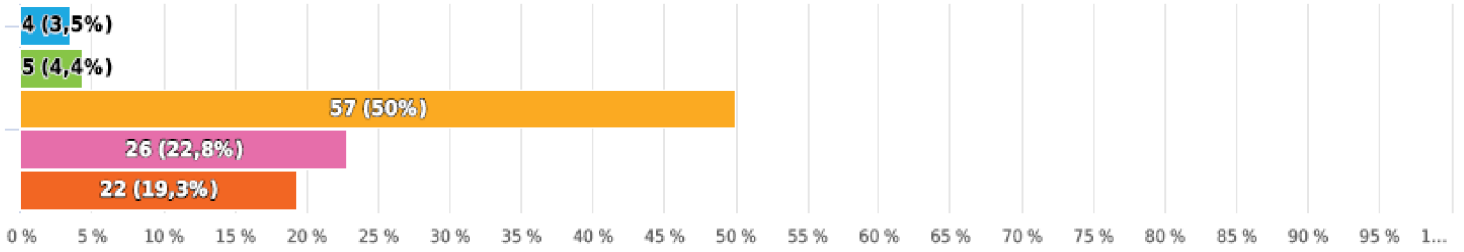
Možnosti odpovědí	Responzí	Podíl
15-25 let	4	3,5%
26 - 40 let	47	41,2%
41 - 55 let	56	49,1%
56 - 70 let	5	4,4%
70 a více let	2	1,8%



3 Jaké je Vaše nejvyšší dosažené vzdělání?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

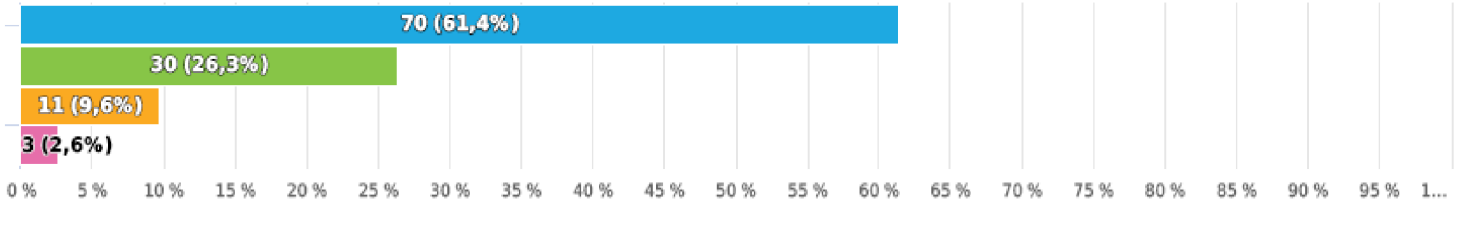
Možnosti odpovědí	Responzí	Podíl
Základní	4	3,5%
Středoškolské bez maturity	5	4,4%
Středoškolské s maturitou	57	50,0%
VŠ - bakalářské	26	22,8%
VŠ - magisterské a vyšší	22	19,3%



4 Víte co je biometrická identifikace?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

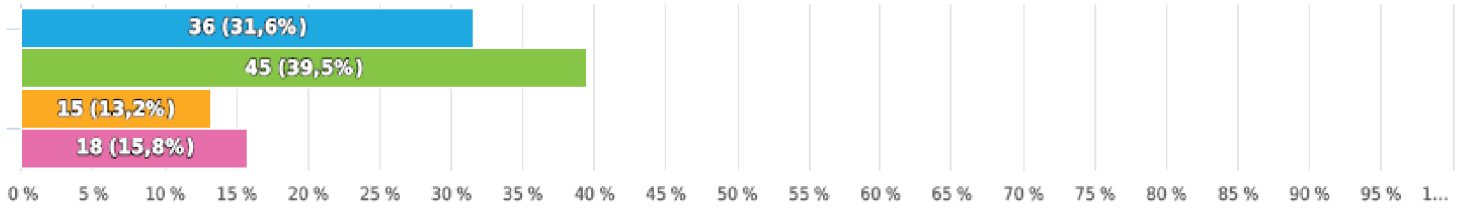
Možnosti odpovědí	Responzí	Podíl
Ano, vím	70	61,4%
Domnívám se, že vím	30	26,3%
Nevím	11	9,6%
Nikdy jsem to neslyšel	3	2,6%



5 Už jste se setkal/a se systémem/zařízením, které využívalo nějaký druh biometrie?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

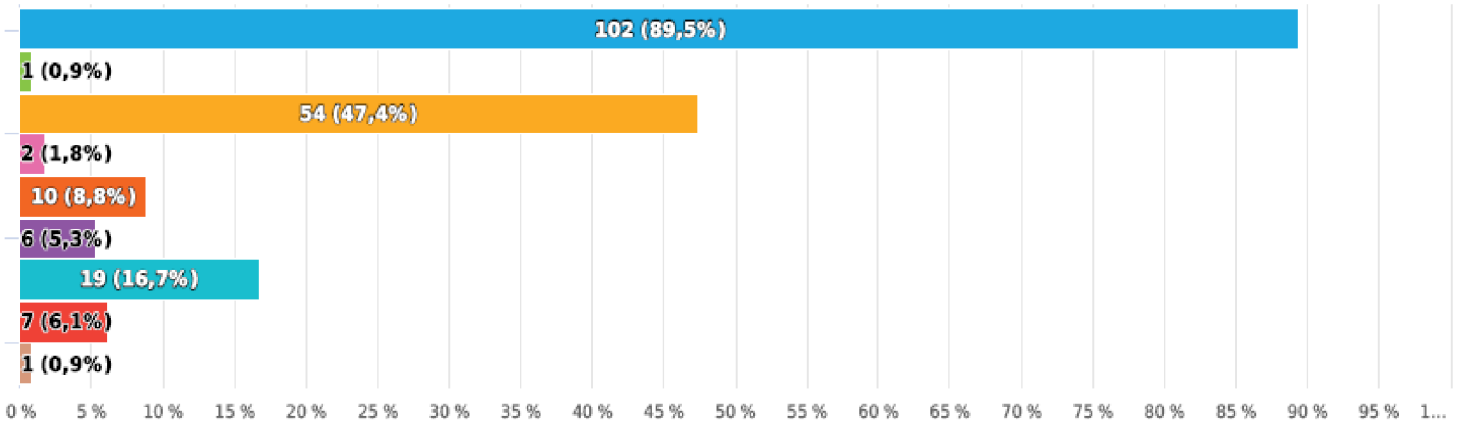
Možnosti odpovědí	Responzí	Podíl
Ano, aktivně pravidelně používám biometrickou identifikaci v zaměstnání i v soukromí.	36	31,6%
Ano, ale pouze v soukromí.	45	39,5%
Ano, ale pouze v zaměstnání.	15	13,2%
Ne, takové zařízení jsem ještě nevyzkoušel.	18	15,8%



6 Znáte nebo aktivně používáte některý z uvedených druhů biometrických identifikátorů?

Výběr z možností, více možných , zodpovězeno 114 x, nezodpovězeno 0 x

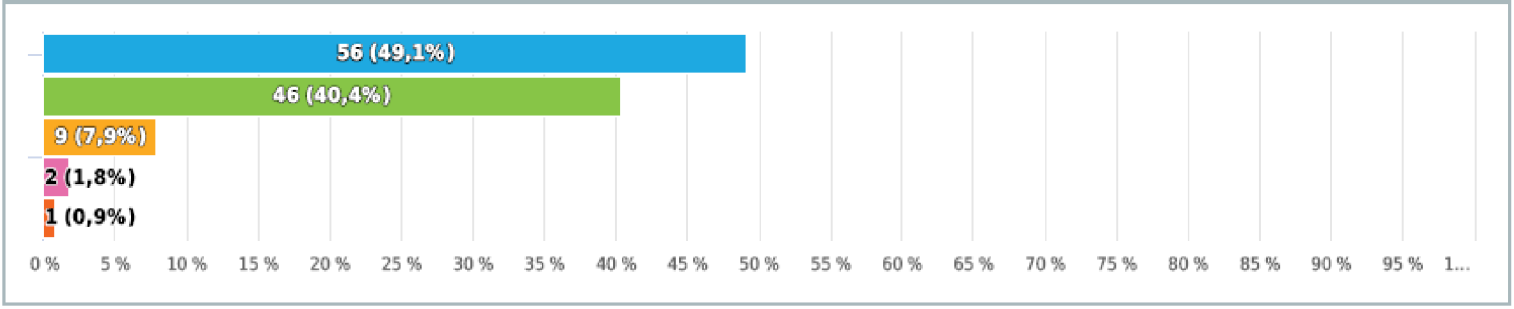
Možnosti odpovědí	Responzí	Podíl
Otisk prstu	102	89,5%
Geometrii ruky	1	0,9%
Obličej	54	47,4%
Žilní obraz dlaně/prstu	2	1,8%
Oční duhovku	10	8,8%
Oční sítnici	6	5,3%
Hlas	19	16,7%
Dynamiku chůze	7	6,1%
Jiný...	1	0,9%



7 Domníváte se, že je využití biometrie bezpečné?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

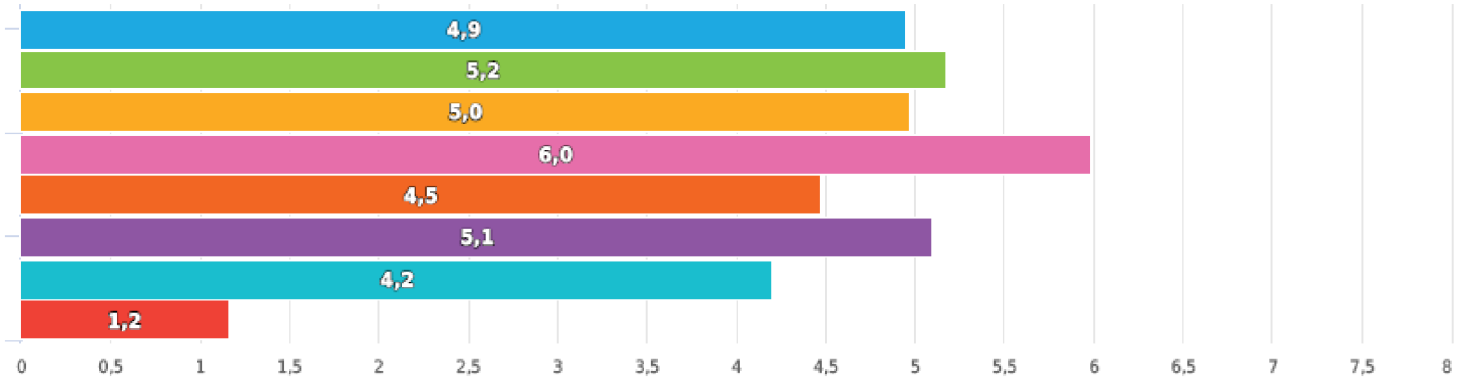
Možnosti odpovědí	Responzí	Podíl
Ano	56	49,1%
Spíše ano	46	40,4%
Nevím	9	7,9%
Spíše ne	2	1,8%
Ne	1	0,9%



8 Pokud byste měl/a na výběr, kterou metodu/formu ověření své osoby byste zvolil/a?

Seřazení dle důležitosti , zodpovězeno 114 x, nezodpovězeno 0 x

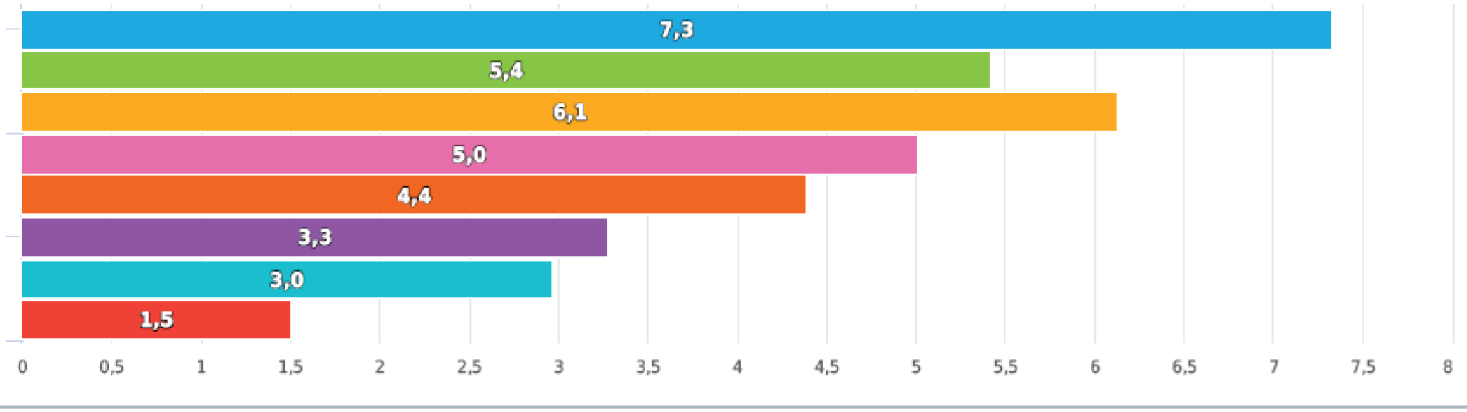
Odpověď	Důležitost
Průkaz s fotografií předkládaný vrátnému/ostraze.	4,9
Čipovou kartu/čip	5,2
PIN - zadávání osobního číselného kódu	5,0
Biometrický identifikátor	6,0
Kombinaci čipové karty/čipu + PIN	4,5
Kombinaci biometrického identifikátoru + PIN	5,1
Kombinaci biometrického identifikátoru + čipové karty/čipu	4,2
Jinou zde neuvedenou.	1,2



9 Který z uvedených biometrických identifikátorů byste preferoval/a v případě použití ve vašem zaměstnání?

Seřazení dle důležitosti , zodpovězeno 114 x, nezodpovězeno 0 x

Odpověď	Důležitost
Otisk prstu	7,3
Geometrie ruky	5,4
Obličej	6,1
Oční duhovku	5,0
Oční sítnici	4,4
Žilní obraz dlaně/prstu	3,3
Hlas	3,0
Dynamiku chůze	1,5

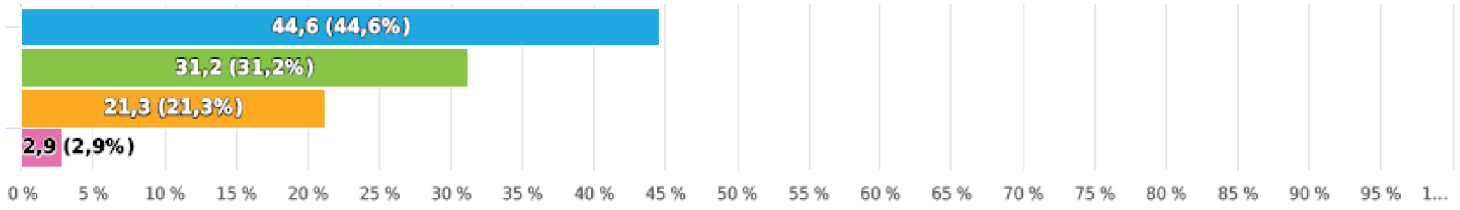


10 Jakou měrou Vás při volbě mezi jednotlivými druhy biometrie ovlivňují uvedená hlediska?

Rozdělovací škála , zodpovězeno 114 x, nezodpovězeno 0 x

Rozdělte: 100 bodů

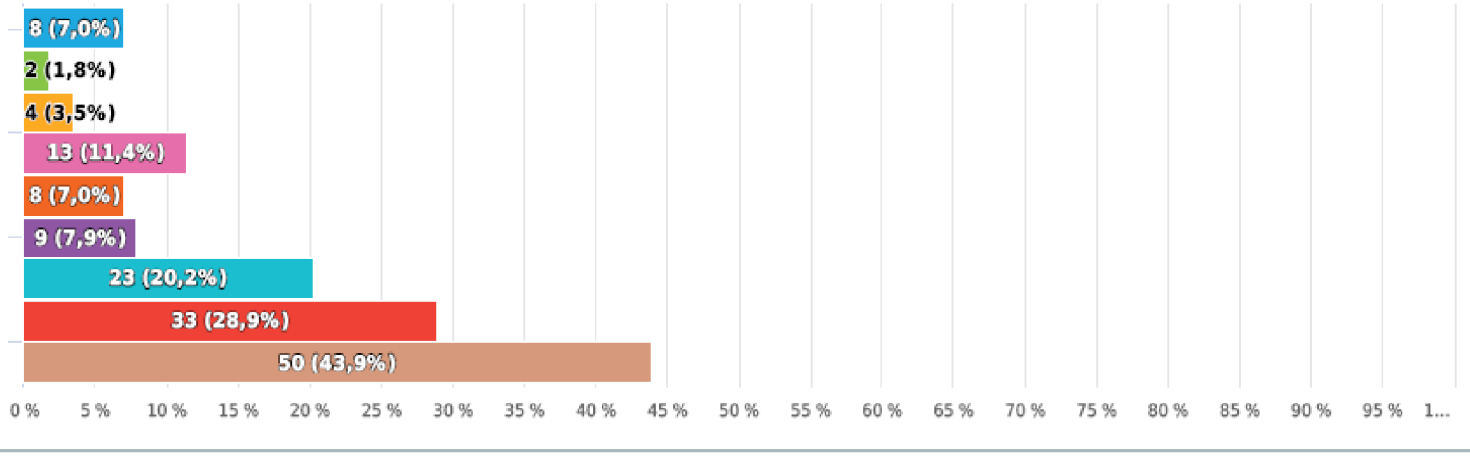
Odpověď	Průměr	Podíl
Uživatelský komfort	44,6	44,6%
Rychlost a přesnost ověření	31,2	31,2%
Bezpečnost zpracovávaných dat	21,3	21,3%
Možnost osobního vyzkoušení nové technologie.	2,9	2,9%



11 Je některý z níže uvedených biometrických identifikátorů pro Vás neakceptovatelný?

Výběr z možností, více možných , zodpovězeno 114 x, nezodpovězeno 0 x

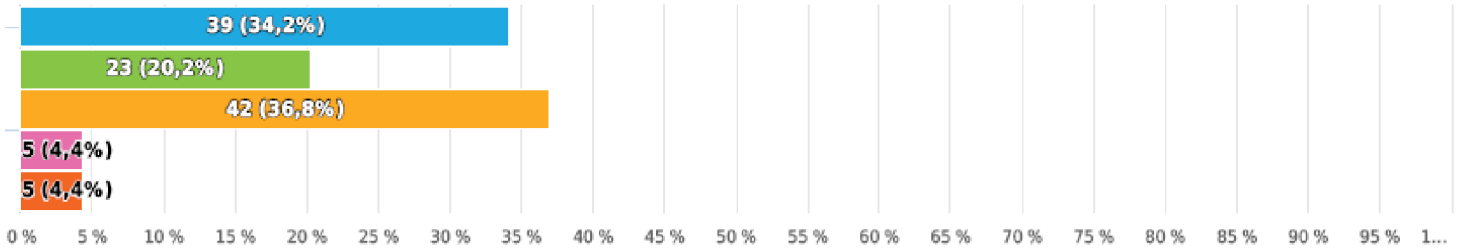
Možnosti odpovědí	Responzí	Podíl
Otisk prstu	8	7,0%
Geometrie ruky	2	1,8%
Obličej	4	3,5%
Žilní obraz dlaně/prstu	13	11,4%
Oční duhovka	8	7,0%
Oční sítnice	9	7,9%
Hlas	23	20,2%
Dynamika chůze	33	28,9%
Všechny uvedené biometriky vnímám jako akceptovatelné.	50	43,9%



12 Byl/a byste ochoten/na poskytnout svá biometrická data zaměstnavateli za účelem jejich využití v docházkovém a přístupovém systému, popř. pro automatické ovládání systému zabezpečení objektu/ů?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
Ano, nemám s tím problém.	39	34,2%
Spíše ano, za ten komfort mi to stojí.	23	20,2%
Nevím, záleželo by na okolnostech.	42	36,8%
Spíše ne, nemám v tyto technologie důvěru.	5	4,4%
Ne	5	4,4%



13 Pokud by Váš zaměstnavatel nainstaloval biometrický sytém v rámci automatizované správy zabezpečení budov, vnímal byste to jako?

Výběr z možností , zodpovězeno 114 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
Krok správným směrem, je třeba jít s dobou a využívat moderní technologie.	45	39,5%
Kvitoval bych, že nemusím neustále nosit/hledat zaměstnaneckou kartu.	30	26,3%
Bylo by mi to jedno.	21	18,4%
Takovou změnu bych pociťoval spíše negativně a s nelibostí.	15	13,2%
Bylo by to pro mě absolutně nepřijatelné a zvažoval bych změnu zaměstnavatele.	3	2,6%