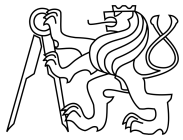
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Studie nasazení biometrických systémů v podnicích
Student:	Aneta Moravcová
Vedoucí:	Ing. David Buchtela, Ph.D.
Studijní program:	Informatika
Studijní obor:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2017/18

Pokyny pro vypracování

Cílem práce je komplexní analýza (studie proveditelnosti) nasazení biometrických systémů v podnikové praxi ČR.

1. Formou rešerše se seznamte s problematikou biometrické identifikace a verifikace uživatelů.
2. Zpracujte přehled základních biometrických metod používaných v praxi a definujte kritéria jejich hodnocení z hlediska funkčnosti a efektivního nasazení v podniku.
3. Definujte tři typové podniky ve zvoleném odvětví (po dohodě s vedoucím práce) a popište jejich typickou IS/ICT infrastrukturu.
4. Vypracujte procesní a ekonomickou (finanční) analýzu nasazení biometrických systémů v typových podnicích dle definovaných kritérií hodnocení.
5. Na základě výsledků analýzy sestavte doporučení pro nasazení biometrických systémů v podnikové praxi ČR.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 8. ledna 2017

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra softwarového inženýrství

Bakalářská práce

Studie nasazení biometrických systémů v podnicích

Aneta Moravcová

Vedoucí práce: Ing. David Buchtela, Ph.D.

15. května 2017

Poděkování

Chtěla bych poděkovat Ing. Davidu Buchtelovi, Ph.D. za rady a odborné vedení mé bakalářské práce. Dále děkuji firmě Abbas, a.s. za poskytnuté informace o cenových relacích biometrických technologií. V neposlední řadě děkuji své rodině za trpělivost a podporu při mém studiu.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 15. května 2017 .....

Odkaz na tuto práci

Moravcová, Aneta. *Studie nasazení biometrických systémů v podnicích.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2017.

Abstrakt

Tato práce se zabývá studií proveditelnosti nasazení biometrických systémů v podnikové praxi ČR.

V první části práce jsou vysvětleny základní biometrické metody využívané v praxi a další pojmy nutné k pochopení praktické části práce, ve které popisuji proces nasazení běžně využívaných biometrických technologií ve třech různých typech podniků z hlediska procesního i ekonomického.

Přínosem této práce není pouze procesní a ekonomická analýza, která je názorně popsána u každého ze tří podniků, ale i doporučení pro nasazení biometrických systémů a shrnutí výhod a nevýhod těchto systémů pro daný typ podniku.

Klíčová slova Studie proveditelnosti, analýza nasazení systému, biometrický systém, ochrana podnikových dat, procesní analýza, ekonomická analýza, biometrie a identita člověka

Abstract

This thesis deals with the feasibility study of biometric system implementation in business practice in Czech Republic.

In the theoretical part of thesis there are explained biometric methods used in practice and other concepts that are essential for understanding of the practical part of thesis. In the practical part of this thesis we look into the process of use of ordinarily exploited biometric systems in three various types of companies in process and economic point of view.

The benefit of this thesis is not only process and economic analysis that is described in each company type, but also recommendation for using of biometric systems and summary of advantages and disadvantages of these systems for the given type of company.

Keywords Feasibility study, deployment analysis, biometric system, business data protection, process analysis, economic analysis, biometrics and human's identity

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Firmy a instituce generují obrovské množství dat a nutnost zabezpečení těchto dat je čím dál aktuálnější. Možné následky zneužití citlivých informací si organizace dobře uvědomují a nezaměřují svou pozornost pouze na umístění svých dat, ale i na způsob jejich ochrany. Potřeba chránit klíčová data vzniká nejen z příčiny finanční ztráty, ale i poškození dobrého jména firmy a v některých kritičtějších případech i z důvodu veřejného ohrožení. Z těchto důvodů jsem zvolila téma týkající se biometrických metod využívaných v systémech pro ochranu dat i majetku.

Cíl práce

Cílem práce je vypracovat procesní a ekonomickou analýzu nasazení biometrických systémů v podnicích a na základě výsledků této studie sestavit doporučení pro nasazení těchto bezpečnostních systémů v podnikové praxi ČR a shrnout výhody a nevýhody, které biometrické technologie přinášejí. Tato analýza je názorně popsána na třech typových podnicích, které jsou vybrány tak, aby pokryly co nejširší oblast IS/ICT infrastruktur.

Očekávám, že pokud nějaká firma alespoň z části ztotožní svou IS/ICT infrastrukturu s IS/ICT infrastrukturou některého ze tří typových podniků definovaných v mé práci, mohlo by mé doporučení pomoci v rozhodování, zda je pro podnik vhodné biometrický systém nasadit a jaké to bude mít výhody a případně i nevýhody.

Motivace

Toto téma jsem si vybrala z důvodu neustále rostoucí relevance bezpečnosti v oblasti informačních technologií a biometrii považuji za velmi zajímavé vědecké odvětví, které se neustále vyvíjí a v ochraně podnikových dat i majetku je mu přikládán stále větší význam.

Struktura práce

Práce je rozdělena do dvou hlavních kapitol - teoretické a praktické části.

Teoretická část se zabývá elementárními pojmy z oblasti biometrie a identity člověka, základním pohledem na identifikaci člověka a myšlenkou biometrické identifikace. Dále jsou v této části práce vysvětleny obecné principy biometrických technologií a systémů. V kapitole jsou popsány biometrické metody využívané v praxi a kritéria hodnocení těchto metod z hlediska funkčnosti a efektivního nasazení v podniku. Předposlední kapitola je věnována měření výkonnosti a spolehlivosti biometrických metod a v poslední kapitole je pomocí grafu znázorněno zastoupení jednotlivých biometrických technologií na trhu.

Druhá (praktická) část obsahuje tři hlavní podkapitoly, z nichž každá se zabývá jiným typovým podnikem. U každého typového podniku je popsána jeho IS/ICT infrastruktura a pomocí diagramu aktivit je znázorněn stav bez biometrického systému a situace po jeho nasazení. Dále každý typový podnik obsahuje analýzu biometrických metod podle kritérií hodnocení a finální zhodnocení a doporučení pro nasazení biometrických systémů v daném typovém podniku.

Kapitola 1

Teoretická část

1.1 Základní pojmy

Pro pochopení dalších podkapitol je důležité objasnit ty nejzákladnější pojmy z oblasti biometrie a identity člověka podle [1]:

- **Identita** - totožnost něčeho s něčím nebo se sebou samým; v čase se nemění
- **Identita osoby** - definována jako „nezbytná podmínka bytí každé konkrétní osoby“
  - *Biologická* - kombinace dědičných i získaných biologických charakteristik, nezávislých na vědomí člověka
  - *Psychologická* - totožnost vědomí
  - *Filosofická* - ztotožnění bytí a myšlení
  - *Sociální* - identita jazyková, kulturní, etnická, morální apod.
- **Identifikace** - proces prokázání nebo zjištění identity
- **Identifikace osoby** - specifický případ obecné identifikace
  - *Vnější* - fyzická (biologická) identita člověka
  - *Vnitřní (sebeidentifikace)* - nalezení a vnímání vlastní identity psychologické, filosofické, sociální apod.
- **Verifikace** - proces ověření identity osoby
- **Biometriky** - měřitelné biometrické charakteristiky (obrazce, data apod.) živého organismu
- **Biometrie** - soubor vědních poznatků, jejichž předmětem je zkoumání a následné praktické využití biometrik živých organismů s cílem jejich následné jednoznačné identifikace nebo verifikace

- **Biometrická identifikace/verifikace** - využití jedinečných, měřitelných, fyzikálních nebo fyziologických znaků (markantů) nebo projevů člověka k jednoznačnému zjištění (identifikace) nebo ověření (verifikace) jeho identity
- **Biometrický systém** - aplikace biometrických technologií, která umožňuje automatickou identifikaci a verifikaci osob

1.2 Základní pohled na identifikaci osoby

Na identifikaci osoby se lze dívat z nejrůznějších pohledů. Osobu nerozlišujeme pouze podle fyzického vzhledu a biologických charakteristik, ale i podle toho, co vlastní nebo zná. Podle [1] existují tři základní přístupy v identifikaci osoby:

- **Vlastnictví** - uměle získané nebo přidělené identifikační charakteristiky, jako jména a příjmení, osobní doklady, identifikační čísla a kódy, identifikační karty a čipy, biočipy
- **Znalosti** - individuální dovednosti a znalosti, o kterých se předpokládá, že je zná pouze daná osoba (data a místa narození svých rodinných příslušníků, vlastní hesla nebo osobní identifikační čísla apod.)
- **Biometrické charakteristiky** - měřitelné biologické charakteristiky, které se dále dělí na anatomicko fyziologické a behaviorální

První dva pohledy na identifikaci osoby, tj. z pohledu vlastnictví a znalostí, jsou zastaralé a zranitelné. Tato práce se bude zaměřovat zejména na poslední pohled na identifikaci osoby, tedy na biometrické charakteristiky lidského těla a jeho projevů.

1.3 Základní myšlenky biometrické identifikace

Základní princip identity říká, že každá osoba je identická pouze sama se sebou. Pokud vědecky prokážeme, že fyzické charakteristiky nějaké osoby jsou jedinečné, pak je lze úspěšně použít pro efektivní identifikaci této osoby. Identitu osoby je téměř nemožné zcela napodobit, odcizit nebo pozměnit. Biometrická identita je pro každého člověka přirozená - je s ním spojena již od narození. [1]

1.4 Místo biometrické identifikace v současném světě

V minulosti byla biometrická identifikace vždy spojena pouze s bezpečností nebo forenzní praxí, ovšem rozvoj technologií umožnil její uplatnění v dalších směrech a oborech lidské činnosti.

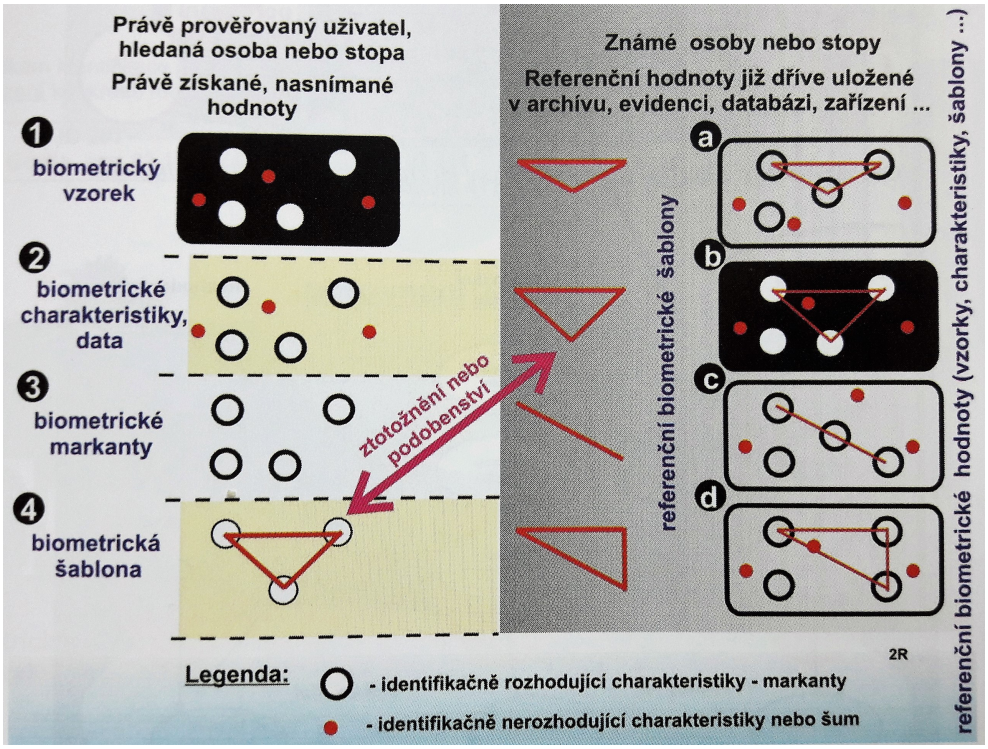
Mezi největší výhody biometrické identifikace podle [1] patří:

- nelze ji zapomenout nebo ztratit,
- je téměř nemožné ji odcizit nebo napodobit,
- je nepřenositelná,
- vysoká přesnost a rychlost identifikace,
- je velice snadno a rychle použitelná,
- je lidsky přirozená,
- možnost plné nebo částečné automatizace.

Různá elektronická zařízení, se kterými se denně setkáváme, jako například počítače, mobilní telefony, bankovní automaty apod. vyžadují identifikaci uživatele. S vývojem informačních technologií zároveň roste i počet neoprávněných přístupů nebo zneužití těchto zařízení jinou, podvodně jednající osobou. Identifikace osoby, založená na vlastnictví nebo znalostech je nedostačující a proto také zranitelná. Zatímco biometrická identifikace je jednou z nejdynamičtěji se rozvíjejících odvětví informačních technologií.

Podle [1] se biometrická identifikace stane nenahraditelnou v oborech jako jsou:

- ochrana platebních a bankovních karet,
- ochrana vstupu do objektů a zařízení,
- cestování a turismus,
- Customer Relationship Management,
- ochrana majetku,
- telekomunikace,
- ochrana elektronických transakcích,
- kontrola pracovní docházky a přítomnosti na pracovišti,
- forenzní a znalecké expertizy,
- vězeňství,
- ochrana zbraňových systémů i individuálních zbraní.



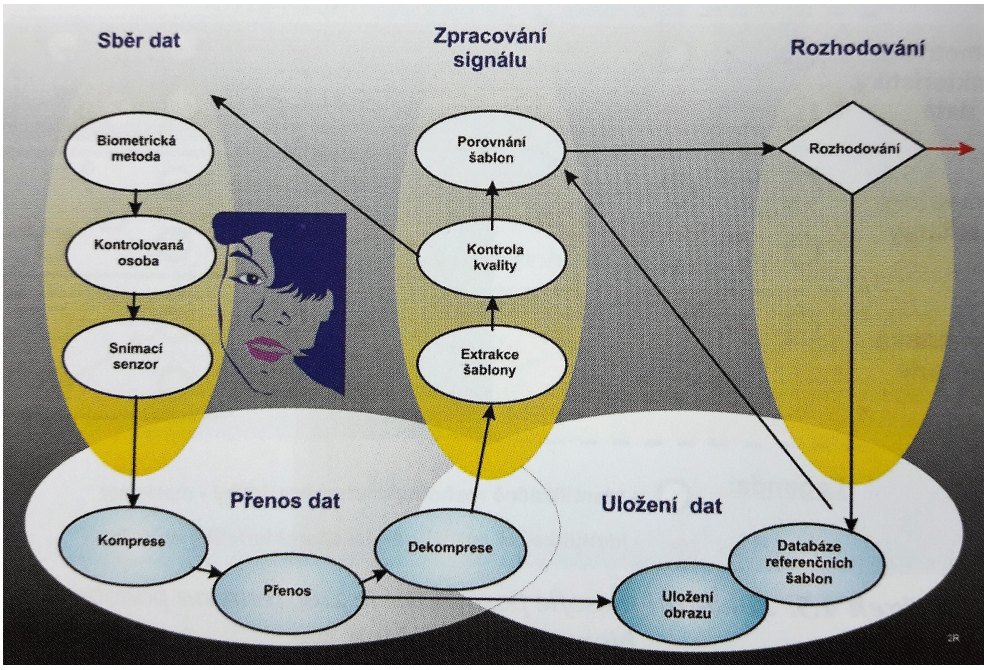
Obrázek 1.1: *Základní filosofie porovnání založená na podobenství šablon.* [1]

1.5 Obecné principy biometrických technologií

Při bližším pohledu na jednotlivé biometrické metody zjistíme, že mezi všemi identifikačními a verifikačními postupy existují společné rysy. Než si tyto obecné technologické postupy popíšeme, je vhodné definovat tyto pojmy:

- **Biometrický vzorek** - biometrická informace získaná pomocí biometrického zařízení (systému) nebo jiným způsobem. Příkladem může být otisk prstu, kapka krve, fotografie, zvukový záznam apod. [8]
- **Biometrické charakteristiky, data** - souhrn měřitelných údajů z biometrického vzorku. [1]
- **Biometrické markanty** - část biometrických charakteristik, kterou lze efektivně využít pro identifikaci nebo verifikaci osoby. [1]
- **Biometrická šablona** - digitální reprezentace biometrických markantů extrahovaných z biometrického vzorku. Šablony jsou využívány v procesu identifikace/verifikace jako základ pro porovnání. [9]

Základní myšlenka biometrického porovnání je znázorněna na obrázku 1.1.



Obrázek 1.2: *Obecný algoritmus zpracování biometrických údajů.* [1]

Obecný algoritmus zpracování biometrických údajů má podle [1] pět etap - sběr dat, přenos dat, zpracování signálu, proces rozhodování a uložení dat (obrázek 1.2).

1.5.1 Sběr dat

Biometrické zpracování začíná snímáním biometrických dat pomocí senzoru nějakého biometrického zařízení. Každý snímací senzor musí být navržen s ohledem na:

- samotné biometrické měření,
- způsob, jakým je měření provedeno (vzdálenost, úhel, chování osoby apod.),
- technické charakteristiky (rychlost, přesnost apod.).

Nasnímaný obraz se nazývá biometrický vzorek a je určený k vytvoření biometrické šablony. [1]

1.5.2 Přenos dat

Některé biometrické aplikace sbírají a skladují/zpracovávají biometrická data na dvou různých místech, proto je důležité zabezpečit přenos těchto dat. Je-

Tabulka 1.1: *Typické extrahované markanty jednotlivých biometrických metod.* [1]

Biometrická metoda	**Extrahované markanty**
Otisky prstů	Umístění a směr charakteristických bodů otisku
Hlas	Frekvence, intonace, trvání jednotlivých hlasových charakteristik
Tvář	Relativní pozice a tvar nosu, očí, lícních kostí
Oční duhovka	Rýhování a proužkování duhovky, geometrické obrazce
Oční sítnice	Tvar markantů krevního řečiště v sítnici
Geometrie prstů a ruky	Délka a šířka kostí a kloubů dlaně a prstů
Krevní řečiště ruky	Struktura sítě cév ruky
Dynamika psaní na klávesnici	Pořadí kláves, časové intervaly mezi jednotlivými úhozy

likož mají biometrická data často velký objem, před samotným přenosem se komprimují. Po přenosu se před dalším zpracováním data dekomprimují.

Na používané kompresní techniky je upřena velká pozornost kvůli ztrátě kvality dekomprimovaného signálu v procesu komprimace a reverzní dekomprimace. Ztráta kvality je nežádoucí a proto jsou hledány takové komprimační metody, které ovlivňují kvalitu minimálně. [1]

1.5.3 Zpracování signálu

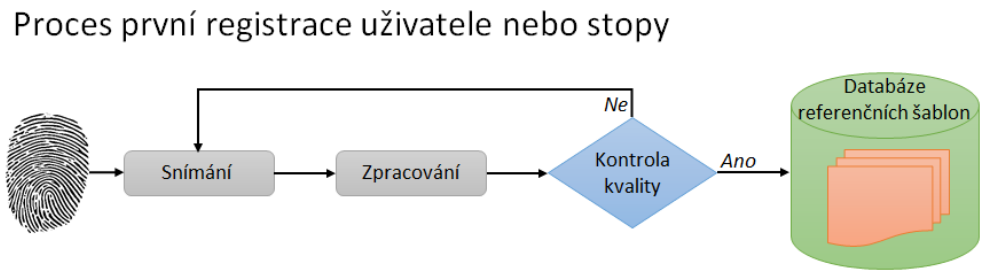
Zpracování biometrického signálu rozdělujeme podle [1] do těchto částí:

- extrakce biometrické šablony z biometrického vzorku,
- kontrola kvality biometrického vzorku,
- vyhledávání v databázi porovnáním s dalšími šablonami.

1.5.3.1 Extrakce šablony

Prvním úkolem v tomto zpravidla automatizovaném procesu je získat všechny biometrické charakteristiky z nasnímaného biometrického vzorku. Druhým cílem je rozlišit jednoznačné identifikační markanty a odfiltrovat všechny rušivé vlivy - šum, redundantní informace apod. Výsledkem extrakce je šablona, která plně odráží individuální specifičnost prověřované osoby a splňuje základní identifikační podmínky - unikátnost, přesnost, časovou neměnnost. [1]

V tabulce 1.1 jsou uvedeny vybrané biometrické metody s jejich typickými extrahovanými markanty.



Obrázek 1.3: *Základní schéma uložení referenční šablony.* Vytvořeno autorem podle [1] [2].

1.5.3.2 Kontrola kvality

Jak v procesu první registrace uživatele nebo stopy (obrázek 1.3), tak i během identifikace (obrázek 1.4) nebo verifikace (obrázek 1.5) potřebujeme vědět, zda je obdržený signál dostatečně kvalitní. Pokud jsou nasnímané charakteristiky nesmyslné nebo nedostatečné, nelze pokračovat v dalším zpracování biometrických údajů. [1]

1.5.3.3 Porovnání šablon

Proces porovnání probíhá mezi šablonou právě nasnímaného vzorku a šablonami již dříve nasnímaných a v databázi uložených vzorků.

Identifikace je proces porovnání „1:n“ nasnímaného biometrického vzorku se všemi referenčními šablonami. Cílem je nalezení/nenalezení konkrétní identity. V případě pozitivní identifikace byla v databázi nalezena šablona, která odpovídá šabloně z nasnímaného vzorku (obrázek 1.4). [1]

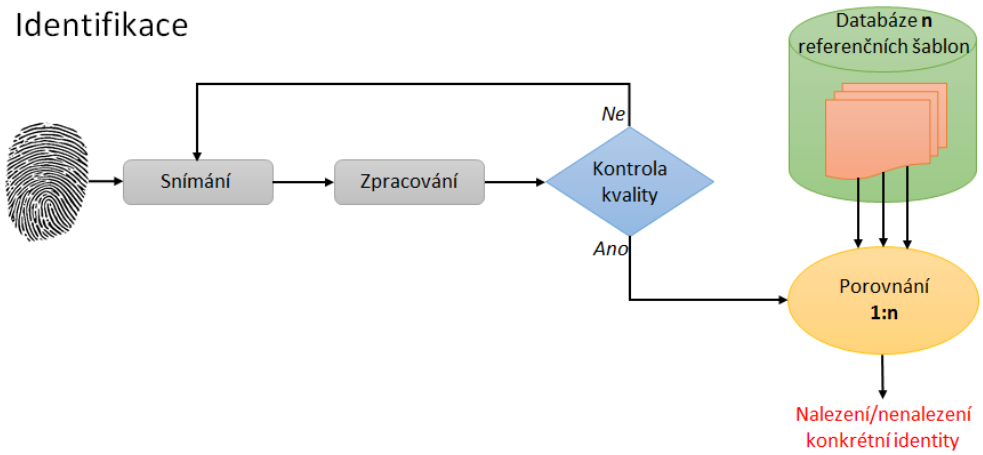
Verifikace je proces porovnání „1:1“ jediné šablony extrahované z biometrického vzorku s jedinou referenční šablonou, patřící prověřované osobě. Cílem je potvrdit/vyvrátit, že prověřovaná osoba je/není opravdu tou, za kterou se vydává (obrázek 1.5). [1]

1.5.4 Rozhodování

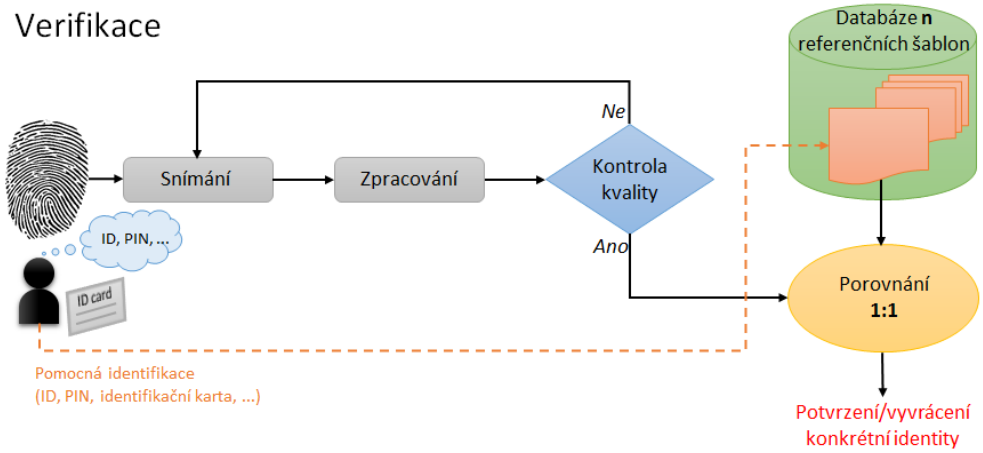
Automatizovaný rozhodovací proces následuje po porovnání šablon a stanovuje se v něm míra shody a identifikační závěr - lze/nelze tuto osobu autorizovat. Etapa rozhodování odpadá pouze v případě prvního zavádění biometrické šablony do databáze - registrace uživatele (obrázek 1.3). [1]

1.5.5 Uložení dat

V poslední etapě dochází v každé biometrické aplikaci k uložení dat - jedna nebo více referenčních šablon v závislosti na biometrickém systému. Referenční



Obrázek 1.4: *Základní filosofie identifikace v počítačové databázi.* Vytvořeno autorem podle [1] [2].



Obrázek 1.5: *Základní filosofie verifikace v počítačové databázi.* Vytvořeno autorem podle [1] [2].

Tabulka 1.2: *Členění biometrické identifikace.* [1]

Anatomicko-fyziologické biometrické charakteristiky	**Behaviorální biometrické charakteristiky**
Oční duhovka	Hlas
Oční sítnice	Lokomoce
Tvář	Písmo
Tvar vnějšího ucha	Podpis
Daktyloskopické otisky prstů, dlaní, chodidel	Dynamika psaní na klávesnici
Geometrie prstů a ruky	
Topografie krevního řečiště ruky	
Pach lidského těla	
Obsah solí v lidském těle	
Rozměry a váhy lidského těla	
DNA	

šablony jsou ukládány za účelem rychlého a efektivního porovnání v budoucnosti. V některých případech se ukládají i biometrické vzorky - např. v policejně soudních aplikacích jsou kromě šablon uloženy i původní biometrické vzorky již známých pachatelů. Největší kapacitu zabírají originálně nasnímané vzorky, šablony z nich odvozené jsou podstatně menší. [1]

1.6 Biometrické metody využívané v praxi

Jak již bylo zmíněno v podkapitole 1.2, podle [1] se k členění biometrické identifikace přistupuje dvěma základními pohledy biometrické charakteristiky - *anatomicko fyziologické* a *behaviorální*. Tyto dva přístupy jsou spolu s jednotlivými praktickými identifikačními metodami uvedeny v tabulce 1.2.

V tabulce 1.2 jsou uvedeny nejen identifikační metody běžně používané v praxi v různých oborech, ale i metody, které jsou zatím intenzivně zkoumány ve výzkumně vývojových laboratořích. Praktická část této práce se bude zabývat pouze některými běžně využívanými biometrickými metodami a v následujících podkapitolách si je detailněji popíšeme.

1.6.1 Daktyloskopie

Identifikace osob v oblasti daktyloskopie vychází z existence papilárních linií na prstech, dlaních a chodidlech. Na jiných místech povrchu lidského těla se papilární linie nevyskytují a s výjimkou některých lidoopů se tyto linie neobjevují u žádných jiných živočichů na Zemi. Papilární linie se vytvářejí jako funkční útvary, spojené s hmatovými a uchopovacími vlastnostmi končetin již mezi čtvrtým a pátým měsícem embryonálního stavu a rozložení větvení

těchto linií je pro každého člověka unikátní. Povrch kůže s papilárními liniemi je prostorově členitý, plastický. Výhody daktyloskopie spočívají v těchto fyziologických zákonitostech: [1]

- Na světě neexistují dva jedinci se shodnými obrazci papilárních linií.
- Obrazce papilárních linií zůstávají po celý život neměnné (pouze ve vysokém věku mohou být narušené vráskami).
- Papilární linie jsou neodstranitelné (pokud není odstraněna i zárodečná vrstva kůže).

1.6.1.1 Snímání a zpracování vzorku

Snímání otisku prstu využívá různé technologie a je realizováno pomocí *kontaktních* a *bezkontaktních* senzorů.

Kontaktní senzory zahrnují technologie používané před více jak třiceti lety i technologie nové. Patří sem senzory:

- *Opto-elektronické.* Skládají se z horní vrstvy, která má kontakt s kůží a je schopna po dotyku emitovat světlo. To je zachyceno v další vrstvě, která obsahuje fotodiody, jež přetvářejí světelný impuls na elektrický. [1]
- *Kapacitní.* Snímání pomocí měření elektrické kapacity. Snímací senzor je složen z několika desítek tisíc vodivých ploch a při dotyku s kůží mají papilární linie význam můstků přes jednotlivé vodivé plošky a brázdy se chovají jako izolant. Měří se napětí a kapacitní úbytky mezi jednotlivými vodivými ploškami. Tento typ senzoru je citlivý na elektromagnetický šum a znečištění pokožky prstu. [1]
- *Tlakové.* Reagují na tlak papilárních linií na elastickou desku snímacího senzoru, která je tvořena piezoelektrickými krystaly, díky nimž je tlak transformován do elektrického signálu. [1]
- *Teplotní.* Velice citlivě reagují na teplotní rozdíly mezi papilárními liniemi a brázdami. Papilární linie jsou v těsné blízkosti snímacího povrchu a brázdy jsou více vzdáleny. Tyto senzory výrazně eliminují pokusy o napodobení otisku, jelikož teplota dokáže určit, zda snímaný otisk patří živé osobě. [1]
- *Multispektrální.* Jsou schopné snímat a zpracovat vlastnosti prstu i pod povrchem kůže. Senzor využívá více osvětlovacích soustav o rozdílných vlnových délkách. Světlo projde pod povrch kůže a umožní tak shromáždit více identifikačních údajů z prstu. Tento typ senzoru funguje i za extrémních podmínek okolního prostředí a umožňuje testovat živost osoby, takže je velmi spolehlivý a odolný vůči falzifikátům. [10]

Obrázek 1.6: *Kvalita otisku prstu.* [1]

Bezkontaktní senzory zahrnují následující skupiny senzorů:

- *Optické.* Princip je podobný dotykovému optickému senzoru. Laserový paprsek umožňuje snímat otisk na vzdálenost 30 až 50 mm. Tento způsob eliminuje jak znečištění senzoru dotyky špinavých prstů, tak ulpívání papilárních linií na povrchu snímače. [1]
- *Ultrazvukové.* Princip je podobný optickým senzorům a lze ho přirovnat k činnosti velmi citlivého sonaru. Podstatou ultrazvukového snímání je vysílání zvukových vln s vysokou frekvencí, které se odrážejí od povrchu kůže. Tento typ snímání dobře odhaluje podvrhy, které jsou zpravidla dvourozměrné a výsledek snímání ultrazvukovým senzorem není zkreslen vlhkostí nebo zašpiněním prstů. [1]

Kvalita výsledného obrazu otisku je závislá na nejrůznějších faktorech, které mohou negativně ovlivnit verifikaci (obrázek 1.6). Smyslem počítačového předzpracování obrazu otisku prstu je zvýraznit kresbu papilárních linií a odstranit nežádoucí šumy (nekvalitní, nečitelné oblasti, falešné markanty, jizvy apod.). [1]

Celkový postup zpracování obrazu otisku je podobný obecnému principu popsanému v kapitole 1.5.

1.6.1.2 Výhody a nevýhody technologie

Výhody a nevýhody této technologie závisí na typu snímače, ale obecně lze říci, že mezi výhody patří unikátnost, neměnnost v průběhu života člověka, poměrně příznivá cena, malé rozměry zařízení a u modernějších zařízení i velká odolnost vůči falzifikátům.

Nevýhodami mohou být relativně vysoká chybovost u levnějších zařízení a neschopnost rozpoznat falzifikát v případě některých typů snímačů. Další nevýhodou je, že některé typy snímačů mají problém se znečištěním prstu a drobnými poraněními. [10] [11]

1.6.1.3 Možnosti využití technologie

Tato technologie nabízí široké uplatnění v rozmanitých oblastech, např. [12]:

- forenzní praxe,
- oprávnění ke vstupu do určitých prostor,
- podnikové zabezpečení,
- lékařství,
- finanční instituce apod.

1.6.2 Oční sítnice

Sítnice je na světlo citlivý povrch zadní části oční bulvy (obrázek 1.7). Je tvořena obrovským počtem specializovaných nervových buněk - tyčinky a čípky, převádějí světelné paprsky na nervové signály. Čípky poskytují barevné vidění. Tyčinky jsou mnohem citlivější na světlo, ale poskytují pouze černobílé vidění. Lidská sítnice je jedinečná, v čase neměnná a snímače sítnice lidského oka se jeví jako nejbezpečnější biometrická identifikační metoda. [13]

1.6.2.1 Snímání a zpracování vzorku

Pro osvětlení sítnice se používá infračervené světlo a specializované kamery. Po nasvícení je sítnice oka téměř průhledná a vynikne tak síť cév, která se nachází za sítnicí. Zdroj světla ozařuje sítnici a odražené světlo dopadá do kamery. [1]

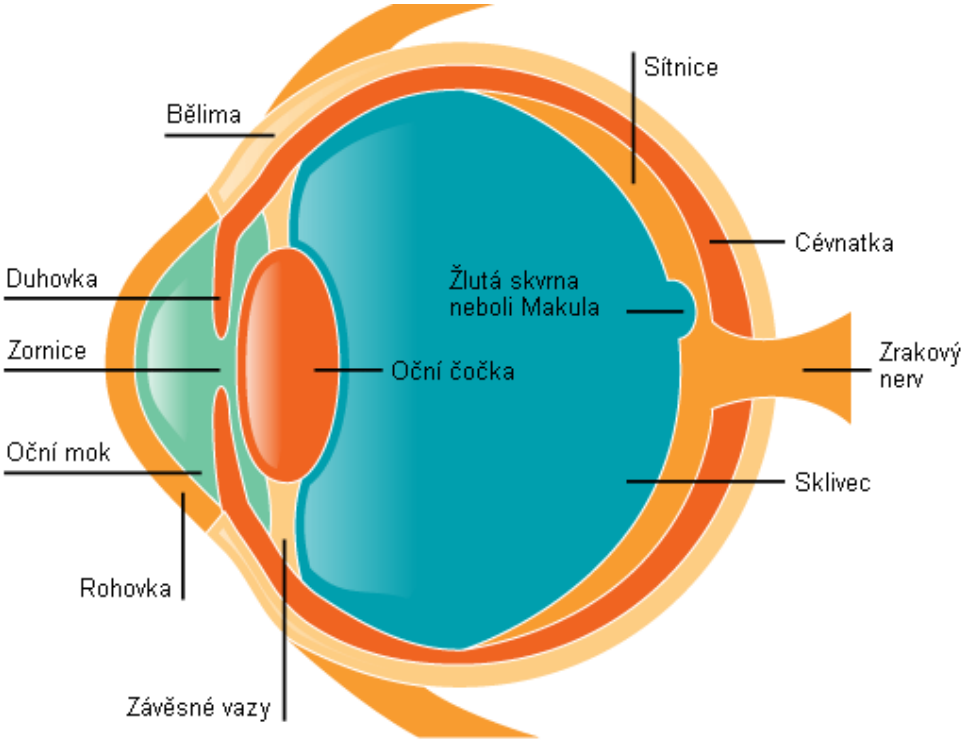
Další zpracování nasnímaného vzorku je podobné obecnému procesu popsanému v kapitole 1.5.

1.6.2.2 Výhody a nevýhody technologie

Technologie snímání duhovky je výhodná zejména z důvodů [13]:

- unikátnost pro každou osobu,
- časová neměnnost sítnice v průběhu života,
- nemožné vytvořit falzifikát,
- maximální úroveň bezpečnosti,
- skenování bez dotyku.

Mezi nevýhody této technologie patří vysoká cena zařízení a hlavně skutečnost, že samotné snímání není příliš uživatelsky příjemné. Ačkoliv je snímání zcela zdravotně nezávadné, lidé mají strach z poškození oka. Z těchto důvodů se příliš nepoužívá, i přestože poskytuje maximální spolehlivost (ze všech biometrických metod nejvyšší). [13]



Obrázek 1.7: *Stavba oka.* [3]

1.6.2.3 Možnosti využití technologie

Tato metoda je ideální pro využití zejména v oblastech s nutností velmi vysoké úrovně zabezpečení, jako jsou např. [1]:

- jaderné elektrárny a zbraně,
- letiště,
- věznice,
- bankovní trezory apod.

1.6.3 Oční duhovka

Duhovka se nachází v přední části oční bulvy (obrázek 1.7) a je pro každou osobu unikátní. Také identická dvojčata mají rozdílné duhovky a dokonce i duhovka očí jedné osoby není shodná. Charakteristické rysy duhovky se stabilizují brzy po narození a zůstávají beze změny po celý život člověka. [13]

1.6.3.1 Snímání a zpracování vzorku

Duhovka oka je viditelná zvenčí a pro snímání se využívají monochromatické CCD kamery. Ve snímcích s dostatečnou ostrostí je detekována duhovka a její vzor je následně kódován pomocí 2D waveletové demodulace (transformace, která umožňuje získat časově-frekvenční popis signálu). [1]

Následný postup zpracování vzorku je podobný obecnému principu popsanému v kapitole 1.5.

1.6.3.2 Výhody a nevýhody technologie

Výhody i nevýhody jsou velmi podobné technologii snímání oční sítnice (kapitola 1.6.2.2). Ovšem snímání duhovky je méně invazivní, než snímání sítnice. Z toho důvodu se pro identifikaci/verifikaci používá častěji oční duhovka než sítnice.

1.6.3.3 Možnosti využití technologie

Technologie snímání oční duhovky najde uplatnění v oblastech s potřebou vysoké úrovně zabezpečení, stejně jako technologie snímání oční sítnice (kapitola 1.6.2.3)

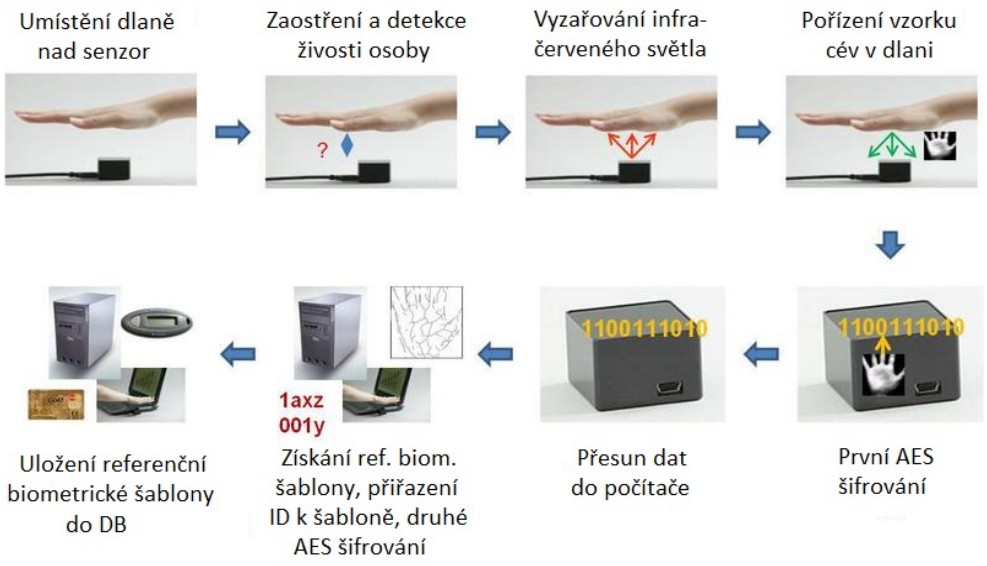
1.6.4 Krevní řečiště ruky

Lidská ruka je protkána sítí tepen a žil. Jejich geometrický tvar, velikost a orientace je pro každou osobu unikátní a dostatečně stabilní v průběhu života. Díky tomu lze na této metodě založit velmi spolehlivou identifikaci/verifikaci. [1]

1.6.4.1 Snímání a zpracování vzorku

Biometrické systémy pro vytváření snímku cév pracují na principu zachycení obrazu cév ruky (dlaně nebo pouze prstu) pomocí infračervených paprsků. Odkysličený hemoglobin v cévách tyto paprsky pohlcuje, čímž snižuje jejich odrážení. Zobrazené cévy tak vytvoří černý vzor. Snímání obrazu cév je bezdotykové, tudíž hygienické a pro uživatele velmi přívětivé. Obraz cév je u každé osoby jedinečný a díky jeho podrobné struktuře lze pro jednotlivé uživatele vytvořit biometrickou šablonu. Snímač zařízení pro vytváření obrazu cév ruky rozpozná vzorec jen v případě, kdy odkysličený hemoglobin cévami aktivně proudí (tj. prověřovaná osoba je živá), tudíž je tato technologie vysoce odolná vůči falšování a umožňuje dosáhnout vysoké úrovně zabezpečení. [14]

Další zpracování nasnímaného vzorku je podobné obecnému procesu popsanému v kapitole 1.5. Na obrázku 1.8 je znázorněn postup snímání obrazu krevního řečiště snímačem PalmSecure^{TM}od firmy Fujitsu.



Obrázek 1.8: *Snímání krevního řečiště ruky (Fujitsu PalmSecure^{TM}scan).* [4]

1.6.4.2 Výhody a nevýhody technologie

Krevní řečiště ruky je vhodné zejména z těchto důvodu [15]:

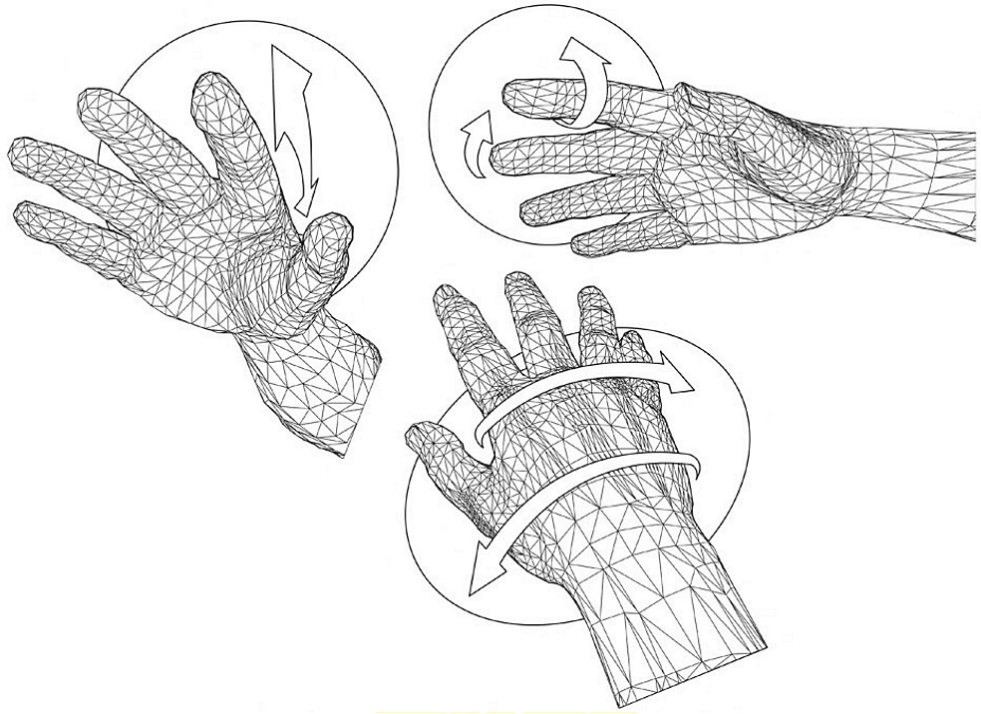
- unikátnost pro každou osobu,
- časová neměnnost sítě cév v průběhu života,
- rychlost zařízení a jednoduchost použití,
- nemožné vytvořit falzifikát,
- odolnost vůči znečištění rukou, vlhkosti a drobným úrazům,
- bezdotykový scan - hygienické a neinvazivní.

Nevýhodou je, že tuto technologii lze využít pouze pro verifikaci uživatele, k identifikaci není vhodná. [16]

1.6.4.3 Možnosti využití technologie

Metodu snímání krevního řečiště lze nasadit v nejrůznějších oblastech, např. bezpečnostní služby, finanční a bankovní služby, zdravotnictví, komerční společnosti, vzdělávací zařízení apod. Toto biometrické zařízení lze použít k následujícím účelům [14]:

- povolení vstupu do zabezpečených oblastí,



Obrázek 1.9: *3D model ruky.* [1]

- přihlašování k počítačům nebo serverovým systémům,
- přístup k pokladním systémům,
- bankomaty nebo prodejní stánky,
- ověřování identity apod.

1.6.5 Geometrie ruky

K identifikaci osoby může být díky své poměrně vysoké geometrické jedinečnosti využita i lidská ruka. V dnešní době již existují zařízení, které umožňují trojrozměrné měření geometrie ruky a za průkopníka je považována firma *Recognition Systems, Inc.*, která jako první vyvinula elektronický skener pro trojrozměrné snímání geometrie ruky (obrázek 1.9). [1]

Kombinace délky, šířky a tloušťky všech prstů jedné ruky, jejich obrys a kontura jsou relativně unikátní a lze na nich založit verifikaci osob. Identifikační charakteristiky ruky jsou od dospělosti neměnné, ovšem případné změny nejsou zcela vyloučeny (např. změna tloušťky prstů a dlaně, nemoci, úrazy apod.). [1]

1.6.5.1 Snímání a zpracování vzorku

Moderní trojrozměrné skenery snímají ruku pomocí optické kamery a soustavy zrcadel. Uživatel klade ruku na základovou desku, která je vyrobena z materiálu s velkou optickou odrazivostí, kamera snímá obraz ze shora i z boku a mikroprocesor konvertuje naměřené geometrické rozměry do několikabytové biometrické šablony. Tudíž vzniká možnost uchovávat obrovské množství referenčních šablon v jediném zařízení. [1]

Referenční šablona vzniká jako aritmetický průměr třech snímání a je do interní paměti zařízení ukládána společně s nějakým identifikačním kódem, který je uchován buď v paměti prověřované osoby (verifikace založená na znalostech), nebo v hmotném nosiči (verifikace založená na vlastnictví). V prvním případě se referenční biometrická šablona určuje pomocí znalostí prověřované osoby (PIN) a v druhém případě pomocí vlastnictví prověřované osoby (identifikační karta, mikročip, čárový kód apod.) [1]

Další zpracování nasnímaného vzorku je podobné obecnému procesu popsanému v kapitole 1.5.

1.6.5.2 Výhody a nevýhody technologie

Tato metoda je technologicky velmi jednoduchá a rychlá a je odolná vůči špíně a drobným povrchovým poraněním. Další velkou výhodou je velice malá velikost referenční šablony (u většiny přístrojů pouhých 9 bytů). Tato velikost šablony patří k nejmenším ze všech biometrických metod.

Nevýhody metody spočívají zejména v nemožnosti zpětné identifikace osoby z referenční šablony a v náchylnosti na vytvořené třírozměrné napodobeniny ruky oprávněné osoby. Navíc některým lidem může být nepříjemné přikládat ruku na „ohmatanýˇ přístroj. [1]

1.6.5.3 Možnosti využití technologie

Snímání geometrie ruky je používáno výhradně k rychlé a efektivní verifikaci osob. Jelikož tato metoda neposkytuje mnoho informací, není vhodné ji nasadit pro identifikaci. Tato metoda najde využití zejména jako verifikační prostředek k přístupu do různých areálů a prostorů s omezeným a známým počtem lidí, kteří jsou ke vstupu oprávněni. Typickými oblastmi využití jsou režimová pracoviště, výrobní závody, sklady, hraniční kontroly, věznice apod. [1]

1.6.6 Hlas

Hlas se řadí mezi behaviorální biometrické metody a je pro každého člověka jedinečný. Lze jej využít pro automatickou identifikaci/verifikaci osob nebo jako doplnění přístupového hesla. Ověření identity osoby je prováděno buď na základě proneseného hlasového hesla, nebo na základě automatické analýzy

řeči ověřované osoby během jejího přirozeného hlasového projevu. Moderní systémy umí odhalit i stoprocentní shodu s existujícím hlasovým vzorkem, a předejít tak zneužití hlasového záznamu. Podobně jako u zašifrovaných hesel, nevyužívá systém hlasové biometrie celých hlasových záznamů, ale z nich vytvořených hlasových šablon. V případě jejich zcizení jsou potenciálnímu útočníkovi prakticky k ničemu, nelze z nich totiž zpětně získat potřebný hlasový vzorek. [17] [18]

1.6.6.1 Snímání a zpracování vzorku

Pro hlasové nahrávky se používají kvalitní záznamová zařízení a hlasový signál by měl být pořízen v klidném prostředí bez rušivých hluků. Při analýze je využit systém hodnocení jednotlivých hlasových a řečových jevů (kvalita hlasu, způsob dýchání, způsob artikulace hlásek a hláskových skupin, frázování, melodie, přízvuk, pauzy, tempo, rytmus, dynamika apod.). V zásadě jsou všechny akustické analýzy pomocí přístrojů založeny na zjišťování spektra zvukového signálu. [1]

Zpracování zvukového vzorku je podobné obecnému procesu popsanému v kapitole 1.5.

1.6.6.2 Výhody a nevýhody technologie

Mezi hlavní výhody biometrie hlasu patří velká uživatelská přijatelnost, dobrá bezpečnost vůči útokům a nízká cena zařízení. [1]

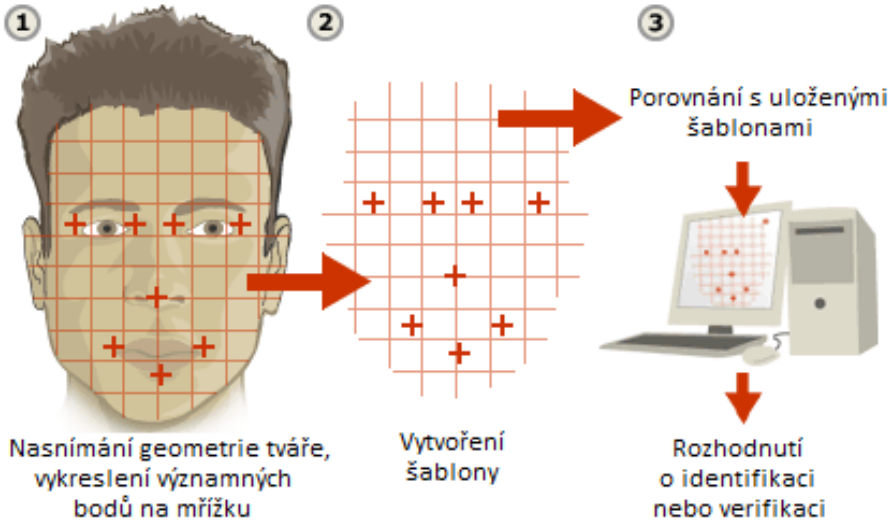
Nevýhody této technologie spočívají v zdlouhavé registraci nového uživatele (kvůli pokrytí všech proměnlivostí hlasu jsou nutná opakovaná registrační sezení), v nízké přesnosti technologie (změny v řečovém signálu vyvolané emočním a zdravotním stavem osoby i věkem, případná podobnost hlasu u příbuzných osob nebo signál s rušivými okolními zvuky může systémy pro hlasovou identifikaci/verifikaci zmást). [1]

1.6.6.3 Možnosti využití technologie

Největší využití tato metoda nachází v oblastech bankovnictví, telekomunikací a služeb, řízení přístupu apod. [18]

1.6.7 Tvář

Při identifikaci obličeje se využívají poznatky z antropologie, která se zabývá popisem a hodnocením znaků lidského těla. Pro jednoznačnou identifikaci je potřeba v obličeji nalézt všechny antropologicky významné body: vnitřní a vnější koutky očí, horizontální koutky rtů, špička nosu, přechod nosu do čela, spojení ušního lalůčku a tváře, body na chrupavce ucha chránící vnější zvukovod apod. [19]



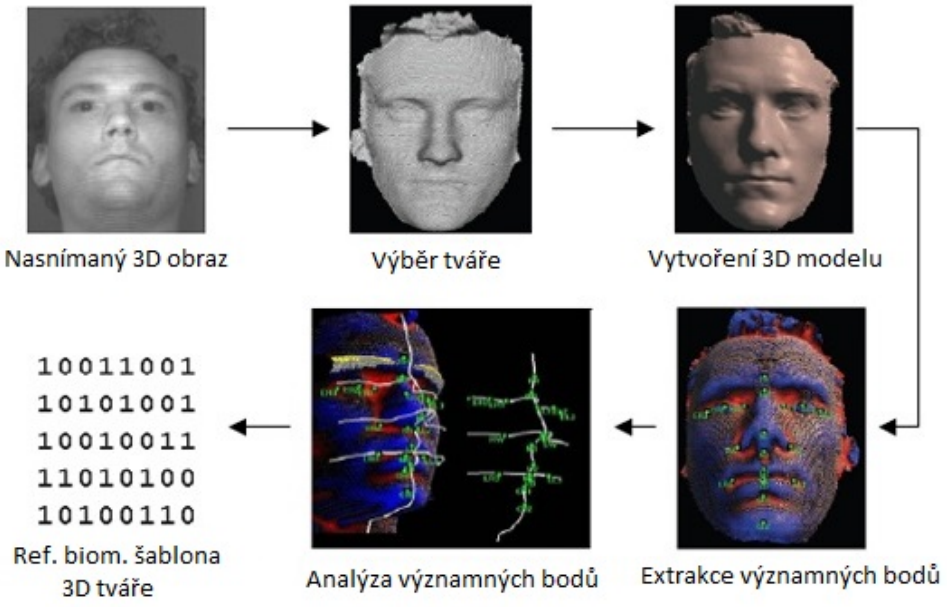
Obrázek 1.10: *2D snímání obličeje.* [5]

Biometrická technologie rozpoznávání tváře využívá dvourozměrné i trojrozměrné měření antropologicky významných bodů. Pro strojové zpracování lidských tváří existuje obrovské množství rozmanitých metod (neuronové sítě a genetické algoritmy, metoda deformačních modelů, metody založené na rozložení odstínů šedi v obraze, rozpoznávání obličejových rysů, informaci o barvách, symetrii apod.). [1]

1.6.7.1 Snímání a zpracování vzorku

2D snímání. Při dvourozměrném snímání obličeje se používá klasická kamera a v nasnímaném obraze se poté pomocí nejrůznějších algoritmů hledají antropologicky významné body (obrázek 1.10). Veškeré vzdálenosti mezi všemi body jsou měřeny pouze dvourozměrně. 2D techniky rozpoznávání obličeje jsou citlivé na měnící se osvětlení, použití kosmetiky a při snímání musí být obličej ve správné pozici (čelní obraz). Pro tuto technologii je stěžejní vysoká kvalita nasnímaného obrazu. Biometrický systém založený na této technologii je poměrně jednoduché oklamat například fotografií. [19] [5]

3D snímání. V případě trojrozměrného snímání se používá 3D skener, pomocí kterého lze vytvořit trojrozměrnou síť obličeje (obrázek 1.11). Křivky tváře jsou poté měřeny s přesností vyšší než na milimetry. Na rozdíl od 2D techniky není trojrozměrné snímání tváře citlivé na měnící se osvětlení ani použití kosmetiky a snímání je uskutečnitelné téměř z jakéhokoliv úhlu. 3D



Obrázek 1.11: *3D snímání obličeje.* [6]

technologie si poradí i s méně kvalitním snímkem. Biometrický systém s touto technologií nelze oklamat fotografií ani maskou. [5]

Počítačové zpracování vzorku nasnímaného klasickou kamerou i 3D skenerem je podobné obecnému procesu popsanému v kapitole 1.5.

1.6.7.2 Výhody a nevýhody technologie

2D technologie. Výhodami 2D technologie rozpoznávání tváře jsou rychlost a malá velikost referenční šablony (biometrický systém nepotřebuje tolik interní paměti). [6]

Negativními jevy, které ovlivňují identifikaci/verifikaci jsou citlivost na osvětlení, orientace hlavy, výrazy obličeje a make-up. Nevýhodou jsou i skutečnosti, že 2D obrázky obsahují omezené množství informací a zařízení s touto technologií je poměrně jednoduché oklamat. [6]

3D technologie. 3D technologie je výhodná z důvodu menší náchylnosti na deformace (mimika) obličeje, tato technologie také překonává problém změny orientace tváře a nevadí ji měnící se osvětlení ani make-up. [6]

Nevýhodou je menší rychlost (výpočetní složitost zpracování 3D dat je vyšší než u 2D dat). [6]

Obecnou výhodou této metody nehledě na techniku snímání je velká univerzálnost a uživatelská přijatelnost/přívětivost.

Obecnou nevýhodou metody je časová nestálost lidské tváře. Na vzhled tváře má vliv stárnutí i změna tělesné hmotnosti nebo úrazy a nemoci.

1.6.7.3 Možnosti využití technologie

Tato biometrická metoda nachází uplatnění ve velkém množství oblastí, jako jsou: bezpečnostní systémy pro kontrolu a regulaci přístupů zaměstnanců do objektu, docházkové aplikace, ochrana věznic, vládních objektů, finančních institucí, hotelů, kasin, zdravotních zařízení i domova, oblasti hraniční, celní a imigrační kontroly, biometrická autentizace spojená s kreditními kartami, pasy, řidičskými průkazy a ostatními doklady, apod. [1]

1.6.8 Dynamika psaní na klávesnici

Dynamika psaní na klávesnici poskytuje unikátní behaviorální biometriku zejména ve spojení s autentizací uživatelů digitálních zařízení. Měří se a vyhodnocuje se především rychlost psaní, frekvence chyb, styl psaní velkých písmen a síla použitá pro stisk klávesy. Dynamika stisku kláves se typicky zkoumá na zadávaném přístupovém heslu nebo frázi. [20] [1]

1.6.8.1 Snímání a zpracování vzorku

Způsob získávání a zpracování biometrických informací se u této technologie vymyká obecnému procesu popsanému v kapitole 1.5, jelikož tato technologie nepotřebuje žádný vlastní specializovaný HW. Informace o stisknutých klávesách se získávají na úrovni operačního systému, který dovoluje zachytit stisk i uvolnění klávesy. [20] [1]

Tato technologie je založena na algoritmech porovnávajících vzory nebo na neuronových sítích a její úspěch závisí čistě na softwarové implementaci. [20]

1.6.8.2 Výhody a nevýhody technologie

Mezi výhody patří unikátnost - úhoz může být měřen s přesností na milisekundy, tudíž je prakticky nemožné najít dva totožné vzorky při tak vysokém rozlišení. Další velkou výhodou je velmi nízká cena implementace a nasazení, jelikož tato technologie je čistě SW produkt a není závislá na specializovaném HW. Pozitivum je také velmi vysoká neinvazivnost technologie - systém požaduje naprosto minimální změnu v chování osoby, tudíž uživatel téměř ani neví, že je prověřován biometrickým systémem. Tato technologie také výrazně zvyšuje sílu a životnost hesla a nabízí způsob, jak průběžně ověřovat identitu uživatele po celou dobu trvání interakce uživatele se systémem prostřednictvím vstupních zařízení (klávesnice). [20]

Mezi nevýhody patří poměrně nízká přesnost při ověřování osoby v důsledku odchylek v psaní způsobené vnějšími faktory, jako je poranění, únava

nebo rozptýlení. Pro úspěšnou verifikaci je potřeba, aby uživatel vždy dokázal psát stejným nebo alespoň velice podobným způsobem. Další negativum této technologie je časová nestálost - dynamika psaní se může měnit z nejrůznějších příčin (rutinní zadávání hesla, zlepšení schopnosti psaní, adaptace na různé klávesnice apod.). Vědci proto doporučují často aktualizovat uložené profily ověřovaných uživatelů. [20]

1.6.8.3 Možnosti využití technologie

Tato technologie najde díky své hardwarové nenáročnosti využití zejména ve spojení s digitálními zařízeními jako jsou počítače, mobilní zařízení, panely s dotykovou obrazovkou apod. [20]

1.7 Kritéria hodnocení pro biometrické technologie

Následující charakteristiky jsou důležité jak pro funkčnost biometrických identifikačních a verifikačních technologií, tak i pro jejich praktické efektivní nasazení, tedy celkovou úspěšnost. Kritéria jsou spojena nejen se základní teorií a praxí identifikace/verifikace a ochrany osobních údajů, ale i s praktičností, ekonomií i společenskou a finanční přijatelností. Tyto kritéria podle [1] dělíme do následujících skupin:

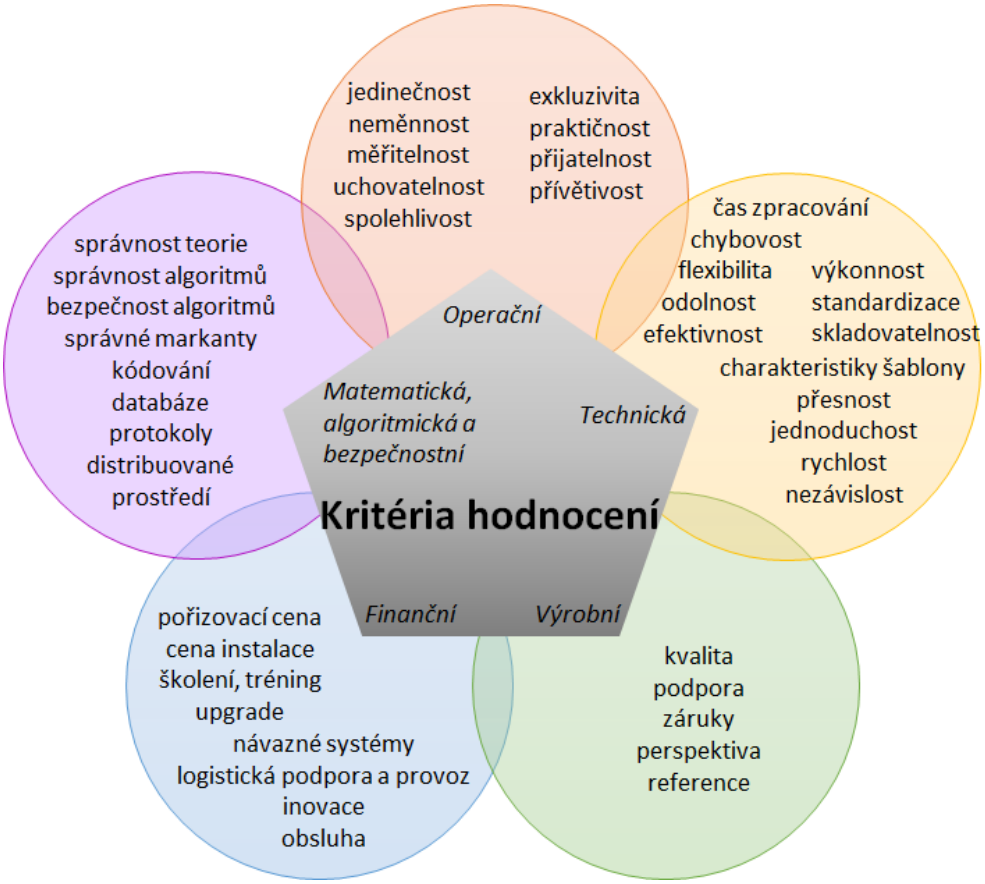
- operační,
- technická,
- výrobní,
- finanční,
- matematická, algoritmická a bezpečnostní.

Následující podkapitoly obsahují podrobnější popis každé skupiny a jejich příslušných charakteristik (obrázek 1.12), podle kterých se posuzuje kvalita dané biometrické technologie.

1.7.1 Operační kritéria

V této skupině se podle [1] posuzují následující charakteristiky:

- **Jedinečnost.** Aby bylo možné odlišit jednu osobu od druhé s vysokou spolehlivostí a přesností, musí být biometrické charakteristiky dané identifikační metody dostatečně unikátní.
- **Neměnnost.** Markanty, na kterých je založena biometrická identifikace, musí být v čase neměnné.



Obrázek 1.12: *Základní kritéria hodnocení biometrických technologií.* [1]

- **Měřitelnost.** Charakteristiky, na kterých je založena identifikace, musí být měřitelné a symbolicky vyjádřitelné.
- **Uchovatelnost.** Naměřené identifikační charakteristiky musí být možné archivovat, aniž by došlo ke ztrátě jejich kvality (např. příliš velká referenční šablona je velmi nepraktická).
- **Spolehlivost.** Proces měření, zpracování, ukládání a vyhodnocování biometrických charakteristik musí být spolehlivý a musí jít kdykoliv zopakovat se stejnými výsledky.
- **Exkluzivita.** Identifikační metoda by měla být úplná (aby nebyla nutná další podpůrná identifikace).
- **Praktičnost.** Metoda musí být ve všech směrech praktická (minimální kontakt s uživatelem, minimum času stráveného procesem identifikace, minimální množství úkonů, jednoduchost měření, minimum tréninku uživatele).

- **Přijatelnost.** Musí být vyloučeny takové technologické metody, které provádějí zásah do integrity lidského těla a jakýmkoliv způsobem lidský organismus poškozují nebo oslabují.

- **Uživatelská přívětivost.** Proces snímání a vyhodnocování má být nerušivý (uživatel by neměl mít pocit diskriminace v souvislosti např. s barvou pleti, věkem, profesí apod.).

1.7.2 Technická kritéria

Mezi nejčastěji vyhodnocovaná kritéria v oblasti technického řešení biometrické identifikace podle [1] patří:

- minimální čas zpracování/vyhodnocení identifikace,
- přijatelná chybovost (FRR, FAR viz kapitoly 1.8.1 a 1.8.2),
- flexibilita,
- odolnost,
- efektivnost,
- výkonnost,
- standardizace (kompatibilita, schopnost užívat části jiných systémů),
- skladovatelnost identifikačních charakteristik,
- požadovaný prostor na uložení a zpracování identifikačních charakteristik, velikost šablony (co nejmenší rozměry, kapacita),
- přesnost,
- jednoduchost,
- rychlost,
- nezávislost na vnějším prostředí (schopnost odfiltrovat rušivé vlivy okolí).

1.7.3 Výrobní kritéria

Při výběru zařízení se zohledňují i kvality dodavatele nebo výrobce technologií a jejich schopnost efektivní a cenově přijatelné podpory při provozu zařízení. Mezi další výrobní kritéria, která můžeme zohlednit, patří také kompatibilita s jinými technologiemi, reference od dalších uživatelů apod. [1]

1.7.4 Finanční kritéria

Finance se posuzují jak z jednorázového, tak i dlouhodobého pohledu a hrají rozhodující roli při vývoji i nákupu biometrických technologií. Pod finanční kritéria podle [1] spadá následující:

- pořizovací cena technologie,
- cena instalace,
- náklady spojené s uvedením do provozu (školení, trénink),
- cena následujících upgradů, nových modifikací,
- cena návazných systémů (počítačových, fyzické ostrahy apod.),
- cena logistické podpory a provozu,
- cena dalších zamýšlených zařízení, budoucího rozvoje systému,
- cena obsluhy zařízení apod.

1.7.5 Matematická, algoritmická a bezpečnostní kritéria

Abychom mohli posoudit kvalitu biometrické technologie, musíme umět ocenit i biometrickou metodu, na níž je technologie založena. Biometrické metody používají různé matematické algoritmy, komprese, kódy a protokoly. Biometrické algoritmy jsou navzájem podobné a liší se pouze v technologiích metod, ve kterých jsou použity. Tyto algoritmy lze z matematického hlediska rozdělit do následujících skupin [1]:

- statistické metody modelování,
- dynamické programování,
- neuronové sítě.

Různé algoritmy nabízejí různý stupeň bezpečnosti. V případě biometrických technologií použitých pro zabezpečení finančních transakcí, požadujeme vysokou úroveň zabezpečení (kryptografické algoritmy a techniky musí odolat i velmi intenzivním útokům). O kvalitě technologie biometrické metody vypovídají kromě matematické teorie i algoritmy implementující danou teorii, kódování výskytu identifikačních markantů, protokoly a databáze, ve kterých jsou biometrická data uložena. Při hodnocení matematických, algoritmických a bezpečnostních kritérií se obvykle posuzují [1]:

- správnost teorie,
- správnost algoritmů,

- bezpečnost algoritmů,
- správnost výběru markantů (identifikačních markantů, klíčů),
- efektivita a zabezpečení kódování biometrických dat,
- zabezpečení databáze s biometrickými daty,
- bezpečnost protokolů,
- bezpečnost síťového a distribuovaného prostředí.

Identifikační proces zahrnuje snímání, kódování, kompresi, přenášení a dekompresi biometrických dat a v každé této části musí být algoritmy dostatečně spolehlivé a bezpečné.

1.8 Měření výkonnosti biometrických metod a zařízení

V případě nasazení fyzického zařízení do praktického využití vzniká zcela oprávněná otázka: Jak je zařízení výkonné a spolehlivé? Existují charakteristiky, pomocí kterých lze porovnávat různé biometrické metody a na jejich základě zkonstruovaná zařízení a stanovit objektivní závěr, jak je dané zařízení vhodné pro daný případ praktického využití. Těchto rozhodujících charakteristik může být mnoho, například počet realizovaných identifikací/verifikací v určité časové jednotce, rychlost zařízení, uživatelská přijatelnost/přívětivost, cena, spolehlivost a odolnost zařízení apod. To však nejsou ta nejdůležitější kritéria, jelikož hlavním cílem veškeré biometrické identifikace nebo verifikace je *jednoznačné* a *bezchybné* nalezení nebo potvrzení identity osoby. V praxi se proto pracuje s dvěmi negativními a nežádoucími jevy, ukazujícími na bezpečnostní a uživatelskou spolehlivost: *False Rejection Rate - FRR* a *False Acceptance Rate - FAR.*

Pravděpodobnost chybného odmítnutí nebo přijetí biometrických metod nelze teoreticky vypočítat. Biometrické metody identifikace/verifikace jsou založeny na statistickém vyhodnocování podobnosti biometrického vzoru a biometrické šablony. Při každém snímání biometrického vzoru nejsou zaznamenávány absolutně stejné hodnoty a markanty. V důsledku toho se pak i obě porovnávané šablony nepatrně liší, tedy *skóre porovnání* (míra shody) je pokaždé odlišné a závisí především na biometrické aplikaci a na jejím technickém řešení. [1]

1.8.1 Pravděpodobnost chybného odmítnutí - FRR

Pravděpodobnost chybného odmítnutí autorizované osoby biometrickým zařízením (*False Rejection Rate*) udává, s jakou pravděpodobností bude biometrické zařízení chybovat a nerozpozná oprávněného uživatele. Tato veličina je

podle [1] definována:

$$FRR = \frac{N_{FR}}{N_{EIA}} \quad \text{nebo} \quad FRR = \frac{N_{FR}}{N_{EVA}}, \tag{1.1}$$

kde:

- N_{FR} – Number of False Rejection (počet chybných odmítnutí)
- N_{EIA} – Number of Enrolle Identification Attemps (počet pokusů oprávněných osob o identifikaci)
- N_{EVA} – Number of Enrolle Verification Attemps (počet pokusů oprávněných osob o verifikaci)

Chybné odmítnutí je sice nežádoucí, ale z hlediska bezpečnosti se nejedná o kriticky negativní jev.

1.8.2 Pravděpodobnost chybného přijetí - FAR

Pravděpodobnost chybného přijetí neoprávněné osoby biometrickým zařízením (*False Acceptance Rate*) udává, s jakou pravděpodobností bude biometrické zařízení chybovat a akceptuje neoprávněnou osobu. Tato veličina je podle [1] definována:

$$FAR = \frac{N_{FA}}{N_{IIA}} \quad \text{nebo} \quad FAR = \frac{N_{FA}}{N_{IVA}}, \tag{1.2}$$

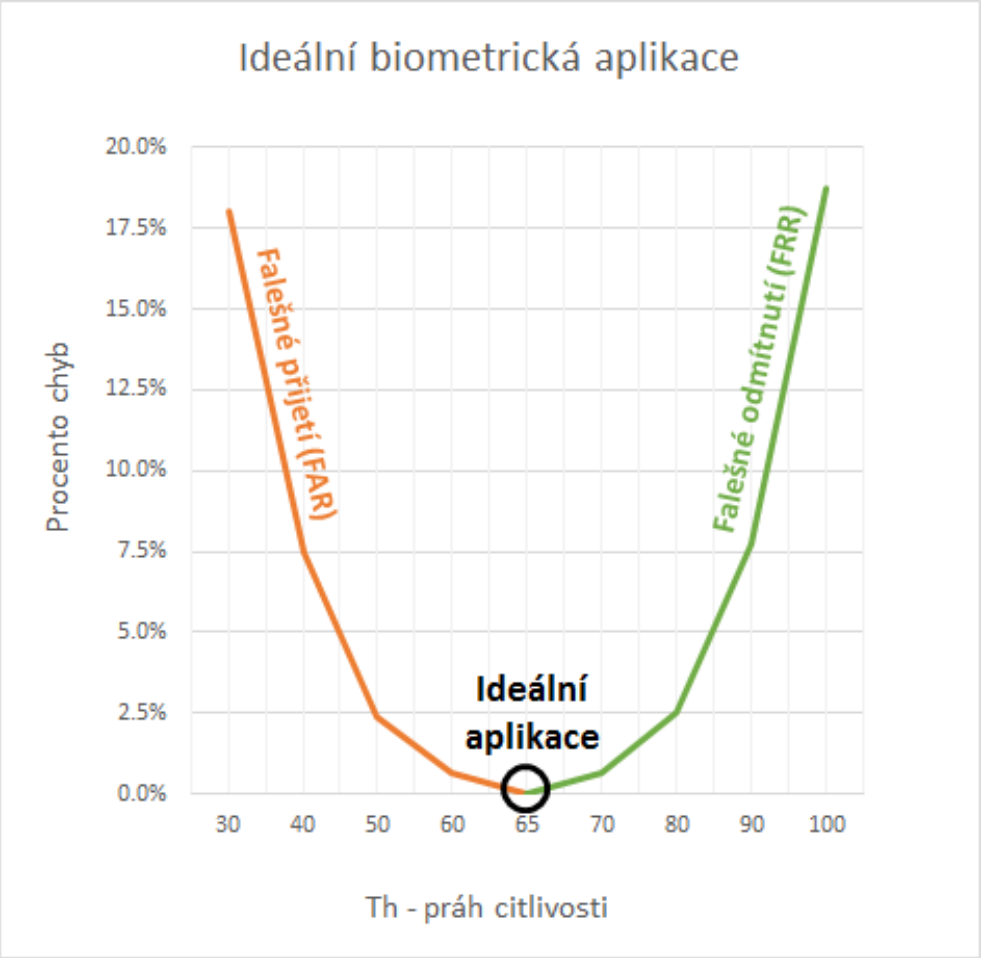
kde:

- N_{FA} – Number of False Acceptance (počet chybných přijetí)
- N_{IIA} – Number of Impostor Identification Attemps (počet pokusů neoprávněných osob o identifikaci)
- N_{IVA} – Number of Impostor Verification Attemps (počet pokusů neoprávněných osob o verifikaci)

Na rozdíl od chybného odmítnutí, může chybné přijetí znamenat kritické narušení bezpečnosti a často mívá závažné následky.

1.8.3 Vztah FRR a FAR

Ideální zařízení by nemělo vykazovat žádnou chybovost, tudíž všechny prověřované osoby by měly být 100 % rozpoznány, tj. neexistují ani neoprávněně odmítnuté, ani neoprávněně akceptované osoby. V tomto případě obecně platí, že FRR = FAR = 0. Graf vztahu FRR a FAR z pohledu ideální biometrické aplikace popisuje obrázek 1.13.



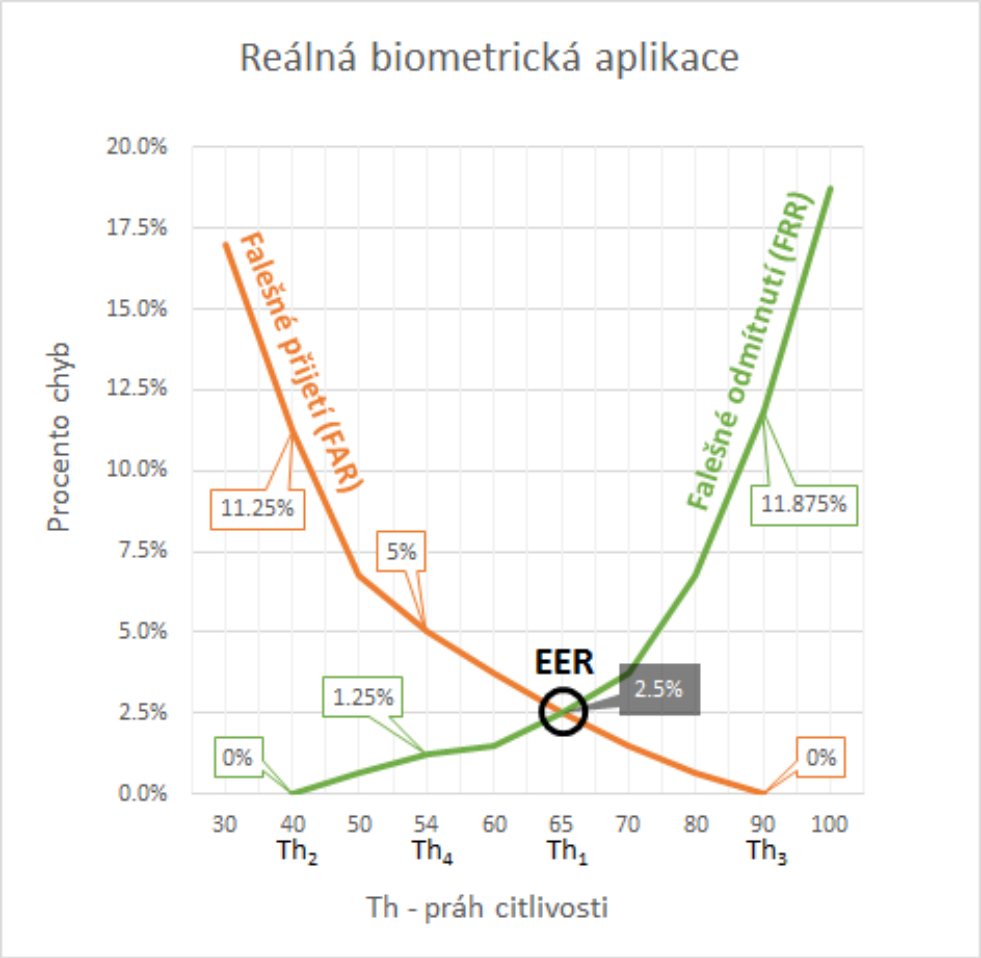
Obrázek 1.13: *Ideální biometrická aplikace.* Vytvořeno autorem podle [1].

V praxi ovšem ideální zařízení neexistuje. Každé reálné zařízení je různě citlivé na rozmanité vlivy, které ovlivňují jeho výslednou činnost. U biometrických zařízeních lze regulovat vstupní citlivost, jež se pak odráží ve výsledném chování biometrického zařízení. Graf vztahu FRR a FAR v případě reálné biometrické aplikace (viz obrázek 1.14) je popsán v kapitole 1.8.3.1.

1.8.3.1 Příklad reálné biometrické aplikace

Máme biometrickou aplikaci, jejímž úkolem je verifikovat oprávněnost vstupu osoby do chráněného objektu.

Na grafu vztahu FRR a FAR reálné biometrické aplikace lze vidět, že pokud posouváme práh citlivosti doprava po ose x, křivka FRR roste a křivka FAR naopak klesá.



Obrázek 1.14: *Reálná biometrická aplikace.* Vytvořeno autorem podle [1].

Předpokládejme, že požadujeme, aby přijetí neoprávněné osoby bylo absolutně vyloučeno, tudíž FAR = 0 (bod Th_3 na ose x). Této hodnotě pak ale odpovídá FRR = 11,875 %, tedy téměř 12 % oprávněných uživatelů bude neoprávněně odmítána. Kdybychom naopak požadovali nulovou pravděpodobnost odmítnutí oprávněné osoby (bod Th_2 na ose x), do objektu pronikne 11,25 % neoprávněných osob.

Nastavíme-li práh citlivosti například na hodnotu 54 (bod Th_4 na ose x), pak FAR = 5,0 % a FRR = 1,25 %. Bod, ve kterém se obě křivky protínají, se nazývá Equal Error Rate (EER) (bod Th_1 na ose x) a platí pro něj podle [1] rovnost:

$$EER_{\mathrm{FRR}} = EER_{\mathrm{FAR}}. \tag{1.3}$$

Bod EER má pouze orientační význam v porovnávání dvou různých aplikací. V praxi je práh citlivosti nastavován podle toho, k čemu má být biometrická

Tabulka 1.3: *Orientační hodnoty FAR, FRR a EER jednotlivých biometrických metod.* [21] [22] [20]

Biometrická metoda	FAR	FRR	EER
Otisky prstů	2%	2%	2%
Hlas	2%	10%	6%
Tvář	1%	10%	nedefinováno
Oční duhovka	0,01%	0,1%	$< 1\%$
Oční sítnice	0%	0,4%	$< 1\%$
Geometrie prstů a ruky	3%	4%	1%
Krevní řečiště ruky	0,1%	0,1%	0,2%
Dynamika psaní na klávesnici	5%	6%	5%

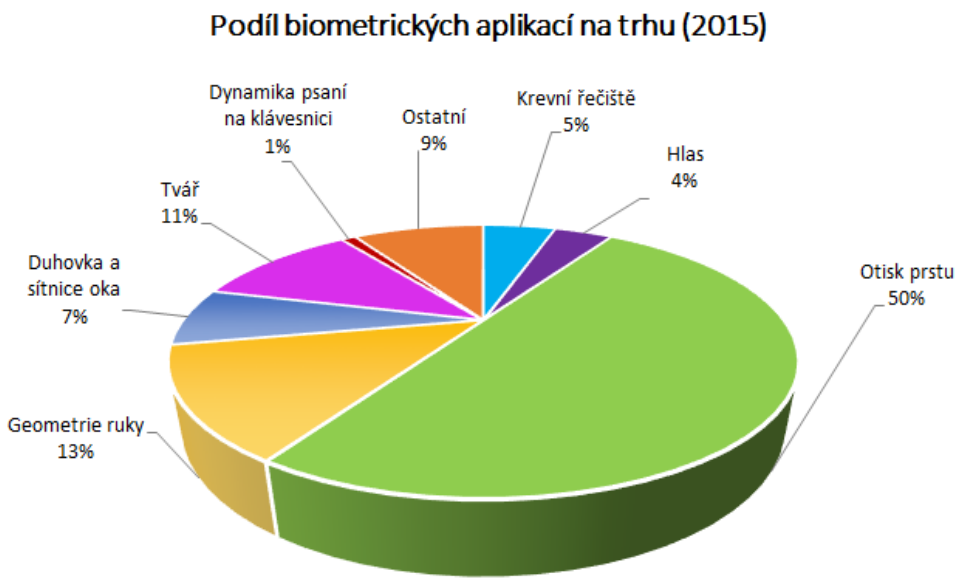
aplikace použita a hodnoty nutně nemusí procházet bodem EER. Biometrické aplikace, na které je kladen velký důraz na bezpečnost, mají citlivostní práh nastaven na vyšší hodnotu a tolik nevadí, že pravděpodobnost jevu FRR je častější. V případě těchto aplikací je důležitá nízká hodnota jevu FAR. [1]

1.8.4 Hodnoty FRR, FAR a EER konkrétních biometrických metod

V tabulce 1.3 jsou uvedeny přibližné hodnoty FAR, FRR a EER vybraných biometrických metod. Na hodnoty v tabulce mají vliv nejrůznější okolnosti. Pokud bychom měřili hodnoty FAR, FRR a EER v ideálních podmínkách, vyšla by jiná čísla než u měření v běžných provozních podmínkách. Stejně tak by se hodnoty měnily v závislosti na kvalitě biometrických zařízení a na výrobci daného zařízení. Faktorů ovlivňujících FAR, FRR a EER je velké množství a při výběru biometrického zařízení záleží na účelu, pro který je zařízení určeno. Obecně platí, že čím více se hodnota EER blíží nule, tím lépe (viz obrázek ideální biometrické aplikace 1.13).

1.9 Podíl biometrických aplikací na trhu

Graf na obrázku 1.15 znázorňuje zastoupení biometrických aplikací na trhu (průzkum z roku 2015). Největší podíl vlastní technologie otisku prstu, geometrie ruky, snímání tváře a duhovky/sítnice. Tato skutečnost se ovšem s vývojem ostatních technologií mění a do popředí se dostávají i sporadicky využívané technologie.



Obrázek 1.15: *Podíl biometrických aplikací na trhu.* Vytvořeno autorem podle [7].

Kapitola 2

Praktická část

Tato kapitola se zabývá podrobnou analýzou biometrických metod podle kritérií hodnocení, procesní analýzou před a po nasazení biometrického systému, finanční analýzou biometrických metod a celkovým porovnáním a zhodnocením těchto metod pro nasazení v typových podnicích. Pro účely této části práce jsem zvolila tyto typové podniky:

1. **Finanční instituce**, které kladou velký důraz na vysokou úroveň bezpečnosti a využití biometrických systémů je samozřejmé.
2. **Výrobní závody**, ve kterých nejde tolik o bezpečnost, ale spíše o kontrolu docházky a osob oprávněných ke vstupu do určitých prostor.
3. **Osoby samostatně výdělečně činné**, jako např. účetní, auditoři, daňoví poradci, právníci apod. pracující s důvěrnými informacemi, jež potřebují chránit.

2.1 Typový podnik č. 1 - Finanční instituce

Všechny organizace, jejichž hlavní činností je hospodaření s finančními zdroji, se souhrnně nazývají finanční instituce (tedy nejen banky, ale i např. kasina a herny). Proto se pro jednoduchost v této práci pod pojmem finanční instituce rozumí pouze banky, pojišťovny a spořitelny. Pro tyto organizace je vysoká úroveň bezpečnosti obzvláště důležitá, neboť denně čelí známým i neznámým kybernetickým hrozbám. To je jeden z důvodů, proč finanční instituce investují do zabezpečení své vnitřní infrastruktury a procesů mnohem více prostředků než ostatní organizace z nefinančního sektoru. Finanční instituce neustále zdokonalují a vylepšují své zabezpečení, aby byly schopné ubránit se kybernetickým útokům, ale i uspokojit nároky svých klientů.

2.1.1 IS/ICT infrastruktura

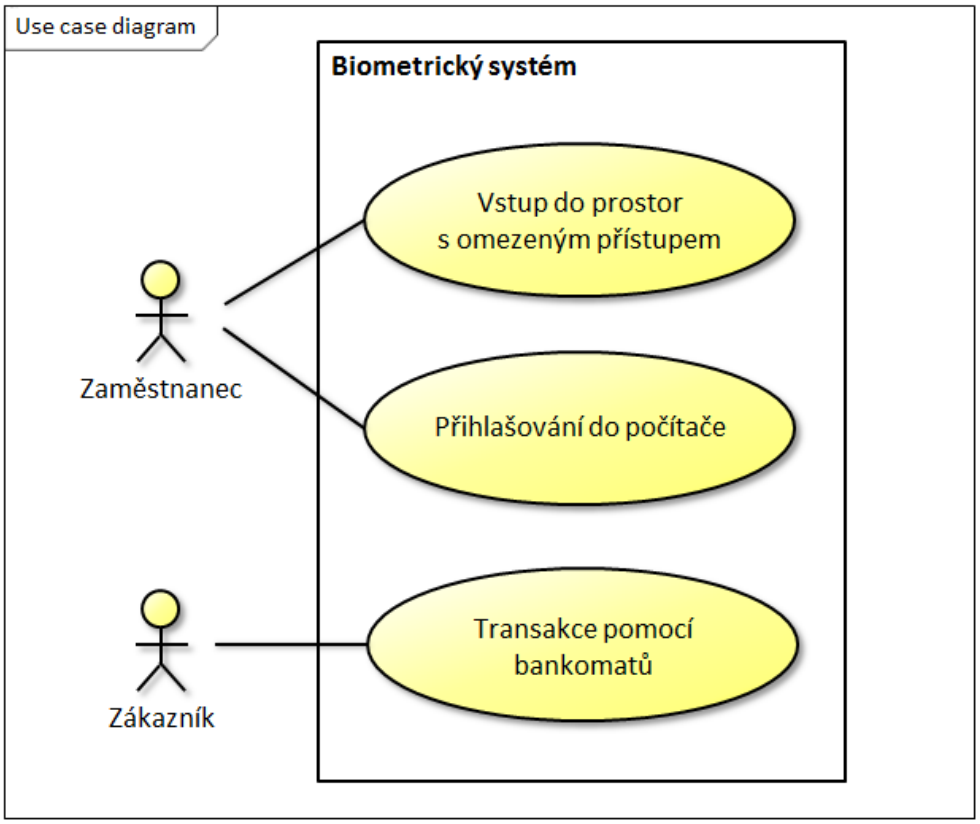
IS/ICT infrastruktura finančních institucí je velmi rozsáhlá, složitá a specifická a těžko se obecně popisuje.

Hlavní činností finančních institucí je zajištění zpracování transakcí. Jelikož většina finančních institucí má více poboček, mají typicky jeden centrální server, na kterém je spuštěn nějaký centrální informační systém, který spravuje veškeré informace o transakcích a navazují na něj další podpůrné systémy a aplikace. Všichni zaměstnanci musí při práci s těmito systémy prokázat svoji identitu a oprávnění, proto je u všech počítačů zapotřebí verifikačních prostředků. Centrální server je umístěný na jedné z poboček nebo v datovém centru. Všechny pobočky s centrálním serverem komunikují přes internet s využitím zabezpečovacích protokolů. Veškeré finanční instituce mají digitálně vyspělou IS/ICT infrastrukturu a všechny části této infrastruktury jsou propojeny mezi sebou nebo s centrálním serverem. Tyto instituce kladou velký důraz na bezpečnost. Komunikaci po síti a oprávnění přístupu do určitých prostor a vykonávání určité činnosti mají zabezpečeno identifikačními kartami, hesly a jistě i nějakými biometrickými systémy.

2.1.2 Případy užití biometrického systému

Finanční instituce s největší pravděpodobností již nějaký biometrický systém využívají (např. při vstupu do trezoru apod.). Takže první případ užití (identifikace/verifikace při pokusu o vstup do různých prostor) není ve finančních institucích neobvyklý. Ovšem v mé práci je vhodné tento případ užití uvést, jelikož ve finančních institucích se jistě najde prostor, který je nedostatečně zabezpečený pouze hesly nebo ID kartami.

Druhý případ užití se týká práce zaměstnanců s počítači. Většinou jsou k přihlašování do počítače využita pouze hesla nebo ID karty, což může být nedostačující a nepraktické (např. při ztrátě/zapomenutí ID karty), proto je vhodné použití biometrického systému i při přístupu do počítače.



Obrázek 2.1: *Diagram případů užití biometrického systému ve finančních institucích.*

Poslední případ užití popisuje využití biometrického systému v bankomatech, se kterými přijdou do styku zákazníci.

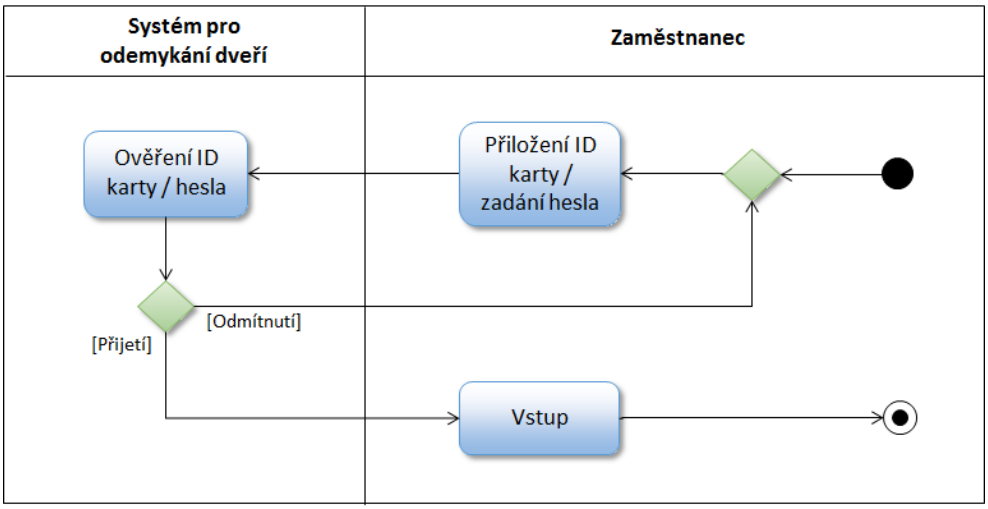
Všechny tyto možnosti využití biometrického systému znázorňuje diagram případů užití na obrázku 2.1.

2.1.3 Procesní analýza - situace bez biometrického systému

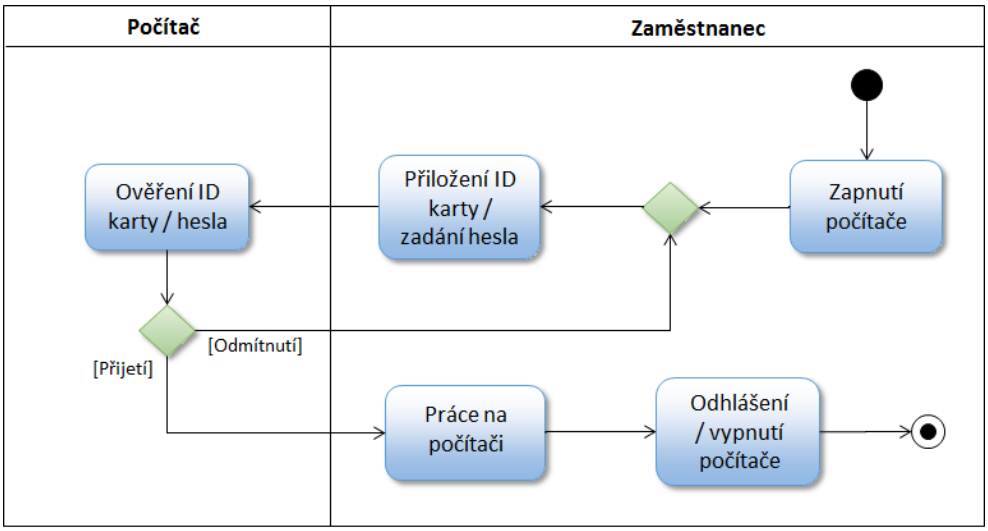
Diagram na obrázku 2.2 zobrazuje proces pokusu o vstup do nějakého prostoru, do kterého by měly vstupovat pouze oprávněné osoby. Tento prostor s omezeným přístupem není chráněn biometrickým systémem, ale pouze nějakým elektronickým systémem pro automatické odemykání dveří, který odemkne dveře na základě pozitivní verifikace pomocí hesla nebo čipové karty.

Tento typ ochrany je nespolehlivý a poměrně snadno lze obejít.

Obrázek 2.3 popisuje aktivity při používání počítače zaměstnancem finančních institucí. Po zapnutí počítače zaměstnanec zadává heslo nebo přikládá čipovou kartu k čtečce propojené s počítačem. Pokud jsou heslo nebo ID karta



Obrázek 2.2: *Diagram aktivit pokusu zaměstnance o vstup do prostor s omezeným přístupem ve finančních institucích.*

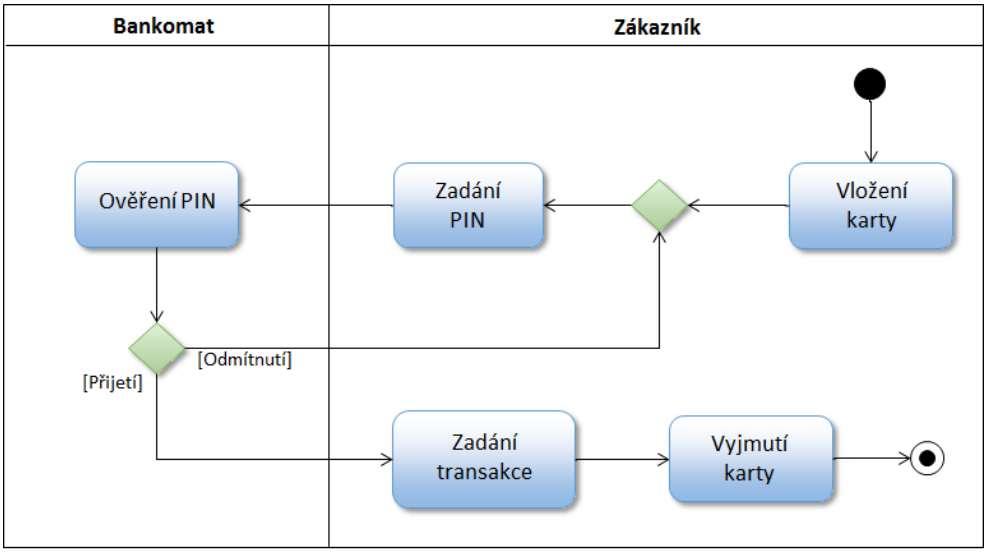


Obrázek 2.3: *Diagram aktivit přihlašování zaměstnance do počítače ve finančních institucích.*

úspěšně ověřeny, zaměstnanec může s počítačem pracovat. V opačném případě je zaměstnanec vyzván k opakované verifikaci své osoby. Po ukončení práce na počítači zaměstnanec uzamkne počítač nebo jej vypne.

Stejně jako u ochrany různých prostor není takové přihlašování k počítači obyčejným heslem nebo čipovou kartou dostatečně bezpečné.

Diagram na obrázku 2.4 se týká především bank a znázorňuje interakci zá-



Obrázek 2.4: *Diagram aktivit použití bankomatu zákazníkem.*

kazníka s bankomatem. Zákazník do bankomatu vloží kartu a zadá svůj PIN. V případě nesprávně zadaného PIN jej musí zákazník zadat znovu. Pokud zákazník zadá nesprávný PIN třikrát po sobě, dochází k blokaci karty, která není zákazníkovi vrácena. Pokud je PIN zadán správně, může zákazník pomocí bankomatu provádět různé transakce, např. vybírat hotovost, převádět nebo vkládat finanční prostředky apod. Po ukončení transakcí zákazník kartu vyjme.

Banky na ochranu a zabezpečení bankomatů nekladou příliš velký důraz a verifikace pomocí PIN je nedostatečná.

2.1.4 Výběr vhodných biometrických metod pro nasazení

✔ **Otisk prstu.** Biometrická metoda otisku prstu poskytuje poměrně vysokou úroveň bezpečnosti a je vhodná jak pro verifikaci, tak i pro identifikaci. Ve finančním sektoru jistě najde své místo k využití.

✘ **Hlas.** Hlasová identifikace/verifikace je nevhodná z důvodu nízké přesnosti technologie, což nevyhovuje potřebám finančních institucí. Stejně tak je důležité tiché prostředí pro snímání zvukové stopy, což firmy s velkým počtem zaměstnanců ne vždy mohou poskytnout.

✔ **Tvář.** Využití 2D technologie ve finančních institucích je z hlediska požadované úrovně bezpečnosti nedostačující, jelikož je tato technologie lehce

oklamatelná falzifikátem. Ovšem 3D technologie řeší nedostatky 2D technologie a díky své vysoké odolnosti vůči falzifikátům je vhodným kandidátem pro nasazení ve finančních institucích.

✔ **Oční duhovka a sítnice.** Tato technologii je velmi nákladná a není uživatelsky příliš přijatelná/přívětivá, ale poskytuje maximální úroveň zabezpečení, která je pro finanční instituce obzvláště důležitá.

✘ **Geometrie ruky.** Biometrická metoda geometrie ruky je nevhodná z důvodu náchylnosti na třírozměrné napodobeniny ruky oprávněné osoby. Navíc se tato technologie nedá použít k identifikaci, ale pouze k verifikaci.

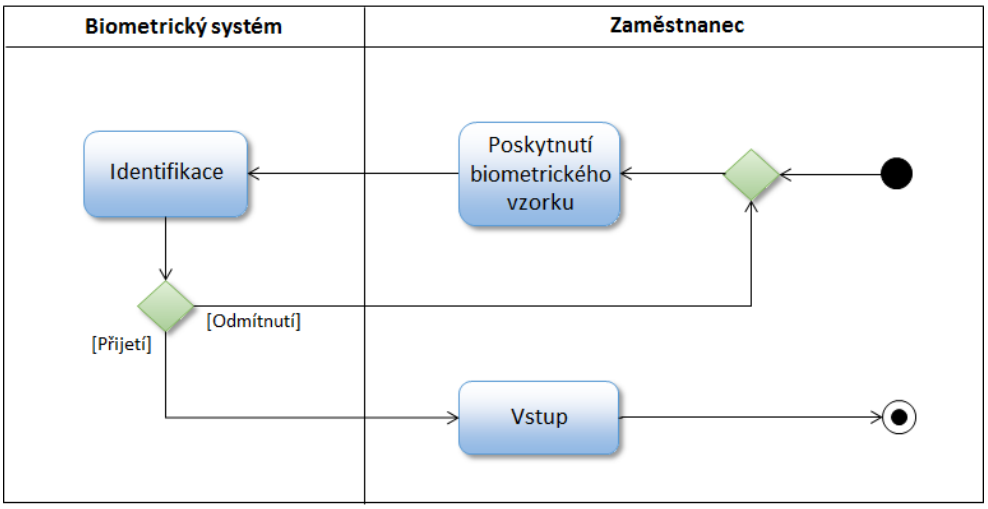
✘ **Krevní řečiště ruky.** Stejně jako biometrická metoda geometrie ruky se technologie krevního řečiště ruky nedá použít pro identifikaci uživatele.

✘ **Dynamika psaní na klávesnici.** Tato biometrická metoda je pro finanční instituce nevhodná hlavně kvůli nízké přesnosti, časové nestálosti měřených biometrik a obecně kvůli nedostačující úrovni zabezpečení.

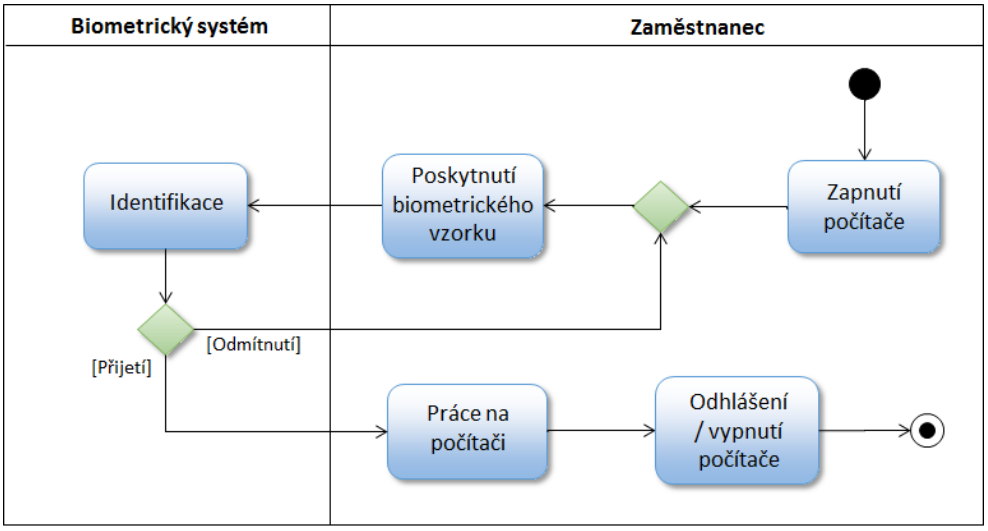
2.1.5 Procesní analýza - situace po nasazení biometrického systému

Diagram na obrázku 2.5 popisuje pokus o vstup zaměstnance do prostor s omezeným přístupem. Dveře do prostoru jsou chráněné biometrickým systémem. Pokud chce zaměstnanec do takového prostoru vstoupit, musí biometrickému systému poskytnout biometrický vzorek, na základě kterého systém vyhodnotí, zda je zaměstnanec oprávněn ke vstupu či nikoliv. V případě nenalezení identity zaměstnance je prověřovaná osoba vyzvána k novému snímání biometrického vzorku. Pokud je identita osoby nalezena, dveře se odemknou a zaměstnanec může vstoupit. Výhodou je, že vybrané biometrické metody z kapitoly 2.1.4 jsou vhodné i pro identifikaci (ne pouze pro verifikaci), takže si zaměstnanec nemusí pamatovat žádná hesla a nemusí při sobě nosit čipovou kartu.

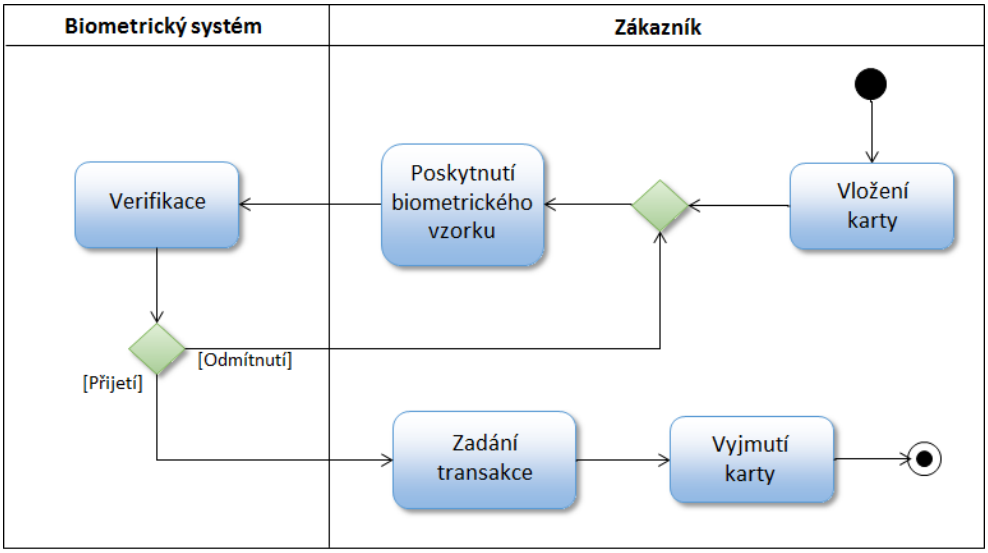
V případě propojení biometrického systému s počítačem (diagram na obrázku 2.6) zaměstnanec poskytne biometrický vzorek a pokud je pomocí vzorku identita osoby nalezena, pak je zaměstnanec úspěšně přihlášen a může s počítačem pracovat. V případě nenalezení identity zaměstnance je prověřovaná osoba vyzvána k novému snímání biometrického vzorku. Po skončení práce zaměstnanec počítač uzamkne nebo vypne. Výhodou je opět skutečnost, že si zaměstnanec nemusí pamatovat žádná hesla a nemusí při sobě nosit čipovou kartu.



Obrázek 2.5: *Diagram aktivit pokusu zaměstnance o vstup do prostor s omezeným přístupem ve finančních institucích.*



Obrázek 2.6: *Diagram aktivit přihlašování zaměstnance do počítače ve finančních institucích.*



Obrázek 2.7: *Diagram aktivit použití bankomatu s biometrickým systémem.*

Poslední případ užití se týká zabezpečení při využívání bankomatu zákazníkem a tento proces znázorňuje diagram na obrázku 2.7. Po vložení karty do bankomatu zákazník poskytne biometrický vzorek biometrickému systému integrovanému do bankomatu. V případě vyvrácení identity je zákazník nucen k novému snímání. Při potvrzení identity může zákazník zadávat transakce a po skončení vyjme kartu z bankomatu. Jelikož je zákazníků mnoho a porovnání jedné šablony s obrovským množstvím šablon v databázi by bylo velmi pomalé a neefektivní, je vhodnější použít porovnání „1:1“, tedy verifikaci.

V následující kapitole jsou vybrané biometrické metody (tvář - 3D, oční duhovka a sítnice, otisky prstů) podrobněji zhodnoceny podle kritérií hodnocení definovaných v teoretické části této práce.

2.1.6 Analýza vybraných metod z hlediska kritérií hodnocení

Kritéria hodnocení v této kapitole popisují biometrické metody obecně. Kritéria, která jsou závislá na konkrétním zařízení nebo matematickém algoritmu nejsou blíže popsána.

2.1.6.1 Otisk prstu

- **Operační kritéria**
  - *Jedinečnost* - vysoká (na malém kousku kůže jsou k dispozici veškeré charakteristiky potřebné pro jednoznačnou identifikaci/verifikaci)

- *Neměnnost* - vysoká (papilární linie zůstávají po celý život neměnné)
- *Měřitelnost* - vysoká (papilární linie lze velmi dobře symbolicky vyjádřit a při strojovém zpracování je navíc zvýrazněna kresba otisku a odstraněny nežádoucí šumy)
- *Uchovatelnost* - vysoká (velikost naměřených charakteristik je velmi nízká, takže je lze dobře uchovávat bez ztráty na kvalitě)
- *Spolehlivost* - střední (typy senzorů, které jsou citlivé na špínu, poranění kůže, vlhkost či prach nebo levné zařízení jsou méně spolehlivé)
- *Exkluzivita* - vysoká (není potřeba další podpůrné identifikace - např. čipová karta, PIN apod.)
- *Praktičnost* - vysoká (proces identifikace/verifikace je rychlý a vyžaduje minimum tréninku uživatele)
- *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
- *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)

- **Technická kritéria**
  - *Chybovost* - střední (některé typy senzorů zejména u levnějších zařízení vykazují vyšší chybovost)
  - *Odolnost* - střední (některé typy senzorů lze oklamat falzifikátem)
  - *Velikost šablony* - malá (řádově stovky bytů)
  - *Rychlost* - vysoká (celý proces identifikace/verifikace je téměř okamžitý)
  - *Nezávislost na vnějším prostředí* - střední (některé senzory jsou citlivé na negativní vlivy jako je vlhkost, prach a špína)

- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 10 000,- Kč (zařízení bez SW); licence k SW je většinou k zařízení dodávána zdarma
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.1.6.2 Tvář 3D

- **Operační kritéria**

- *Jedinečnost* - vysoká (geometrie a rozměry tváře jsou pro každého člověka unikátní)
- *Neměnnost* - střední (tvář se může v průběhu života měnit - věk, úrazy, nemoci apod.)
- *Měřitelnost* - vysoká (přesné rozměry tváře lze 3D technologií dobře geometricky vyjádřit)
- *Uchovatelnost* - vysoká (velikost naměřených charakteristik je větší, ale ne natolik, aby při archivaci musela být použita ztrátová komprese)
- *Spolehlivost* - vysoká (mnohem méně náchylná na pozici tváře a její deformace a měnící se osvětlení než 2D technologie snímání tváře)
- *Exkluzivita* - vysoká (není potřeba další podpůrné identifikace - např. čipová karta, PIN apod.)
- *Praktičnost* - střední (sice není potřeba školit uživatele, ale proces identifikace/verifikace je pomalejší)
- *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
- *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)

- **Technická kritéria**
  - *Chybovost* - nízká (hodnoty jevů FAR a FRR jsou nižší než u 2D technologie snímání tváře)
  - *Odolnost* - vysoká (nelze oklamat fotografií ani maskou)
  - *Velikost šablony* - střední (několik kilobytů)
  - *Rychlost* - střední (pomalejší kvůli vyšší výpočetní složitosti při zpracování 3D dat)
  - *Nezávislost na vnějším prostředí* - vysoká (snímání není ovlivňováno nežádoucími vlivy okolí)

- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 100 000,- Kč (zařízení bez SW); cena SW závisí na počtu registrovaných uživatelů a licence se prodávají jednorázově (zhruba od 10 000,- Kč pro několik stovek uživatelů k registraci)
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.1.6.3 Oční duhovka a sítnice

- **Operační kritéria**
  - *Jedinečnost* - vysoká (struktura duhovky i síť cév za sítnicí je pro každého člověka unikátní)
  - *Neměnnost* - vysoká (charakteristické rysy duhovky i sítnice jsou po celý život neměnné)
  - *Měřitelnost* - vysoká (duhovku i sítnici oka lze velmi dobře změřit a symbolicky vyjádřit)
  - *Uchovatelnost* - vysoká (velikost naměřených charakteristik duhovky a sítnice není příliš vysoká, takže jsou dobře uchovatelné bez ztráty na kvalitě)
  - *Spolehlivost* - vysoká (celý proces identifikace neovlivňují nežádoucí vlivy a je kdykoliv zopakovatelný se stejnými výsledky)
  - *Exkluzivita* - vysoká (není potřeba další podpůrné identifikace - např. čipová karta, PIN apod.)
  - *Praktičnost* - střední (proces identifikace není tak rychlý a školení uživatelů je většinou potřeba)
  - *Přijatelnost* - nízká (zejména snímání sítnice je velmi invazivní a většina lidí má strach z poškození oka)
  - *Přívětivost* - nízká (může vyvolávat nepříjemné pocity, nutno sejmout brýle nebo kontaktní čočky)
- **Technická kritéria**
  - *Chybovost* - nízká (hodnoty FAR a FRR jsou velmi nízké)
  - *Odolnost* - vysoká (metody poskytují velmi vysokou úroveň bezpečnosti a vytvořit falzifikát je nemožné)
  - *Velikost šablony* - střední (několik kilobytů)
  - *Rychlost* - střední (proces verifikace/identifikace je zejména u sítnice delší)
  - *Nezávislost na vnějším prostředí* - vysoká (proces snímání není ovlivněn vnějším prostředí)
- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 70 000,- Kč (zařízení bez SW); cena SW závisí na počtu registrovaných uživatelů a licence se prodávají jednorázově (zhruba od 10 000,- Kč pro několik stovek uživatelů k registraci)
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

Tabulka 2.1: *Porovnání vybraných biometrických metod podle operačních a technických kritérií hodnocení.*

Kritéria hodnocení	Otisk prstu	Tvář 3D	Oční duhovka/sítnice
Jedinečnost	vysoká	vysoká	vysoká
Neměnnost	vysoká	střední	vysoká
Měřitelnost	vysoká	vysoká	vysoká
Uchovatelnost	vysoká	vysoká	vysoká
Spolehlivost	střední	vysoká	vysoká
Exkluzivita	vysoká	vysoká	vysoká
Praktičnost	vysoká	střední	střední
Přijatelnost	vysoká	vysoká	nízká
Přívětivost	vysoká	vysoká	nízká
Chybovost	střední	nízká	nízká
Odolnost	střední	vysoká	vysoká
Velikost šablony	nízká	střední	střední
Rychlost	vysoká	střední	střední
Nezávislost na vnějším prostředí	střední	vysoká	vysoká

2.1.7 Závěrečné zhodnocení a doporučení

V tabulce 2.1 jsou shrnuta operační a technická kritéria hodnocení biometrických metod vybraných pro nasazení ve finančních institucích.

V tabulce 2.2 jsou shrnuty výhody a nevýhody biometrických metod vybraných pro nasazení ve finančních institucích.

V tabulce 2.3 jsou porovnány cenové relace pouze jednorázových nákladů vybraných biometrických technologií pro nasazení ve finančních institucích. Uvedené částky jsou orientační a mění se v závislosti na výrobci a kvalitě zařízení. Na trhu jsou dostupné zařízení i za nižší částky, ale nejsou tak spolehlivé. Uvedené ceny platí pro profesionální zařízení. Pořizovací cena licencí je závislá na počtu osob, které chceme do biometrického systému zaregistrovat. Suma za licence u vybraných systémů většinou startuje zhruba na deseti až dvaceti tisících za několik stovek registrovaných uživatelů (kromě technologie otisku prstu, kde je většinou SW dodáván k zařízení zdarma). Dlouhodobé náklady jsou velmi nízké, tudíž je zanedbávám.

Doporučení. Všechny tři vybrané biometrické metody poskytují vysokou úroveň bezpečnosti, tudíž jsou všechny vhodné pro nasazení ve finančních institucích. Výběr dané biometrické technologie záleží na preferencích jednotlivých finančních institucí a konkrétním případě použití.

Z hlediska bezpečnosti je maximálně spolehlivá technologie snímání oční

Tabulka 2.2: *Výhody a nevýhody vybraných biometrických metod.*

Biometrická metoda	**Výhody**	**Nevýhody**
Otisky prstů	– vysoký podíl trhu (velký výběr zařízení) – rychlost – časová neměnnost – malé rozměry zařízení – příznivá cena	– vyšší chybovost u levnějších zařízení – některé typy snímačů nemusí rozpoznat falzifikát – některé typy snímačů může negativně ovlivnit vnější prostředí, poranění, špinavé ruce apod.
Tvář 3D	– nezávislost na pozici tváře, make-upu, mimice ani osvětlení – vysoká uživatelská přijatelnost/přívětivost	– časová nestálost tváře – vysoká cena – nižší rychlost
Oční duhovka a sítnice	– maximální spolehlivost – časová neměnnost – nemožné vytvořit falzifikát – bezdotykové snímání	– nízká uživatelská přijatelnost/přívětivost – vysoká cena

Tabulka 2.3: *Porovnání cen v českých korunách vybraných biometrických metod.*

	Otisk prstu	**Tvář 3D**	**Oční duhovka/sítnice**
Pořizovací cena zařízení	od 10 000	od 100 000	od 70 000
Pořizovací cena SW (licence)	0	od 10 000	od 10 000
Celkem	**od 10 000**	**od 110 000**	**od 80 000**

sítnice, ale je velmi invazivní a uživatelsky nepřívětivá. Ovšem tato nevýhoda je v případě potřeby vysoké úrovně bezpečnosti často přehlížena nebo je místo snímání sítnice využito snímání duhovky, které je také velmi spolehlivé a pro člověka není tak nepříjemné. Technologie snímání oční duhovky nebo sítnice se hodí zejména pro zabezpečení vstupů do prostor s přísně omezeným přístupem jako jsou např. trezory.

3D technologie snímání tváře je také poměrně spolehlivá a navíc i uživatelsky velmi přívětivá a přijatelná. Stejně jako snímání oční duhovky a sítnice se hodí pro ochranu různých prostor a objektů.

Otisky prstů jsou v případě použití kvalitnějších zařízení a vhodných senzorů také velmi spolehlivá biometrická technologie. Výhodou je její obrovská rozšířenost na trhu s biometrickými zařízeními. Díky tomu je výběr opravdu velký a rozmanitý. Pro případy užití popsané v kapitole 2.1.2 se otisky prstů nejvíce hodí k spojení s počítači, ke kterým se přihlašují zaměstnanci finančních institucí a pro integraci do bankomatů jako efektivní verifikační prostředek zákazníků bank.

Přínos. Biometrické technologie by ve finančních institucích neměly kvůli nutnosti vysoké úrovně zabezpečení chybět. Nejdůležitějším přínosem je získání nových zákazníků, díky větší důvěře a pocitu, že jsou jejich finance v dobrých rukách. Dalším přínosem je, že díky vyššímu zabezpečení finanční instituce budou schopny lépe předcházet interním i externím hrozbám.

2.2 Typový podnik č. 2 - Výrobní závody

U většiny výrobních závodů není nutná tak vysoká úroveň zabezpečení jako u finančních institucí, vládních nebo vojenských sektorů, ale biometrické systémy jsou zde využity spíše pro zefektivnění business procesů firmy. U větších podniků s velmi vysokým počtem zaměstnanců se docházka a prostory s omezeným přístupem jen těžko hlídají (při tak velkém počtu lidí si nikdo nemusí všimnout neoprávněného vstupu do určitých prostor nebo případů, kdy zaměstnanec odejde domů dříve a požádá kolegu, aby za něj později zaznamenal odchod - to by se u docházkového systému, který vyžaduje biometrickou verifikaci, stát nemohlo). Z těchto důvodů se biometrické technologie ve výrobních závodech nasazují nejčastěji pro kontrolu docházky nebo regulaci vstupů osob do určitých prostor.

2.2.1 IS/ICT infrastruktura

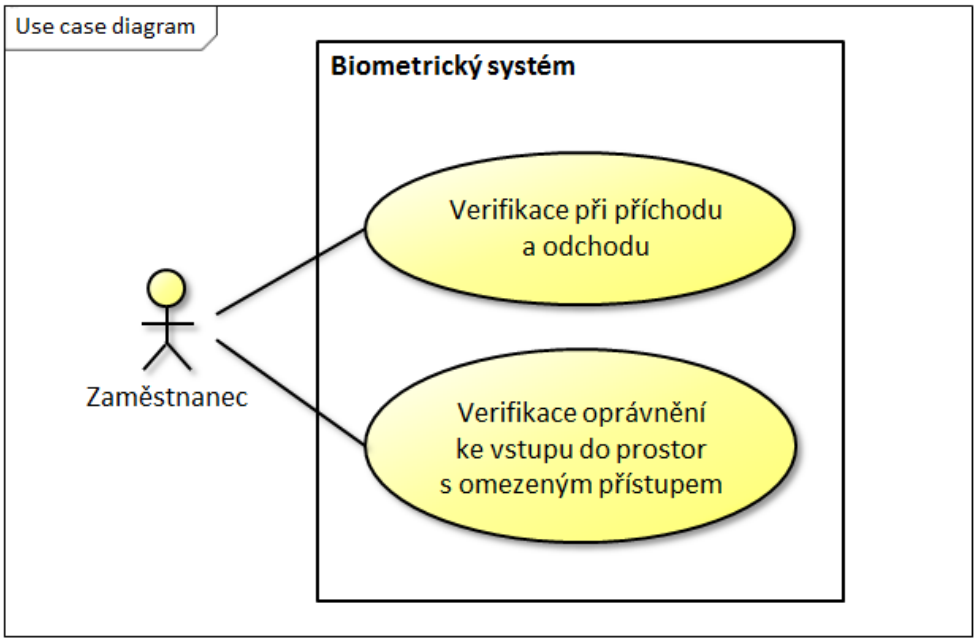
Jeden z hlavních a základních informačních systémů, který výrobní závody využívají je systém evidence docházky zaměstnanců. V tomto systému jsou uvedeny veškeré časy příchodů a odchodů všech zaměstnanců, jejich pracovní výkony a efektivnost a podklady pro udělení finančního ohodnocení a případných bonusů. Dalším systémem ve výrobních závodech jsou většinou různé přístupové systémy pro odemykání dveří do prostor s omezeným přístupem. V ideálním případě mají podniky centrální server a veškerá zařízení a informační systémy jsou k tomuto serveru připojeny a vzájemně komunikují a uživatelé se autentizují pomocí čipových karet nebo PIN kódů či hesel. Veškerá zařízení, systémy a server jsou připojeny do privátní sítě pomocí kabelů nebo bezdrátově. Rozsáhlost této privátní sítě se odvíjí od velikosti podniku a síť dále může zahrnovat různé propojovací síťové prvky (router, switch apod.) a bezpečnostní prvky (firewall). V takovém případě lze snadno biometrickým systémem nahradit nebo rozšířit tu část infrastruktury, která je zodpovědná za verifikaci osob. Biometrický systém by komunikoval s dosavadním informačním systémem.

2.2.2 Případy užití biometrického systému

Biometrické systémy naleznou ve výrobních závodech využití zejména jako verifikační nástroj pro evidenci příchodů a odchodů zaměstnanců a pro regulaci vstupů osob do prostor s omezeným přístupem. Tyto dvě možnosti využití biometrického systému znázorňuje diagram případů užití na obrázku 2.8.

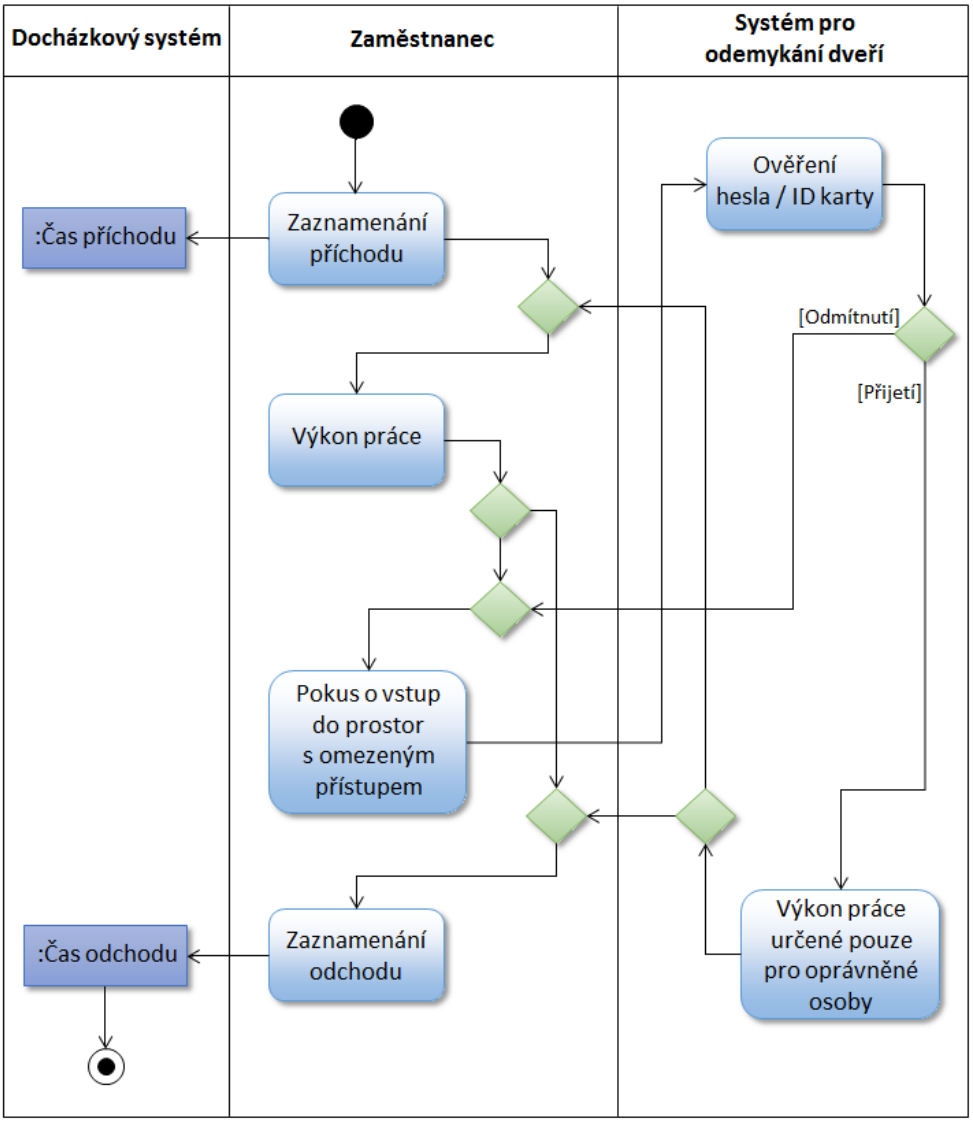
2.2.3 Procesní analýza - situace bez biometrického systému

V dnešní době už snad ve všech výrobních závodech existuje nějaký elektronický docházkový systém, který zaznamenává příchody a odchody zaměstnanců a nějaký systém pro odemykání dveří do prostor s omezeným přístupem.



Obrázek 2.8: *Diagram případů užití biometrického systému ve výrobních závodech.*

Na obrázku 2.9 je pomocí diagramu aktivit znázorněn běžný pracovní den zaměstnance ve výrobním závodu. Při příchodu do práce zaměstnanec přiloží svou identifikační čipovou kartu (verifikace založená na vlastnictví) k elektronickému zařízení pro kontrolu docházky nebo zadá svůj PIN (verifikace založená na znalostech). Docházkový systém uloží ke konkrétnímu identifikačnímu číslu zaměstnance čas příchodu a zaměstnanec pokračuje na pracoviště. Z diagramu je vidět, že zaměstnanec může navštěvovat prostory s omezeným přístupem v případě, že má oprávnění (přiloží čipovou kartu nebo zadá heslo). Po návratu z těchto prostor může zaměstnanec buď dál vykonávat běžnou práci, nebo skončila směna a chce jít domů. Zaměstnanec tedy znovu přiloží identifikační kartu k zařízení pro kontrolu docházky a docházkový systém uloží čas odchodu k identifikačnímu číslu zaměstnance. Nevýhodou absence biometrického zařízení je, že při velkém počtu zaměstnanců se mohou vyskytovat nesrovnalosti v datech docházkového systému (např. zaměstnanec zapomene zaznamenat příchod/odchod, zaměstnanec sdělí svůj pin, nebo půjčí svou identifikační kartu kolegovi, kterého požádá o zaznamenání jiného času příchodu/odchodu). Další nevýhodou je, že zaměstnanci mohou vstupovat do prostor, ve kterých nejsou oprávněni být, pokud zjistí heslo nebo najdou/odcizí čipovou kartu patřící oprávněné osobě. Všechny tyto negativa umí biometrický systém vyřešit.



Obrázek 2.9: *Diagram aktivit interakce zaměstnance s obyčejným docházkovým systémem a systémem pro ověření oprávnění ke vstupu do určitých prostor ve výrobních závodech.*

2.2.4 Výběr vhodných biometrických metod pro nasazení

✘ **Otisk prstu.** Biometrická metoda otisku prstu pro docházkový systém i kontrolu oprávnění ke vstupu do určitých prostor obecně vhodná je. Ale jelikož ve výrobních závodech může dojít ke znečištění rukou, s čímž můžou mít některé typy snímačů otisků prstů problém, je tato biometrická metoda nedostačující.

✘ **Hlas.** Výrobní závody většinou zaměstnávají velký počet zaměstnanců, který se zpravidla často mění. Biometrická metoda založená na rozpoznání hlasu není vhodná do prostor, ve kterých se pohybuje velké množství lidí, jelikož pro pořízení hlasového signálu je důležité tiché okolní prostředí. Navíc tato technologie vyžaduje zdlouhavou a opakovanou registraci nových uživatelů a to by při častějších změnách v řadách zaměstnanců bylo obtížné.

✔ **Tvář.** Verifikace pomocí 3D technologie rozpoznávání tváře je poměrně pomalá, proto se nehodí k ověření identity při docházce. Ovšem 2D technologie poskytuje velmi rychlou verifikaci a výhodou je i malá velikost referenční šablony. Díky tomu je vhodná jak pro kontrolu docházky u výrobních závodů s velkým počtem zaměstnanců a hodí se i jako verifikační prostředek pro vstup do určitých prostor.

✘ **Oční duhovka a sítnice.** Technologie verifikace/identifikace podle oční duhovky nebo sítnice má spoustu výhod, které by se daly využít pro účely docházkového systému i povolení vstupu do prostor. Ovšem samotné snímání není pro uživatele příliš příjemné, natož kdyby ho museli podstupovat několikrát denně. Navíc se jedná o drahou technologii s velmi vysokou úrovní zabezpečení a to je pro účely výrobních závodů zbytečně přehnané.

✔ **Geometrie ruky.** Biometrická metoda geometrie ruky poskytuje rychlou verifikaci, je odolná vůči špíně i drobným povrchovým poraněním a velikost referenční šablony je velmi malá (možnost uchovávat obrovské množství šablon v jediném zařízení). Z těchto důvodů je vhodnou technologií pro biometrický systém výrobních závodů pro kontrolu docházky i jako verifikační prostředek k přístupu do různých prostor.

✔ **Krevní řečiště ruky.** Stejně jako verifikace pomocí geometrie ruky je technologie krevního řečiště ruky vhodným kandidátem pro nasazení ve výrobních závodech. Tato technologie je rychlá, odolná vůči špíně a drobným povrchovým poraněním a navíc díky bezdotykovému snímání je hygienická a uživatelsky vysoce přijatelná/přívětivá.

✘ **Dynamika psaní na klávesnici.** Tato biometrická metoda nabízí čistě SW řešení a nachází uplatnění zejména ve spojení s počítači, proto není vhodná k nasazení jako docházkový biometrický systém nebo k ověření identity pro vstup do určitých prostor.

2.2.5 Procesní analýza - situace po nasazení biometrického systému

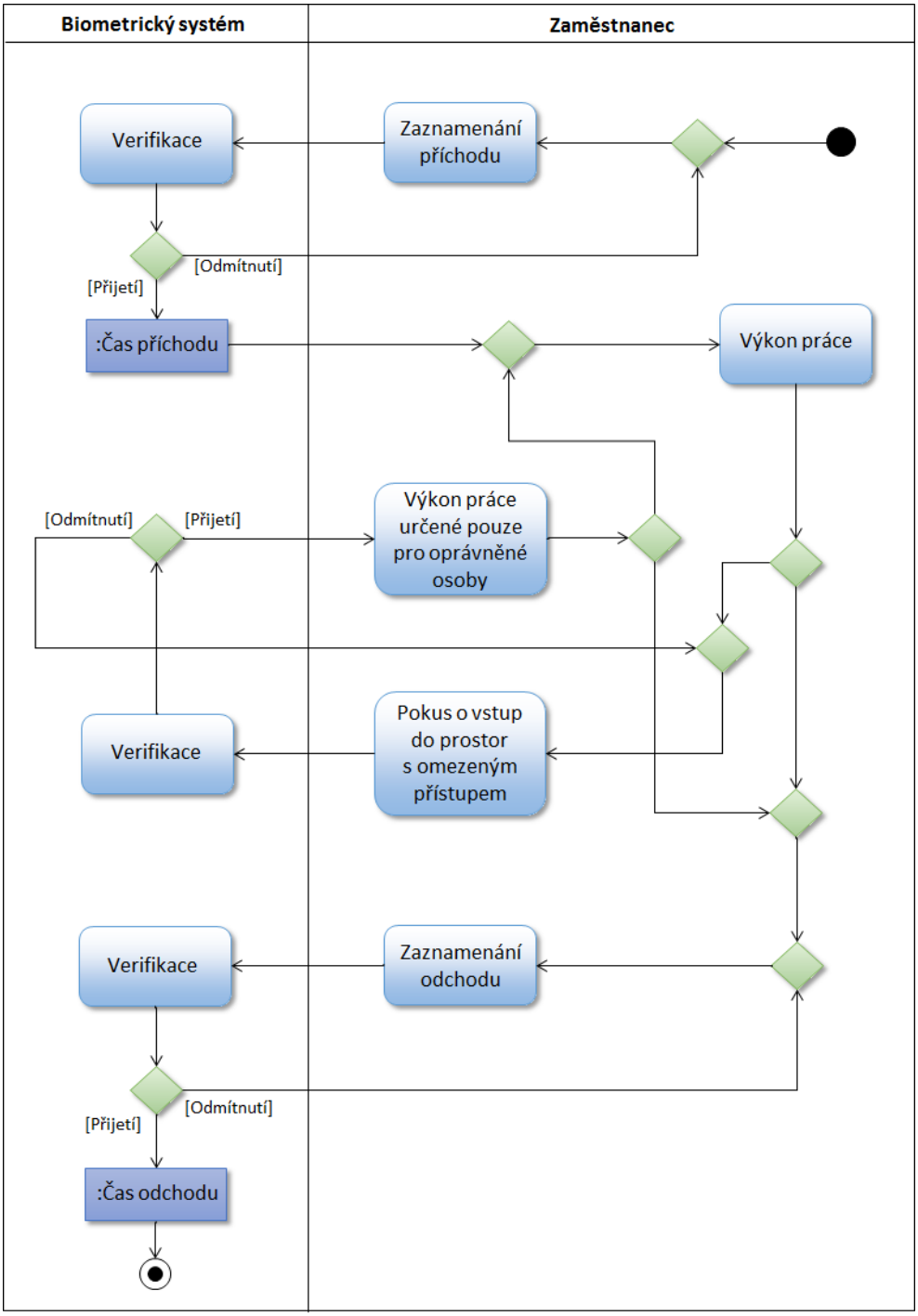
Vybrané biometrické metody jsou vhodnější k verifikaci než k identifikaci, proto je podpůrná identifikace pomocí hesla nebo ID karty zachována.

Celý proces interakce zaměstnance s biometrickým systémem (obrázek 2.10) začíná ihned po příchodu zaměstnance do práce, kdy zaměstnanec přiloží svou identifikační čipovou kartu k biometrickému zařízení nebo zadá svůj PIN a poskytne biometrickému systému svůj biometrický vzorek. Biometrický systém pomocí čipové karty nebo zadaného PIN vyhledá v databázi konkrétní referenční šablonu asociovanou právě s daným pomocným identifikátorem (čipová karta, PIN). Na základě porovnání sejmutého vzorku a referenční šablony rozhodne o výsledku verifikace, tedy potvrdí nebo vyvrátí identitu zaměstnance. V případě neúspěšné verifikace není zaměstnanec puštěn přes turniket a je vyzván k novému snímání. Pokud je identita potvrzena, do systému je uložen čas příchodu a zaměstnanec pokračuje na pracoviště. V případě, že zaměstnanec při výkonu práce potřebuje navštívit prostor s omezeným přístupem (např. sklad materiálu), bude muset prokázat svou identitu a oprávnění k přístupu (proces verifikace je stejný jako u zaznamenání příchodu). Stejně tak při odchodu domů zaměstnanec prokazuje svou identitu a pokud je verifikace úspěšná, systém zaznamená čas odchodu, pokud není úspěšná, zaměstnanci není dovoleno projít turniketem a musí znovu poskytnout biometrický vzorek.

V následující kapitole jsou vybrané biometrické metody (tvář - 2D, geometrie ruky a krevní řečiště ruky) podrobněji zhodnoceny podle kritérií hodnocení definovaných v teoretické části této práce.

2.2.6 Analýza vybraných metod z hlediska kritérií hodnocení

Kritéria hodnocení v této kapitole popisují biometrické metody obecně. Kritéria, která jsou závislá na konkrétním zařízení nebo matematickém algoritmu nejsou blíže popsána. Např. jsou vynechána kritéria výrobní, u kterých záleží na konkrétním typu biometrického zařízení a výrobci. Stejně tak nejsou uvedena kritéria matematická, algoritmická a bezpečnostní, jelikož např. pro hledání významných bodů v tváři se využívá velké množství různých metod a záleží na konkrétních algoritmech, které jsou implementovány v reálných zařízeních.



Obrázek 2.10: *Diagram aktivit interakce zaměstnance s biometrickým systémem ve výrobních závodech.*

2.2.6.1 Tvář - 2D

- **Operační kritéria**
  - *Jedinečnost* - střední (lidská tvář obecně unikátní samozřejmě je, ale 2D technologie rozpoznávání tváře není tak detailní a komplexní, aby dokázala identifikovat tvář na základě všech biologických rysů - používá omezené množství významných bodů tváře; na rozdíl např. od otisku prstu, kde na malém kousku kůže jsou k dispozici veškeré charakteristiky potřebné pro jednoznačnou identifikaci)
  - *Neměnnost* - střední (tvář se může v průběhu života měnit - věk, hmotnost, úrazy, nemoci apod.)
  - *Měřitelnost* - střední (charakteristiky tváře nejsou dobře měřitelné, pokud prověřovaná osoba nemá hlavu ve správné pozici a důležitou roli hrají i správnost algoritmu pro hledání významných bodů tváře a kvalita nasnímaného obrazu)
  - *Uchovatelnost* - vysoká (velikost naměřených charakteristik je velmi nízká, takže jsou dobře uchovatelné bez ztráty na kvalitě)
  - *Spolehlivost* - střední (změna osvětlení, výrazy obličeje, make-up nebo pozice hlavy může zkreslit výsledky měření a vyhodnocování biometrických charakteristik; další problém při hledání antropologicky významných bodů obličeje přestavuje nižší kvalita nasnímaného obrazu)
  - *Exkluzivita* - vysoká (není potřeba další podpůrné identifikace - např. čipová karta, PIN apod.)
  - *Praktičnost* - střední (proces identifikace/verifikace rychlý, ale vyžaduje trénink uživatele)
  - *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
  - *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)
- **Technická kritéria**
  - *Chybovost* - střední (vyšší pravděpodobnost chybného odmítnutí)
  - *Odolnost* - nízká (zařízení lze oklamat např. fotografií)
  - *Velikost šablony* - malá (řádově stovky bytů)
  - *Rychlost* - vysoká (celý proces identifikace/verifikace je téměř okamžitý)
  - *Nezávislost na vnějším prostředí* - nízká (citlivost na měnící se osvětlení)

- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 20 000,- Kč (zařízení bez SW); licence k SW je většinou k zařízení dodávána zdarma
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.2.6.2 Geometrie ruky

- **Operační kritéria**
  - *Jedinečnost* - střední (není tak unikátní jako např. otisk prstu)
  - *Neměnnost* - střední (geometrie ruky se může v průběhu života měnit - úrazy, nemoci apod.)
  - *Měřitelnost* - vysoká (přesné rozměry ruky lze velmi dobře geometricky vyjádřit)
  - *Uchovatelnost* - vysoká (velikost referenční šablony je nejmenší ze všech biometrických metod)
  - *Spolehlivost* - střední (při nesprávném umístění ruky na desku snímače mohou být naměřené hodnoty zkreslené)
  - *Exkluzivita* - střední (metoda je pouze k verifikaci, tedy je nutné použít další podpůrné identifikace - např. čipová karta, PIN apod.)
  - *Praktičnost* - střední (proces verifikace rychlý, ale je potřeba vyškolit uživatele - ruka se musí na snímací desku položit přesně na požadované místo)
  - *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
  - *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)
- **Technická kritéria**
  - *Chybovost* - střední (hodnoty FAR a FRR se pohybují kolem 4%)
  - *Odolnost* - střední (zařízení, která netestují živost osoby lze oklamat 3D modelem ruky)
  - *Velikost šablony* - malá (nejmenší ze všech biometrických metod - přibližně 9 bytů)
  - *Rychlost* - vysoká (celý proces verifikace trvá přibližně jednu sekundu)
  - *Nezávislost na vnějším prostředí* - vysoká (snímání není ovlivňováno vlivy okolí, ani znečištěním rukou či povrchovým poraněním)

- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 40 000,- Kč (zařízení bez SW); cena SW závisí na počtu registrovaných uživatelů a licence se prodávají jednorázově (zhruba od 10 000,- Kč pro několik stovek uživatelů k registraci)
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.2.6.3 Krevní řečiště ruky

- **Operační kritéria**
  - *Jedinečnost* - vysoká (síť cév i v menší části ruky, např. v prstu, je pro každého člověka unikátní)
  - *Neměnnost* - vysoká (v průběhu života se síť cév mění naprosto minimálně)
  - *Měřitelnost* - vysoká (krevní řečiště je dobře měřitelné pomocí infračervených paprsků)
  - *Uchovatelnost* - vysoká (velikost naměřených charakteristik sítě cév není příliš vysoká, takže jsou dobře uchovatelné bez ztráty na kvalitě)
  - *Spolehlivost* - vysoká (na celý proces verifikace nemají vliv negativní faktory a je kdykoliv zopakovatelný se stejnými výsledky)
  - *Exkluzivita* - střední (metoda je pouze k verifikaci, tedy je nutné použít další podpůrné identifikace - např. čipová karta, PIN apod.)
  - *Praktičnost* - vysoká (kontakt s uživatelem je minimální, proces verifikace rychlý a vyžaduje minimum tréninku uživatele)
  - *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
  - *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)
- **Technická kritéria**
  - *Chybovost* - nízká (hodnoty FAR a FRR jsou velmi nízké)
  - *Odolnost* - vysoká (při snímání se kontroluje, zda ruka patří živé osobě a vytvořit falzifikát je tedy nemožné)
  - *Velikost šablony* - střední (několik kilobytů)
  - *Rychlost* - vysoká (celý proces verifikace je téměř okamžitý)

Tabulka 2.4: *Porovnání vybraných biometrických metod podle operačních a technických kritérií hodnocení.*

Kritéria hodnocení	Tvář 2D	Geometrie ruky	Krevní řečiště ruky
Jedinečnost	střední	střední	vysoká
Neměnnost	střední	střední	vysoká
Měřitelnost	střední	vysoká	vysoká
Uchovatelnost	vysoká	vysoká	vysoká
Spolehlivost	střední	střední	vysoká
Exkluzivita	vysoká	střední	střední
Praktičnost	střední	střední	vysoká
Přijatelnost	vysoká	vysoká	vysoká
Přívětivost	vysoká	vysoká	vysoká
Chybovost	střední	střední	nízká
Odolnost	nízká	střední	vysoká
Velikost šablony	nízká	nízká	střední
Rychlost	vysoká	vysoká	vysoká
Nezávislost na vnějším prostředí	nízká	vysoká	vysoká

  - *Nezávislost na vnějším prostředí* - vysoká (proces snímání není ovlivněn vnějším prostředí, ani znečištěním rukou či povrchovým poraněním)

- **Finanční kritéria**

  - *Pořizovací cena* - zhruba od 50 000,- Kč (zařízení bez SW); cena SW závisí na počtu registrovaných uživatelů a licence se prodávají jednorázově (zhruba od 10 000,- Kč pro několik stovek uživatelů k registraci)
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.2.7 Závěrečné zhodnocení a doporučení

V tabulce 2.4 jsou shrnuta operační a technická kritéria hodnocení biometrických metod vybraných pro nasazení ve výrobních závodech.

V tabulce 2.5 jsou shrnuty výhody a nevýhody biometrických metod vybraných pro nasazení ve výrobních závodech.

V tabulce 2.6 jsou porovnány cenové relace pouze jednorázových nákladů vybraných biometrických technologií pro nasazení ve výrobních závodech. Uvedené částky jsou pouze orientační a mění se v závislosti na výrobci a

Tabulka 2.5: *Výhody a nevýhody vybraných biometrických metod.*

Biometrická metoda	**Výhody**	**Nevýhody**
Tvář 2D	– rychlost – malá velikost referenční šablony – vysoká uživatelská přijatelnost/přívětivost	– nižší časová neměnnost – závislost na vnějším prostředí – nízká odolnost vůči falzifikátům
Geometrie ruky	– rychlost – odolnost vůči špíně a povrchovým poraněním – malá velikost referenční šablony	– nižší časová neměnnost – menší odolnost vůči falzifikátům – pouze k verifikaci
Krevní řečiště ruky	– rychlost – časová neměnnost – odolnost vůči špíně a povrchovým poraněním – nemožné vytvořit falzifikát – bezdotykové snímání	– pouze k verifikaci

Tabulka 2.6: *Porovnání cen v českých korunách vybraných biometrických metod.*

	Tvář 2D	**Geometrie ruky**	**Krevní řečiště ruky**
Pořizovací cena zařízení	od 20 000	od 40 000	od 50 000
Pořizovací cena SW (licence)	0	od 10 000	od 10 000
Celkem	**od 20 000**	**od 50 000**	**od 60 000**

kvalitě zařízení. Na trhu jsou dostupné zařízení i za nižší částky, ale nejsou tak spolehlivé. Uvedené ceny platí pro profesionální zařízení. Pořizovací cena licencí je závislá na počtu osob, které chceme do biometrického systému zaregistrovat. Suma za licence u biometrických systémů většinou startuje zhruba na deseti až dvaceti tisících za několik stovek registrovaných uživatelů, ale může se vyšplhat až na půl milionu korun v případě velkého počtu uživatelů k registraci (např. 10 000 uživatelů). Dlouhodobé náklady jsou velmi nízké, tudíž je zanedbávám.

Doporučení. Všechny tři vybrané biometrické metody jsou vhodné pro nasazení ve výrobních závodech, jelikož jsou rychlé, disponují malou velikostí referenční šablony a velmi dobrou uživatelskou přijatelností a přívětivostí. Výběr konkrétní biometrické technologie se odvíjí od priorit výrobního závodu.

Nejméně nevýhod s sebou nese technologie snímání krevního řečiště ruky, která je ze všech třech vybraných biometrických metod nejspolehlivější a nejodolnější vůči falzifikátům. Proto je tato biometrická metoda vhodná zejména do výrobních závodů, ve kterých je kladen větší důraz na bezpečnost.

Verifikace založená na geometrii ruky se zase hodí do závodů s obrovským počtem zaměstnanců. Díky velmi malé velikosti referenční šablony totiž šetří náklady na uchovávání biometrických charakteristik.

2D technologie snímání tváře je z těchto tří vybraných biometrických metod nejméně spolehlivá a poměrně snadno oklamatelná například kvalitní fotografií. Ovšem výsledky zhodnocení podle kritérií jsou pro většinu výrobních závodů dostačující a výhodou je poměrně nízká cena této technologie.

Přínos. Biometrické technologie nabízí účinné řešení pro kontrolu docházky a regulaci vstupů do určitých prostor/objektů. Přínosy jsou zejména bezpečnost proti podvodům v docházce zaměstnanců, efektivnější monitorování docházky a lepší přehled o pohybu zaměstnanců na pracovišti.

2.3 Typový podnik č. 3 - Osoby samostatně výdělečně činné

Nejenom rozsáhlé korporace využívají biometrické bezpečnostní systémy, ale i osoby samostatně výdělečně činné, které denně pracují s citlivými údaji, uvítají rozmanité možnosti zabezpečení, jež biometrické technologie nabízejí. Mezi takové osoby patří například účetní a auditoři, kteří disponují účetními výkazy a dalšími citlivými dokumenty, které se týkají různých podniků nebo daňoví poradci a právníci, kteří také pracují s důvěrnými informacemi o svých zákaznících. Potřeba chránit tyto data je jistě žádoucí.

2.3.1 IS/ICT infrastruktura

Většina OSVČ vlastní jeden nebo více počítačů s různými informačními systémy nebo softwarem, který usnadňuje poskytování finančních, účetních a poradenských služeb. Jelikož se jedná pouze o malé množství samostatných počítačů (typicky jeden notebook a/nebo stolní počítač), nedá se hovořit o IS/ICT infrastruktuře jako takové. OSVČ samozřejmě potřebuje počítač připojovat k internetu, je proto nutné použití firewallu a antivirového programu.

2.3.2 Případy užití biometrického systému

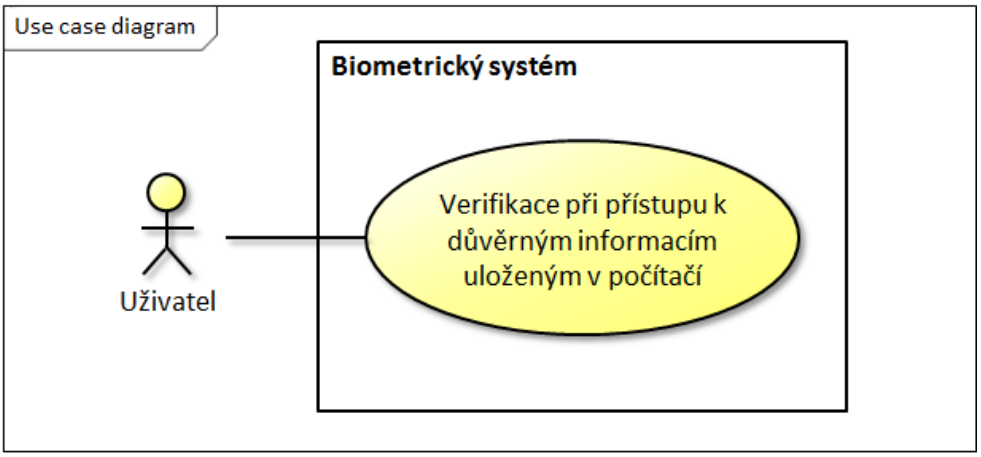
V případě OSVČ, které pracují s důvěrnými informacemi svých zákazníků, jsou biometrické technologie vhodné pro verifikaci uživatele, který chce přistupovat k datům a informacím uložených v počítači. Tuto možnost využití biometrického systému znázorňuje diagram případů užití na obrázku 2.11.

2.3.3 Procesní analýza - situace bez biometrického systému

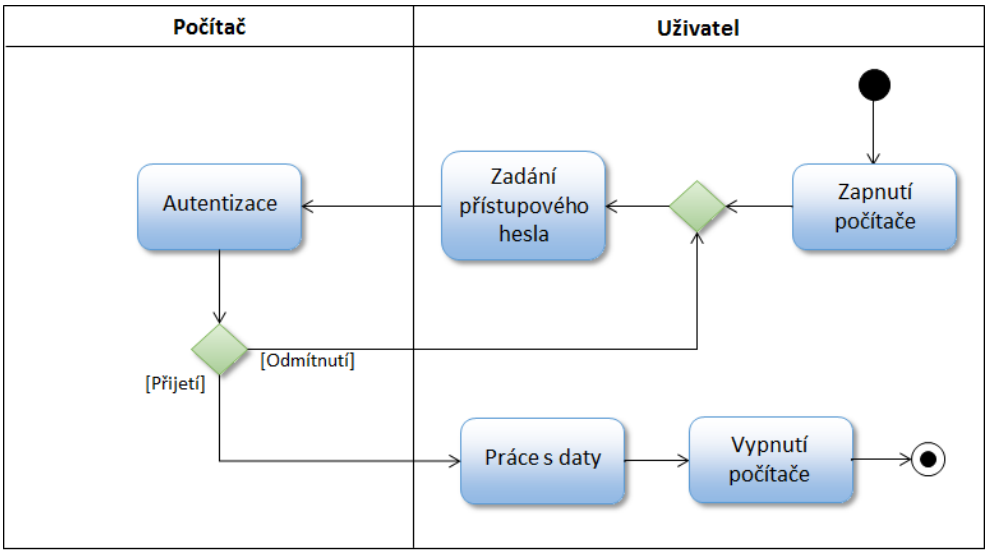
Uživatelé (OSVČ), kteří k ochraně dat ve svém počítači nevyužívají žádnou biometrickou technologii (obrázek 2.12), po zapnutí počítače zadají přístupové heslo (identifikace osoby založená na znalostech), které systém buď přijme, nebo odmítne. Při nesprávné autentizaci je uživatel systémem vyzván k opětovnému zadání hesla. V případě zadání správného hesla se počítač odemkne a uživatel může přistupovat k datům. Po ukončení práce uživatel počítač vypne.

2.3.4 Výběr vhodných biometrických metod pro nasazení

✔ **Otisk prstu.** Biometrická metoda otisku prstu najde uplatnění v nejrůznějších oblastech. Existuje velké množství řešení v podobě integrované čtečky otisku prstu v notebooku nebo počítačové myši.



Obrázek 2.11: *Diagram případů užití biometrického systému osobami samostatně výdělečně činnými.*



Obrázek 2.12: *Diagram aktivit interakce OSVČ s počítačem chráněným pouhým heslem.*

✔ **Hlas.** Jelikož je technologie snadno integrovatelná do počítače a skvěle se hodí k doplnění přístupového hesla, je ideální k ochraně dat uložených v počítači OSVČ.

✘ **Tvář.** 2D technologii je příliš snadné zmást kvalitní fotografií, proto k ochraně důležitých dat vhodná není. 3D technologie rozpoznávání tváře se tak snadno zmást nedá, ale v současné době není k dispozici 3D technologie snímání tváře, kterou by bylo možné integrovat do počítače.

✘ **Oční duhovka a sítnice.** Technologie verifikace/identifikace pomocí oční duhovky nebo sítnice je nákladná a poskytuje velmi vysokou úroveň zabezpečení a to je pro tento typ nasazení zbytečně přehnané.

✘ **Geometrie ruky.** Biometrická metoda geometrie ruky je vhodná pro kontrolu docházky nebo jako verifikační prostředek k přístupu do různých prostor. Biometrické zařízení s touto technologií je ale kvůli větším rozměrům těžko integrovatelné do počítače.

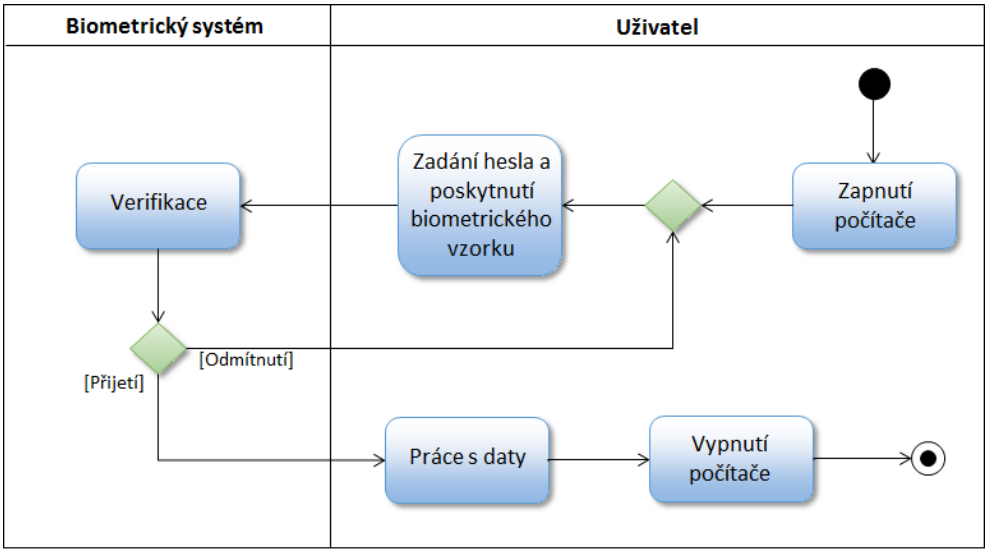
✔ **Krevní řečiště ruky.** Verifikace pomocí krevního řečiště ruky je rychlá, spolehlivá a vhodná pro ochranu citlivých dat a v současné době jsou k dispozici notebooky a počítačové myši s touto technologií.

✔ **Dynamika psaní na klávesnici.** Jelikož tato biometrická metoda představuje čistě SW řešení, které má minimální nároky na HW, je ideální pro propojení s počítačem.

2.3.5 Procesní analýza - situace po nasazení biometrického systému

Při přístupu do počítače chráněného biometrickou technologií (obrázek 2.13) nebo systémem uživatel po zapnutí počítače zadá heslo a je vyzván k poskytnutí biometrických charakteristik ke snímání. Biometrický systém rozhodne o verifikaci, tedy potvrdí nebo vyvrátí identitu uživatele. V případě neúspěšné verifikace musí uživatel znovu poskytnout biometrickou charakteristiku k opakovanému snímání. Pokud je identita potvrzena, počítač se odemkne a uživatel může přistupovat k datům. Po ukončení práce uživatel počítač vypne.

V následující kapitole jsou vybrané biometrické metody (otisk prstu, hlas, krevní řečiště ruky, dynamika psaní na klávesnici) podrobněji zhodnoceny podle kritérií hodnocení definovaných v teoretické části této práce.



Obrázek 2.13: *Diagram aktivit interakce OSVČ s počítačem chráněným biometrickým systémem/technologií.*

2.3.6 Analýza vybraných metod z hlediska kritérií hodnocení

Kritéria hodnocení v této kapitole popisují biometrické metody obecně. Kritéria, která jsou závislá na konkrétním zařízení nebo matematickém algoritmu nejsou blíže popsána.

2.3.6.1 Otisk prstu

Kritéria hodnocení jsou již popsána v kapitole 2.1.6.1 u prvního typového podniku, proto nemá smysl je znovu rozebírat.

2.3.6.2 Hlas

- **Operační kritéria**
  - *Jedinečnost* - střední (každý člověk má unikátní hlas, ale extrahované biometrické markanty hlasu mohou být velmi podobné např. mezi příbuznými osobami)
  - *Neměnnost* - nízká (hlas se může měnit v důsledku zdravotního a emočního stavu uživatele)
  - *Měřitelnost* - vysoká (zvukovou stopu lze velmi dobře měřit a následně symbolicky vyjádřit)
  - *Uchovatelnost* - vysoká (nahrané zvukové záznamy lze dobře uchovávat, aniž by došlo ke ztrátě kvality)

- *Spolehlivost* - nízká (nižší spolehlivost technologie je způsobená zejména podobností hlasu u příbuzných osob a možnými změnami v hlasovém signálu - emoční a zdravotní stav)
- *Exkluzivita* - vysoká (není potřeba další podpůrné identifikace - např. čipová karta, PIN apod.)
- *Praktičnost* - vysoká (proces identifikace/verifikace je rychlý a vyžaduje minimum tréninku uživatele)
- *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
- *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)

- **Technická kritéria**
  - *Chybovost* - střední (vyšší pravděpodobnost chybného odmítnutí)
  - *Odolnost* - vysoká (moderní zařízení umí detekovat přesnou shodu a tudíž je nelze obejít hlasovým záznamem)
  - *Velikost šablony* - střední (několik kilobytů)
  - *Rychlost* - vysoká (celý proces identifikace/verifikace je téměř okamžitý)
  - *Nezávislost na vnějším prostředí* - nízká (citlivost na hluk v okolí)

- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 5 000,- Kč (zařízení bez SW); licence k SW vyjde řádově na několik tisíc korun
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky
  - *Údržba a provoz* - zanedbatelné částky

2.3.6.3 Krevní řečiště ruky

Kritéria hodnocení jsou již popsána v kapitole 2.2.6 u druhého typového podniku, proto nemá smysl je znovu rozebírat. Jediný rozdíl je u finančních kritérií, jelikož senzor pro snímání krevního řečiště lze jednoduše integrovat do počítače a bývá levnější než zařízení se snímačem krevního řečiště pro kontrolu docházky. Většinou je tento senzor připojen k počítači pomocí USB konektoru a stojí řádově tisíce korun nebo se dá zakoupit přímo notebook s integrovanou čtečkou uvnitř (několik desítek korun).

2.3.6.4 Dynamika psaní na klávesnici

- **Operační kritéria**
  - *Jedinečnost* - vysoká (díky vysoké přesnosti měření úhozů je prakticky nemožné najít 2 totožné vzorky)
  - *Neměnnost* - nízká (dynamika psaní se může časem měnit např. kvůli zlepšování se v psaní nebo adaptaci na klávesnici)
  - *Měřitelnost* - vysoká (velmi dobře a jednoduše měřitelné s vysokou přesností)
  - *Uchovatelnost* - vysoká (naměřené charakteristiky lze dobře uchovávat, aniž by došlo ke ztrátě kvality)
  - *Spolehlivost* - nízká (tato metoda není až tak spolehlivá, jelikož dynamiku psaní ovlivňují nejrůznější faktory a je nutné, aby uživatel vždy psal stejně nebo alespoň velmi podobně)
  - *Exkluzivita* - vysoká (dynamika psaní na klávesnici nepotřebuje další podpůrnou identifikační činnost - heslo totiž nemusí být tajné, může se jednat o jakékoliv slovo nebo frázi)
  - *Praktičnost* - vysoká (praktičnost je velmi vysoká, technologie uživatele nijak nezdržuje, nevyžaduje žádné školení a poskytuje kontinuální ověřování identity)
  - *Přijatelnost* - vysoká (nijak nezasahuje do integrity lidského těla, je neinvazivní)
  - *Přívětivost* - vysoká (nevyvolává nepříjemné pocity, nedochází k diskriminaci)
- **Technická kritéria**
  - *Chybovost* - vysoká (obě hodnoty FAR a FRR jsou poměrně vysoké)
  - *Odolnost* - vysoká (je prakticky nemožné napodobit dynamiku psaní na klávesnici jiné osoby)
  - *Velikost šablony* - střední (několik kilobytů)
  - *Rychlost* - vysoká (celý proces verifikace je téměř okamžitý)
  - *Nezávislost na vnějším prostředí* - vysoká (technologii nemůžou ovlivnit žádné rušivé faktory, jako jsou hluk, světlo, teplota, vlhkost, kouř apod.)
- **Finanční kritéria**
  - *Pořizovací cena* - zhruba od 2 000,- Kč za licenci (zkušební verze jsou dostupné zdarma)
  - *Uvedení do provozu (školení, trénink)* - zanedbatelné částky, školení není potřeba
  - *Údržba a provoz* - zanedbatelné částky

Tabulka 2.7: *Porovnání vybraných biometrických metod podle operačních a technických kritérií hodnocení.*

Kritéria hodnocení	**Otisk prstu**	**Hlas**	**Krevní řečiště ruky**	**Dynamika psaní na klávesnici**
Jedinečnost	vysoká	střední	vysoká	vysoká
Neměnnost	vysoká	nízká	vysoká	nízká
Měřitelnost	vysoká	vysoká	vysoká	vysoká
Uchovatelnost	vysoká	vysoká	vysoká	vysoká
Spolehlivost	střední	nízká	vysoká	nízká
Exkluzivita	vysoká	vysoká	střední	vysoká
Praktičnost	vysoká	vysoká	vysoká	vysoká
Přijatelnost	vysoká	vysoká	vysoká	vysoká
Přívětivost	vysoká	vysoká	vysoká	vysoká
Chybovost	střední	střední	nízká	vysoká
Odolnost	střední	vysoká	vysoká	vysoká
Velikost šablony	nízká	střední	střední	střední
Rychlost	vysoká	vysoká	vysoká	vysoká
Nezávislost na vnějším prostředí	střední	nízká	vysoká	vysoká

2.3.7 Závěrečné zhodnocení a doporučení

V tabulce 2.7 jsou shrnuta operační a technická kritéria hodnocení biometrických metod vybraných pro ochranu dat v počítači OSVČ.

V tabulce 2.8 jsou shrnuty výhody a nevýhody biometrických metod vybraných pro ochranu počítačových dat.

V tabulce 2.9 jsou porovnány cenové relace pouze jednorázových nákladů vybraných biometrických technologií pro integraci do počítače OSVČ. Uvedené částky jsou pouze orientační a mění se v závislosti na výrobci a kvalitě zařízení. Na trhu jsou dostupné zařízení i za nižší částky, ale nejsou tak spolehlivé. Uvedené ceny platí pro profesionální zařízení. Pořizovací cena licencí je závislá na počtu osob, které chceme do biometrického systému zaregistrovat. V případě OSVČ většinou postačí jedna licence a suma za ní startuje na několika tisících. Dlouhodobé náklady jsou velmi nízké, v tomto případě spíše nulové.

Doporučení. Všechny čtyři vybrané biometrické metody jsou vhodné pro ochranu dat v počítačích, jelikož jsou rychlé, uživatelsky přijatelné a přívětivé, tudíž vhodné ke každodennímu použití a jsou i cenově příznivé. Při výběru konkrétní biometrické technologie záleží na preferencích uživatele (OSVČ).

Velkou výhodou technologie otisku prstů je její obrovský podíl na trhu.

Tabulka 2.8: *Výhody a nevýhody vybraných biometrických metod.*

Biometrická metoda	**Výhody**	**Nevýhody**
Otisky prstů	– vysoký podíl trhu (velký výběr zařízení) – rychlost – časová neměnnost – malé rozměry zařízení – příznivá cena	– vyšší chybovost u levnějších zařízení – některé typy snímačů nemusí rozpoznat falzifikát – některé typy snímačů může negativně ovlivnit vnější prostředí, poranění, špinavé ruce apod.
Hlas	– vysoká uživatelská přijatelnost/přívětivost – vysoká odolnost vůči falzifikátům – nízká cena zařízení	– zdlouhavá registrace – nízká přesnost – hlasová nestálost ve spojitosti se zdravotním stavem a věkem osoby
Krevní řečiště ruky	– rychlost – časová neměnnost – odolnost vůči špíně a povrchovým poraněním – nemožné vytvořit falzifikát – bezdotykové snímání	– pouze k verifikaci
Dynamika psaní na klávesnici	– unikátnost – nízká cena implementace a nasazení – čistě SW technologie – vysoká uživatelská přijatelnost/přívětivost – kontinuální ověřování identity	– vyšší chybovost – časová nestálost –nižší přesnost

Tabulka 2.9: *Porovnání cen v českých korunách vybraných biometrických metod.*

	Otisk prstu	**Hlas**	**Krevní řečiště ruky**	**Dynamika psaní na klávesnici**
Pořizovací cena zařízení	od 10 000	od 5 000	od 10 000	X
Pořizovací cena SW (licence)	0	od 1 000	od 1 000	od 2 000
Celkem	**od 10 000**	**od 6 000**	**od 11 000**	**od 2 000**

Výběr zařízení s různými typy senzorů pro snímání papilárních linií je rozmanitý a díky tomu lze pořídit přístroj „ušitý na míru“. Od typu senzoru se odvíjí i cena - opto-elektronické jsou nejlevnější a multispektrální nejdražší, ale nejspolehlivější.

Biometrická metoda založená na analýze hlasu není tak spolehlivá a časově stálá a při ověřování identity je nutné tiché prostředí, ale je poměrně dobře odolná vůči falzifikátům v podobě zvukových nahrávek. Ovšem nevýhody této metody jsou značné a ostatní technologie vybrané pro ochranu počítačových dat jsou přece jen vhodnější.

Technologie snímání krevního řečiště ruky má spoustu důležitých výhod - velmi vysokou spolehlivost a odolnost a nízkou chybovost. Také cena zařízení, které lze jednoduše integrovat do jakéhokoliv počítače je velmi příznivá.

Technologie dynamiky psaní na klávesnici je díky nezávislosti na HW ze všech metod nejjednodušší na uvedení do provozu a zkušební verze SW jsou dokonce dostupné zdarma z internetu. Je to velmi odolná a praktická biometrická metoda, která poskytuje mimo verifikace při zapnutí počítače také kontinuální prověřování identity po celou dobu práce s počítačem. Ovšem obtěžující může být častější jev FRR z důvodu proměnlivého stylu psaní (uživatel se musí snažit psát při každé verifikaci stejně nebo alespoň velmi podobně).

Přínos. Ať už se uživatel (OSVČ) rozhodne pro jakoukoliv biometrickou technologii, její přínosy budou významné. V první řadě by uživatel mohl získat nové zákazníky, kteří by ocenili takové zabezpečení a byli by si jisti, že jsou jejich důvěrné informace v bezpečí. Zároveň použití některé biometrické metody může předejít vážným problémům při úniku/zcizení citlivých dat zákazníků.

Závěr

Ve své bakalářské práci jsem popsala běžně používané biometrické metody v praxi a definovala kritéria hodnocení jejich kvality. Na základě toho jsem sestavila doporučení a primární přínos pro každý typový podnik. Všechny popsané biometrické technologie mají své výhody i nevýhody a záleží na konkrétní oblasti využití a prioritách daného podniku. Má práce by měla usnadnit rozhodování reálných podniků, které plánují nasadit nějaký biometrický systém. V práci jsem se snažila popsat stěžejní oblasti, které jsou pro konkrétní podniky nejdůležitější při rozhodování, jaký biometrický systém zvolit pro nasazení. Po přečtení mé bakalářské práce by měl mít čtenář komplexní představu o běžně používaných biometrických technologiích, jejich ceně, výhodách i nevýhodách a přínosu pro firmu.

Literatura

[1] Rak, R.; Matyáš, V.; Říha, Z.; aj.: *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, a.s., první vydání, 2008, ISBN 978-80-247-2365-5.

[2] File:Fingerprint picture.svg. *Wikimedia Commons [online]*, září 2009, [cit. 2017-04-05]. Dostupné z: `https://commons.wikimedia.org/wiki/File:Fingerprint_picture.svg`

[3] Stavba oka. *Ocuvite [online]*, [cit. 2017-03-26]. Dostupné z: `http://www.ocuvite.cz/zdravi-oci-stavba-oka.html`

[4] To enter with the world or sensing technology on a picture of veins of Fujitsu PalmSecure. *Developers Club [online]*, únor 2013, [cit. 2017-04-05]. Dostupné z: `http://developers-club.com/posts/166787/`

[5] Face Recognition. *creativentechno [online]*, únor 2012, [cit. 2017-04-07]. Dostupné z: `https://creativentechno.wordpress.com/2012/02/18/face-recognition/`

[6] Face Recognition Technology Whitepaper. *FingerTec [online]*, 2014, [cit. 2017-04-09]. Dostupné z: `http://www.fingertec.com/companyprofile/development/wp-facerecognition.html`

[7] Biometrics as a Market for Professional Services (Big Data and Security). *LinkedIn [online]*, květen 2015, [cit. 2017-03-26]. Dostupné z: `https://www.linkedin.com/pulse/biometrics-market-professional-services-big-data-security-alan-crean`

[8] Biometric Sample. *Technovelgy.com - where science meets fiction^{TM} [online]*, [cit. 2017-03-15]. Dostupné z: `http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=73`

[9] Template. *Technovelgy.com - where science meets fiction^{TM} [online]*, [cit. 2017-03-15]. Dostupné z: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=90

[10] Biometrie otisku prstu. *Biometric Line [online]*, [cit. 2017-04-03]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

[11] What biometric attributes does a signature have? *Quora [online]*, prosinec 2015, [cit. 2017-04-02]. Dostupné z: https://www.quora.com/What-biometric-attributes-does-a-signature-have

[12] Biometrics. *LinkedIn SlideShare [online]*, září 2012, [cit. 2017-04-03]. Dostupné z: https://www.slideshare.net/pratishsardar/biometric-14819642

[13] Biometrie oka. *Biometric Line [online]*, [cit. 2017-03-26]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

[14] Fujitsu PalmSecure. *FUJITSU [online]*, [cit. 2017-03-26]. Dostupné z: http://www.fujitsu.com/cz/solutions/business-technology/security/product/palmsecure/

[15] Bezkontaktní biometrická identifikace osob pomocí obrazu krevního řečiště – unikátní technologie Fujitsu Palmsecure. *Agora Plus [online]*, březen 2016, [cit. 2017-03-26]. Dostupné z: http://www.agoraplus.cz/zajimavosti/detail/browse/1/article/273/bezkontaktni-biometricka-identifikace-osob-pomoci-obrazu-krevniho-reciste-unikatni-tec.html

[16] Iris recognition Vs. Palm Vein Biometrics – How do they compare? *M2SYS Blog On Biometric Technology [online]*, leden 2016, [cit. 2017-04-03]. Dostupné z: http://www.m2sys.com/blog/scanning-and-efficiency/iris-recognition-vs-palm-vein-biometrics-how-do-they-compare/

[17] SpeechTech Hlasová biometrie. *SpeechTech [online]*, [cit. 2017-04-09]. Dostupné z: http://www.speechtech.cz/cz/produkty/speechtech-hlasova-biometrie

[18] Hlasová biometrie pomáhá klientovi i operátorovi. *SystemOnLine [online]*, březen 2015, [cit. 2017-04-09]. Dostupné z: https://www.systemonline.cz/crm/hlasova-biometrie-pomaha-klientovi-i-operatorovi.htm

[19] Biometrie obličeje. *Biometric Line [online]*, [cit. 2017-04-05]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/

[20] A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal [online]*, srpen 2013, [cit. 2017-04-03]. Dostupné z: https://www.hindawi.com/journals/tswj/2013/408280/

[21] Enterprise Single Sign-On. *Global Tech Consulting Group [online]*, [cit. 2017-04-03]. Dostupné z: http://globaltechconsultants.org/?q=content/enterprise-single-sign

[22] Identity recognition with palm vein feature using local binary pattern rotation Invariant. *IEEE [online]*, září 2016, [cit. 2017-04-03]. Dostupné z: http://ieeexplore.ieee.org/document/7571952/

Příloha **A**

Seznam použitých zkratek

IS/ICT Information Systems / Information and Communication Technologies - souhrnné označení pro informační systémy, informační a komunikační technologie

FRR False Rejection Rate - pravděpodobnost chybného odmítnutí autorizované osoby biometrickým zařízením

FAR False Acceptance Rate - pravděpodobnost chybného přijetí neoprávněné osoby biometrickým zařízením

EER Equal Error Rate - bod, ve kterém se protínají křivky FRR a FAR

CCD Charge-Coupled Device - zařízení s vázanými náboji; elektronická součástka používaná pro snímání obrazové informace

HW Hardware

SW Software

2D Dvoudimenzionální, dvourozměrný

3D Trojdimenzionální, trojrozměrný

PIN Personal Identification Number - osobní identifikační číslo

OSVČ Osoba samostatně výdělečně činná

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `zadani.pdf` ..... zadání práce ve formátu PDF