
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# DYNAMICKÝ BIOMETRICKÝ PODPIS JAKO EFEKTIVNÍ NÁSTROJ PRO VNITROPODNIKOVOU KOMUNIKACI

DYNAMIC BIOMETRIC SIGNATURE AS AN EFFICIENT TOOL FOR INTERNAL CORPORATE COMMUNICATION

DIZERTAČNÍ PRÁCE
DOCTORAL THESIS


AUTOR PRÁCE
AUTHOR

Ing. et Ing. František Hortai

ŠKOLITEL
SUPERVISOR

prof. Ing. Vladimír Smejkal, CSc.



BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání dizertační práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Ing. et Ing. František Hortai** |
| Studijní program: | Ekonomika a management |
| Studijní obor: | Řízení a ekonomika podniku |
| Vedoucí práce: | **prof. Ing. Vladimír Smejkal, CSc.** |
| Akademický rok: | 2018/19 |

## DYNAMICKÝ BIOMETRICKÝ PODPIS JAKO EFEKTIVNÍ NÁSTROJ PRO VNITROPODNIKOVOU KOMUNIKACI

**Charakteristika problematiky úkolu:**

Stanovení cílů disertační práce.
Metodika zpracování disertační práce.
Kritické zhodnocení současného stavu řešené problematiky.
Vlastní výzkum v oblasti biometrických metod pro identifikaci a autentizaci.
Návrhy a doporučení.
Přínosy pro teorii, praxi i pedagogický proces.

**Cíle, kterých má být dosaženo:**

Hlavním cílem disertační práce je podat ucelenou informaci o možnostech identifikace a autentizace pomocí biometrických metod v podnikové praxi elektronické komunikace. V práci má být zkoumána využitelnost biometrických technologií, principy jejich funkčnosti, příklady použití, výhody a nevýhody, které přinášejí v podnicích, resp. i jiných organizacích. Podrobně budou zkoumány dynamické biometrické metody, zejména pak dynamický biometrický podpis, jako přirozený, snadno dostupný, a tedy vhodný nástroj pro efektivní a bezpečnou komunikaci. Problematika technologie dynamického biometrického podpisu a jeho implementace budou zkoumány z komplexního hlediska včetně zohlednění vlastních i cizích provedených experimentů. Závěry práce by měly odpovědět na otázku, zda dynamický biometrický podpis může sloužit jako metoda podporující bezpečnou podnikovou komunikaci a zredukovat autentizační rizika typické pro jednofaktorovou autentizaci a statickou autentizaci s využitím biometrických dat.

**Základní literární prameny:**

Drahanský, M.; Orság, F.; Dvořák, R.; Hájek, J.; Váňa, J.; Herman, D.; Kněžík, J.; Marvan, A.; Lodrová, D.; Doležel, M. (2011). Biometrie. Brno: Computer Press, s.r.o. , p. 294. ISBN: 978-80-254-8979-6

Rak, R., Matyáš, V., Říha, Z. (2008). Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: GRADA. ISBN 978-80-247-2365-5.

Smejkal, V., Kodl, J. (2008). Development trends of electronic authentication. Proceedings of the 42nd Annual Conference IEEE International Carnahan Conference on Security Technology, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1 – 6.

Smejkal, V. Kodl, J. (2011). Strong authentication using dynamic biometric signature. In: Proceedings of 45th Annual 2010 IEEE International Carnahan Conference on Security Technology (ICCST), Barcelona, Spain, October 18-21, p. 340–344, ISBN 978-145-7709-02.

Smejkal, V. Kodl, J., Kodl, J. Jr., (2013). Implementing trustworthy dynamic biometric signature according to the electronic signature regulations. In: Proceedings of 47th International Carnahan Conference on Security Technology, ICCST 2013; Medellin; Colombia, pp. 165–170, ISBN 978-958-8790-65-7.

Smejkal, V. Kodl, J. (2014). Assessment of the authenticity of Dynamic Biometric Signature. In Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST), 13-16 October 2014, Roma, Italia, p. 45–49, ISBN: 978-1-4799-3530-7.

Smejkal, V.; Kodl, J.; Sieger, L.; Novák, D.; Schneider, J. (2015). The Dynamic Biometric Signature. Is the Biometric Data in the Created Signature Constant? In Proceedings of 49th Annual 2015 IEEE International Carnahan Conference on Security Technology (ICCST). Taipei, Taiwan: R.O.C.,. pp. 385-390. ISBN 978-9-860-46303-3.

Smejkal, V.; Kodl, J.; Sieger, L. (2016). The Influence of Stress on Biometric Signature Stability. In Proceedings of 50th Annual 2016 IEEE International Carnahan Conference on Security Technology. Orlando, Florida, USA, New York: Institute of Electrical and Electronics Engineers,. s. 37-41. ISBN: 978-1-5090-1070- 7.

Termín odevzdání dizertační práce je stanoven časovým plánem akademického roku 2018/19.

V Brně, dne 5. 5. 2017

L. S.

| | |
|---|---|
| prof. Ing. Vojtěch Koráb, Dr., MBA<br>předseda oborové rady | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

## Abstract (English)

The aim of this thesis is to provide comprehensive information on the possibilities of authentication, combination of authentication factors and the integration of this issue into corporate communication. The work focuses on this issue and specifies the possibilities for obtaining authentication information, analyses the authentication methods, identification and authorization. It examines the applicability of biometric technologies, the principle of their functionality, examples of their use, their impact, the advantages and disadvantages they bring. A natural, easy-to-use, convenient tool for effective and secure communication is authentication including the dynamic biometric signature. The issues of the dynamic biometric signature technology and its implementation are examined from a comprehensive perspective involving experiments. The research proved that the dynamic biometric signature can serve as a method for supporting secure corporate communication and reduce authentication risks in companies and for individuals.

## Keywords

Electronic communication, identification, authentication, authorization, biometrics, dynamic biometric signature, cybersecurity.

## Abstrakt (česky)

Cílem práce je podat ucelenou informaci o možnostech autentizace, kombinace autentizačních faktorů a začlenění této problematiky do podnikové komunikace. Práce se zaměřuje na tuto problematiku a specifikuje možnosti získání autentizačních informací, dále analyzuje metody autentizace, identifikace a autorizace. Zkoumaná je využitelnost biometrických technologií, princip funkčnosti, příklady jejich použití, jejich vliv, výhody a nevýhody, které přinášejí. Přirozený, snadno dostupný, a tedy vhodný nástroj pro efektivní a bezpečnou komunikaci je autentizace zahrnující dynamický biometrický podpis. Problematika technologie dynamického biometrického podpisu a jeho implementace jsou zkoumány z komplexního hlediska včetně provedených experimentů. Z výzkumu vyplývá, že dynamický biometrický podpis dokáže sloužit jako metoda podporující bezpečnou podnikovou komunikaci a zredukovat autentizační rizika ve společnostech i pro jednotlivce.



## Klíčová slova

Elektronická komunikace, identifikace, autentizace, autorizace, biometrie, dynamický biometrický podpis, kybernetická bezpečnost.

## Abstrakt (slovensky)

Cieľom práce je podať ucelenú informáciu o možnostiach autentizácií, kombinácií autentizačných faktorov a začlenenia tejto problematiky do podnikovej komunikácie. Práca sa zameriava na túto problematiku a špecifikuje možnosti získania autentizačných informácií, ďalej analyzuje metódy autentizácií, identifikácií a autorizácií. Skúmaná je využiteľnosť biometrických technológií, princíp funkčnosti, príklady ich použitia, ich vplyv, výhody a nevýhody, ktoré prinášajú. Prirodzený, ľahko dostupný a preto vhodný nástroj pre efektívnu a bezpečnú komunikáciu je autentizácia zahrňujúca dynamický biometrický podpis. Problematika technológie dynamického biometrického podpisu a jeho implementovania sú skúmané z komplexného hľadiska vrátane experimentov. Z výskumu vyplýva, že dynamický biometrický podpis dokáže slúžiť ako metóda podporujúca bezpečnú podnikovú komunikáciu a zredukovať autentizačné riziká v spoločnostiach i pre jednotlivcov.



## Kľúčové slová

Elektronická komunikácia, identifikácia, autentizácia, autorizácia, biometria, dynamický biometrický podpis, kybernetická bezpečnosť.

## Bibliografická citace:

HORTAI, F. *Dynamický biometrický podpis jako efektivní nástroj pro vnitropodnikovou komunikaci*. Disertační práce. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 181 s. Vedoucí dizertační práce: prof. Ing. Vladimír Smejkal, CSc. LL.M.

## Čestné prohlášení

Prohlašuji, že předložená práce je původní a zpracoval jsem ji samostatně. Prohlašují, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů).

V Brně dne 30. 08. 2018 ……

podpis autora

## Poděkování

Děkuji vedoucímu doktorského studia prof. Ing. Vladimíru Smejkalovi, CSc. LL.M. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při doktorském studiu a při zpracování mé práce.

Děkuji mé rodině, která mě inspirovala a podporovala během celého studia. Děkuji mým rodičům za trpělivost, důvěru a za vše na co slova nestačí…

V Brně dne: 30. 08. 2018 ……

podpis autora

# Obsah

# Úvod

V novodobej informačnej spoločnosti je základný predpoklad úspechu spoločnosti, manažéra či jedinca sa „správne“ rozhodnúť. Rozvinutejšie pochopenie pre efektívne rozhodovanie platí, že relevantné informácie musia byť odovzdané na správne miesto, správnej osobe, v správny čas - podľa oblasti činnosti, zodpovednosti a právomoci. Predpoklad správnej informovanosti je komunikácia. Informácie musia ísť vhodne zvoleným komunikačným kanálom. Komunikačný kanál musí byť zabezpečený aby sa zredukovali alebo eliminovali možné hrozby. Zneužitie informácií alebo dezinformácia by spôsobila pravý opak toho, čo by racionálne uvažujúci manažér chcel dosiahnuť. Preto základ efektívnej komunikácie tvorí bezpečný tok informácií. Zabezpečená komunikácia má zaručiť jednoznačné určenie identity, autority a autentizáciu používateľov komunikácie, inými slovami napr.: kto, čo, kedy tvrdil a podpísal. Okrem profesionálneho života aj v každodennom živote sa vyskytujú situácie, ktoré vyžadujú čo najpresnejšie určenie, kto daná osoba/entita v skutočnosti je. Bežne sa každý človek môže pri osobnom jednaní identifikovať predložením občianskeho alebo iného preukazu. V oblasti informačných technológií autentizácia zohráva dôležitú úlohu všade tam, kde je nutné overovať pravosť osôb, dokumentov alebo systémov (overiť či je systém naozaj certifikovaný či legálny), najmä v prípade diaľkového prístupu. Rovnako je potrebné mať pod kontrolou prístupové práva jednotlivých používateľov.

Novodobé trendy v informačných a komunikačných technológiách prinášajú mnoho výhod, ale spolu s nimi prinášajú hrozby zneužitia a odcudzenia aktív a identity subjektov. Prostredie elektronickej komunikácie, napr. online služieb a internetových platieb je stále viac ohrozované najrôznejšími útokmi. Prevažná väčšina používateľov svojou neznalosťou podstupuje toto riziko útoku, napr. pri používaní nedostatočne zabezpečenej pracovnej stanice. Hrozba môže byť útok pomocou sociálneho inžinierstva využívajúceho podvodné stránky alebo sociálne siete na účely zberu citlivých dát od používateľov, alebo špeciálny útočný softvér (malware), prostredníctvom ktorého útočník ovláda zariadenie klienta. Spoločným menovateľom týchto útokov je nedostatočná schopnosť včas odhaliť nový útok. Príčinou sú aj neustále sa meniace stratégie útokov, ale aj skutočnosť, že súčasné technické prostriedky neposkytujú dostatočnú úroveň detailu ani analytické schopnosti pre odhaľovanie vzorov nových útokov v týchto údajoch. Pre mnoho spoločností je riziko nezabezpečenej komunikácie a nedostatočná autentizácia používateľa riešená retenciou rizika. Táto nedbanlivosť v dobe

kybernetickej kriminality môže viesť ku škodlivým následkom ako pre spoločnosti tak aj pre jednotlivca.

Jeden z kľúčových faktorov vo fungovaní spoločností sú informačné systémy (ďalej tiež iba IS). Vybrané IS sa stali kritickou súčasťou modernej spoločnosti (viď legislatívu ČR, zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů),* ale vo všeobecnosti spoločnosti sú závislé aj na fungovaní ostatných IS - štátnych aj súkromných. Preto je dôležité IS okrem správnej funkčnosti zabezpečiť aj príslušnými ochrannými opatreniami, aby sa nedali zneužiť obsahované informácie, nepovoleným prístupom vykonávať škodlivé procesy a všeobecne znížiť riziko ich zneužitia. Výpadok alebo porušenie IS by mohlo spôsobiť obrovské škody (napr. vysoké náklady), v niektorých prípadoch aj katastrofu (napr. porucha jadrovej elektrárne).

Zaistenie bezpečnosti je nepretržitý proces. Dôvodom sú nové technológie a rozvoj ľudského poznania. Obe totiž umožňujú nové typy útokov a vyžadujú nutnosť priebežných inovácií ochrán. Pri informačných systémov sa preto indukovala otázka: ako spoľahlivo overiť používateľov a vyhnúť sa neoprávnenému prístupu a zneužitiu? Práca preto skúma delenie faktorov autentizácie a možné kombinácie autentizačných faktorov. Jednotlivé faktory a metódy autentizácií sú stručne zhrnuté, sú znázornené ich výhody, ba aj úskalia. Výsledný cieľ práce je nájsť prirodzený, dostupný nástroj pre autentizáciu a efektívnu bezpečnú komunikáciu použiteľnú pre organizácie. Ako vhodný nástroj pre zabezpečenie dokumentov a autentizáciu používateľov v IS sa javí dynamický biometrický podpis (DBP), preto sa táto práca zameriava práve na túto technológiu.

Práca sa delí na logicky nadväzujúce časti podľa názvov číslovaných kapitol. Prvá kapitola slúži pre unifikáciu hlavných pojmov, použitých skratiek a cudzích slov. Druhá kapitola uvádza zdôvodnenie a zameranie dizertačnej práce. Tretia kapitola integruje sekundárny výskum na rozpoznanie stavu vedeckého poznania danej problematiky. Štvrtá kapitola definuje ciele, výskumné otázky a hypotézy dizertačnej práce. V piatej kapitole je vyhodnotený ako sekundárny, tak aj primárny výskum, ktorý zhŕňa aspekty pri implementácii a samotného používania dynamického biometrického podpisu. Šiesta kapitola sumarizuje prínos dizertačnej práce. Na konci v nečíslovanej záverečnej kapitole sa sumarizujú dosiahnuté výsledky.

# 1 Pojmy, skratky a predpisy

Pojmami v mnohých prípadoch sa už nakladá ako s notorietou, popritom nie každý a vždy si uvedomuje, aký presný význam sa pod určitým termínom skrýva. Pre unifikáciu pojmov a skratiek je určená táto kapitola, ktorá definuje často používané pojmy, ktoré sú relevantné na skúmanú tému. Vysvetlené pojmy v niektorých prípadoch vychádzajú z existujúcej legislatívy, v ostatných prípadoch sa jedná o pojmy skôr technologické, ktoré svoje vysvetlenie čerpajú ako z tuzemskej tak zo svetovej literatúry. Podkapitoly združujú pojmy, ktoré sú na seba logicky naviazané. V poslednej podkapitole sú v abecednom poradí vysvetlené ostatné skratky a cudzie slová.

## 1.1 Autentizácia, autorizácia, identifikácia a riadenie prístupu

Pojmy, ako sú identifikácia, autentizácia, autorizácia a kontrola prístupu patria medzi najčastejšie používané terminológie v oblasti bezpečnosti informačných systémov. (Akyildiz et al., 2002; Porada, Smejkal, 2017)

**Autentizácia**

Definícia autentizácie sa dá chápať ako: overovanie proklamovanej identity subjektu. Vykonáva sa predmetmi (preukazy, čipové karty, mobilný telefón a iné), svedkami, prejavom osobnej povahy (podpis, hlas, chôdza atď.), osobnými vlastnosťami (odtlačok prsta, hlas, chôdza, atď.), znalosťami (heslá, PIN, odpovede na kontrolnú otázku apod.) (Mates, Smejkal, 2012).

**Identifikácia**

Identifikácia sa dá chápať ako: rozpoznanie entity systémom, a to na základe určitého identifikátora, ktorý je spojený s určitou osobou, reprezentuje jeho identitu a môže byť známy iným osobám. (Meno a priezvisko, prípadne ďalšie identifikátory, odstraňujúce zameniteľnosť: rodné číslo, číslo sociálneho poistenia, bezvýznamový identifikátor atď.) Právne je identifikácia určenie osoby, ktorá urobila určitý úkon (Mates, Smejkal, 2012). Laicky definované ako zistenie identity (totožnosti) subjektu.

V praxi sa identifikácia na písomnom dokumente (listine) vykonáva najčastejšie uvedením mena, priezviska, adresy, prípadne iných údajov o dotknutej osobe. Autentizácia (overenie), že dokument skutočne podpísala uvedená osoba, sa vykonáva podpisom, podpisom

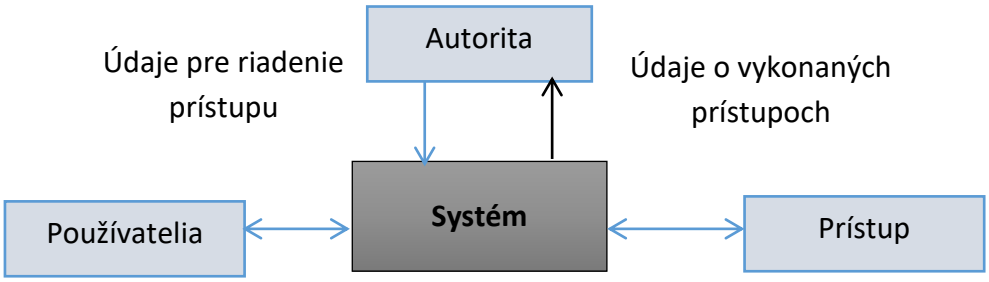
pred svedkami, overením totožnosti poverenou osobou. Najistejšia je zatiaľ stála legalizácia formou úradne overeného podpisu alebo notárskej zápisnice. Pravosť podpisu na papieri v prípade sporu o obsahu dokumentu je preukazovaná následne tiež znalecky znalcom v odbore písmoznalectvo (Mates, Smejkal, 2012).

### Autorizácia

Autorizáciu je možné chápať ako: pridelenie, respektíve overenie oprávnenia osoby k určitým činnostiam (Prístup do IS, povolenie na vykonávanie jednotlivých operácií) (Mates, Smejkal, 2012). Logická postupnosť je, že po prvej identifikácii autoritou sú pridelené aj práva daného subjektu.

### Riadenie prístupu

Riadenie prístupu (access control) je bezpečnostné opatrenie na základe stanovenej bezpečnostnej politiky autority (organizácie). Jeho zmysel je umožňovať autorizovaným používateľom prístup a neoprávneným subjektom v tomto prístupe zabrániť. Systém riadenia prístupu zaisťuje používateľom prístup v súlade s prístupovými právami stanovenými autoritou. Za účelom účtovacieho alebo bezpečnostného auditu môže zhromažďovať informácie o vykonaných prístupoch (autentizáciách). Pre grafické znázornenie viď Obrázok 1.1 nižšie:




*Obrázok 1.1: Systém riadenia prístupu*

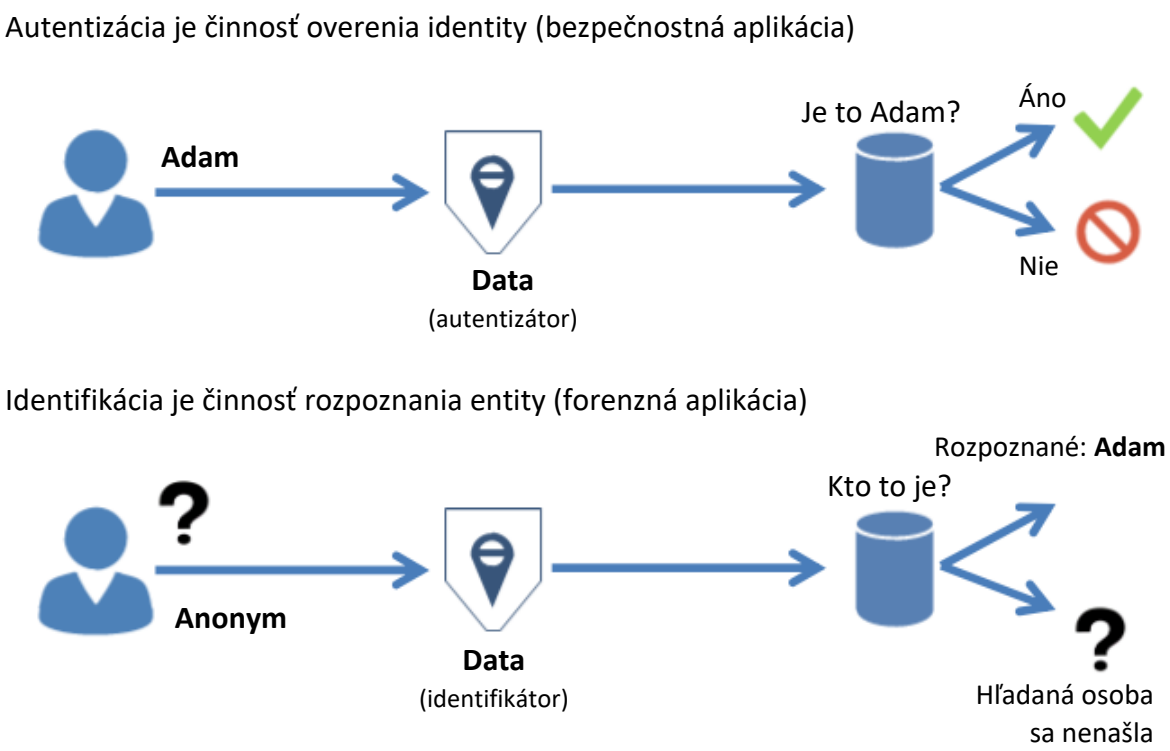
*Zdroj: vlastné spracovanie.*

### Naviazanosť procesov

Ako prvé je nutné entitu (platného používateľa) do systému zaregistrovať (prideliť identitu), následne mu priradiť autentizačné informácie a definovať jeho práva. Samotná autentizácia pozostáva z niekoľkých fáz. Základ procesu autentizácie je vyžiadanie od používateľa pridelenej identity (užívateľ zadá nejakú informáciu: svoje meno, *login* -

používateľského meno, *ID* – pridelená identita, atď.), týmto prebehne identifikácia. V druhej fáze sú od používateľa získané autentizačné informácie. Tie môžu mať rôznu formu, počínajúc heslom z klávesnice až po dáta prečítané z čipovej karty (tokenu) a podobne. Množstvom týchto autentizačných informácií, akého typu môžu byť, alebo akou postupnosťou sa získavajú, sa táto práca zaoberá zvlášť. Údaje sú potom spracované spôsobom, ktorý predpisuje príslušný autentizačný protokol systému k preukázaniu totožnosti používateľa systému. V poslednom kroku nasleduje jeden, alebo viacero komunikačných procesov na základe ktorých systém vydá rozhodnutie o tom, či autentizačnú požiadavku prijme alebo odmietne. Po autentizácii sú povolené vykonávať príslušné procesy podľa práv pridelené autoritou. Pri vykonávaní procesov sa skontroluje, či daná entita má právo vykonať príslušnú akciu.

Dôležitosť autentizácie používateľov závisí od toho, o aké aktívum sa jedná a aké riziko znáša zneužitie alebo strata daného aktíva. Zvyšujúcim rizikom by sa mala zvyšovať aj bezpečnosť autentizácie. Žiadny spôsob hodnotenia neumožňuje zaradiť systém bez základnej autentizácie do vyhovujúcej bezpečnostnej triedy (rada noriem „*ISO/IEC 27000*“ a „*ČSN ISO/IEC TR 13335 1 – 4 Informační technologie – Směrnice pro řízení bezpečnosti IT*“).




*Obrázok 1.2: Rozdiel medzi autentizáciou a identifikáciou*

*Zdroj: prerobené zo zdroja (Cinkais, Vábek, 2015)*

## 1.2 Dáta - údaje, informácia a znalosti

Na vyššie uvedené pojmy nájdeme nasledujúce pohľady definované v literatúre a v normách. Z hierarchickej logiky vyplýva: dáta → informácie → znalosť.

**Dáta (data), údaje sa dajú definovať ako (Smejkal, Rais, 2013):**

- Opakovane interpretovateľná formalizovaná podoba informácie vhodná pre komunikáciu, vyhodnocovanie alebo spracovanie (*ČSN ISO/IEC 2382-1*).
- Organizovaná informácia zbieraná pre špecifický účel (Black et al., 1993, s. 373).
- Označenie akýchkoľvek údajov spracovávaných programom (Krištoufek, 1982, s. 34).
- V českej legislatíve nájdeme aj pojem *„datový prvek“*, čím sa rozumie jednotka dát, ktorá je v danom kontexte ďalej považovaná za nedeliteľnú a je jednoznačne definovaná *(§ 2 písm.g zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů)*.

**Informácie sú definované ako (Smejkal, Rais, 2013):**

- Poznatok týkajúci sa akýchkoľvek objektov, napríklad fakty, udalosti, vecí, procesov alebo myšlienok vrátane pojmov, ktorý má v danom kontexte špecifický význam (podľa *ČSN ISO/IEC 2382-1)*
- Význam dát, ako ich má chápať človek. Dáta sú fakty; informáciami sa stávajú vtedy, keď sú v kontexte a nesú význam pochopiteľný ľuďmi (Woodcock et al., 1993, s. 198).
- Význam, ktorý je prisúdený dátam (Krištoufek et al., 1982, s. 74).
- Každé oznámenie obohacujúce vedomie príjemcu (Madar et al., 1995, s. 336).
- Informácia je akýkoľvek energetický či hmotný prejav, ktorý môže mať zmysel buď pre toho, kto oznamuje, alebo pre toho, kto oznamované prijíma (Mates, Matoušová, 1997, s. 27).
- Poznatok, ktorý obmedzuje alebo odstraňuje neistotu týkajúcu sa výskytu určitého javu z danej množiny možných javov (podľa *ČSN ISO/IEC 2382-16*).
- Informáciou sa na účely tohto zákona rozumie akýkoľvek obsah alebo jeho časť v akejkoľvek podobe, zaznamenaný na akomkoľvek nosiči, najmä obsah písomného záznamu na listine, záznamu uloženého v elektronickej podobe alebo záznamu zvukového, obrazového alebo audiovizuálneho (*zákon č. 106/1999 Sb., o svobodném*

*přístupu k informacím, ve znění pozdějších předpisů*). Na tejto definícii vidíme, ako sú informácie často zamieňané s ich nosičom.

**Znalosť:**

Znalosť je informácia, ktorá bola zorganizovaná a analyzovaná tak, aby bola zrozumiteľná a použiteľná pre riešenie problémov, rozhodovania a učenia. Znalosť možno tiež chápať ako kategórie vyššej formy obrazu o správaní objektov alebo o ich charakteristikách. Môžeme definovať niekoľkými spôsobmi (Smejkal, Rais, 2013):

- jasná a zaručená predstava niečoho,
- praktická skúsenosť, zručnosť,
- vedomosti, poznanie, atď.

### 1.2.1 Biometria a biometrický údaj

**Biometria:**

Predstavuje súbor vedeckých odborov, ktorý skúma človeka a iné živé organizmy podľa jedinečných merateľných charakteristík. Rozpoznávanie ľudí je možné na základe ich anatomických charakteristických rysov (fyziologické), alebo ich charakteristického správania (behaviorálne), ktoré slúžia pre jedinečnú identifikáciu osoby. (Jain, Ross, 2015)

**Biometrický údaj:**

V práci sa tento pojem používa podľa definícii aktuálnej legislatívy. Biometrický údaj v Európskej únii je regulovaný všeobecným nariadením EÚ o ochrane údajov - GDPR (Nariadenie Európskeho parlamentu a Rady č. 2016/679). GDPR začalo v celej EÚ platiť jednotne s účinnosťou od 25. 5. 2018. Aby členské štáty EU spĺňali všeobecné podmienky GDPR museli si prispôsobiť vlastnú legislatívu daným nariadením. V českom a slovenskom právnom poriadku sú biometrické údaje vymedzené takto:

- Aktuálna legislatíva Slovenskej republiky (účinnosťou od 25. 05. 2018): zákon č. 18/2018 Z. z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vymedzuje pojem biometrický údaj: „*biometrickými údajmi osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto*

*fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje,"*. Tento zákon reguluje a konkretizuje spracúvanie osobitných kategórií osobných údajov, t. j.: kto, za akých podmienok a akým spôsobom môže biometrické údaje spracúvať.

- V Česku GDPR nahradil právnu úpravu ochrany osobných údajov, ktorá bola v podobe *„směrnice 95/46/ES*" a súvisiaci zákon: *„zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů"* kde bolo vymedzenie pojmu v kategórii tzv. citlivých údajov v § 4 písm. b) *„citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,"*. Návrh nového zákona o spracovaní osobných údajov (Poslanecká sněmovna Parlamentu ČR, 2018, Sněmovní tisk č. 138, 2. čtení) je adaptovaný na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 a z časti implementuje smernicu Európskeho parlamentu a Rady (EÚ) 2016/680 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV*, kde biometrickým údajom sa rozumie: *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje"* (čl. 4 odst. 14 Nařízení). Vzhľadom k dikcii Nariadeniu EU č. 2016/679 český zákon žiadnu vlastnú definíciu biometrických údajov neobsahuje, pretože zákonodarca je viazaný textom nariadenia.

### 1.2.2 Autentizačné informácie a autentizačný faktor

Základ procesu autentizácie je vyžiadanie pridelenej identity od používateľa. Tento proces predpokladá, že entita je evidovaná autentizačným systémom a používateľ už má pridelené autentizačné informácie. Tieto pridelené autentizačné informácie sa rozlišujú podľa typu, charakteru, meniteľnosti, šírkou informácií a postupnosťou.

V literatúre nájdeme viacero delení. Niektorí autori v článkoch toto delenie nazývajú „autentizačné faktory" (Smith, 2002; Krhovják, Matyáš, 2007; FFIEC, 2005, Burr et al. 2013; apod.). Pri určovaní proklamovanej identity žiadateľa informačnými a komunikačnými technológiami je možné voliť zo 3 základných faktorov autentizácie, ktoré zahŕňajú veľa

spôsobov a typov. Podľa počtu týchto základných **faktorov autentizácie** sa autentizácia delí na jeden alebo viac faktorovú autentizáciu (Burr et al., 2013, str. 11). Delenie by mohlo byť:

- **Autentizačný faktor na základe znalosti a autentizácia pomocou znalosti** (niečím čo vieme). Používateľ svoju identitu dokazuje vedomosťou tajnej informácie. Od používateľa je vyžiadaná táto tajná informácia. Užívatelia majú mať túto tajnú informáciu uloženú vo svojej pamäti tak, aby bola ľahko zapamätateľná a nevznikli nepríjemnosti, že na ňu dotyčný zabudne. Tajná informácia môže mať podobu reťazca numerických znakov (**PIN**), reťazca alfanumerických znakov (**heslo** – *„password“*), alebo sekvenciu písmen alebo slov tzv. *„pass phrase“*.
- **Autentizačný faktor na základe vlastníctva a autentizácia pomocou vlastníctva.** K tejto forme autentizácie sa používajú predmety, s ktorými si osoby preukazujú svoju identitu (identifikačná karta, platobná karta a pod.). Autentizačný predmet je prakticky úložiskom autentizačných informácií a môže byť vybavený aj elektronikou.
- **Autentizačný faktor na základe charakteristiky používateľa a autentizácia pomocou charakteristiky používateľa** (niečím čím sme). Používateľ svoju identitu dokazuje svojimi vlastnými charakteristikami, biometrickými informáciami (napríklad odtlačkom prsta, hlasom a podobne). Identita sa dokazuje porovnaním aktuálne zistených biometrických charakteristík žiadateľa s dôveryhodnými záznamami týchto charakteristík. Sledované charakteristiky sa musia najprv u žiadateľa zistiť, nasnímať a až potom dôveryhodným spôsobom uložiť. Záznamy charakteristík sa ukladajú v kontrolných zariadeniach, alebo ich majú žiadatelia uložené vo svojich certifikátoch podpísaných autoritou. Pri žiadosti sa zistia aktuálne charakteristiky žiadateľa a porovnajú sa so zaznamenanými údajmi. Podľa miery zhody zistených a zaznamenaných údajov autentizačný systém rozhodne, či autentizačnú požiadavku prijme alebo odmietne.
- **Dodatočné údaje fyzického umiestnenia**, resp. geografická poloha. Poloha, miesto kde sa autentizácia odohrá, alebo je limitovaná na možné použitie. Samotne ale tento „faktor“ je pre autentizáciu nedostatočný.

## 1.3 Spracovávanie informácií a informačný systém

Spracovanie informácií je systematické vykonávanie operácií s informáciami, zahŕňajúce spracovanie dát a prípadne aj dátovú komunikáciu a automatizáciu kancelárskych prác (ČSN

ISO/IEC 2382-1, Informační technologie – Slovník. Část 1). Spracovanie dát (automatické spracovávanie dát) je analogicky obdobná spracovaniu informácií.

### 1.3.1 Informačný systém

V širšom slova zmysle informačný systém je systém na zber, udržiavanie, spracovanie a poskytovanie informácií. Systém nemusí byť nutne automatizovaný pomocou počítačov a môže byť aj v inej forme napr. papierovej. Príkladom informačného systému je aj kartotéka, telefónny zoznam, kniha došlej pošty alebo účtovníctvo.

Podľa (Mates, Smejkal, 2012) v najširšom pojatí je „informačný systém“ definovaný v českej legislatíve:

- *„v zák. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (ISVSZ), jako funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracováni a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností (§, 2 písm. b) - PÚTZ,“*
- *„v zák. č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, se informačním systémem nakládajícím s utajovanými informacemi rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací - PÚTZ.“*

Táto práca používa pojem *informačný systém* (skratkou IS) ako počítačový informačný systém. Je to celok zložený z počítačového hardvéru a súvisiaceho softvéru, zapojeného do danej počítačovej siete, do ktorého patria aj ľudia, ktorí daný hardvér a softvér využívajú a procesy (činnosti), ktoré pritom vykonávajú na účely zberu, spracovania a šírenia informácií potrebných na špecifické účely.

## 1.4 Skratky a cudzie slová

V abecednom poradí:

*AP* – z anglického *„Accounts Payable“* – pohľadávky.

*DBP* – dynamický biometrický podpis.

*ERT* – Electromagnetic Resonance Technology.

*etalón* – cudzie slovo a znamená „meradlo“. Táto práca používa tento pojem ako vzor nameranej a uloženej biometrie používanú ako vzor pre porovnanie pri autentizácii konkrétneho používateľa.

*FAR* - (False Acceptance Rate) reprezentuje hodnotu chybného prijatia (nesprávne stotožnenie používateľa so vzorkou niekoho iného). Výpočet je podľa vzorca v kapitole 3.6.6 na str. 62.

*FRR* - (False Reject Rate) reprezentuje hodnotu chybného odmietnutia (nestotožnenie používateľa s jeho vlastnou vzorkou). Výpočet je podľa vzorca v kapitole 3.6.6 na str. 63.

*GDPR* - (General Data Protection Regulation) všeobecné nariadenie o ochrane údajov podľa: Nariadenie Európskeho parlamentu a Rady č. 2016/679.

*H. (a číslo)* – Hypotéza s indexom značená číslom.

*hack* – je útok na počítačový systém za cieľom prelomiť jeho bezpečnosť a umožniť jeho neoprávnené používanie. Sloveso tejto činnosti je *„hackovať“* alebo *„hackovanie“*, kedy sa útočník dopúšťa kybernetickej kriminality.

*hash* – je vytvorený údaj prevodom údajov, či obsahu dokumentu matematicko-kryptografickou metódou na jeho reprezentáciu reťazcom čísel s pevne definovanou dĺžkou pomocou jednocestnej funkcie (dnes používané napr. SHA-256). Sloveso tejto činnosti je *„hashovať“* alebo *„hashovanie“*, s ktorým získame štandardný odtlačok (*hash*) z akéhokoľvek elektronického údaju napr. dokumentu, ktorý je následne jedným zo vstupov do procesu podpísania alebo zabezpečenia integrity hashovaného dokumentu.

*HW* – ustálená textová skratka hardvér, či hardware.

*ICT* – (information and communications technology) anglický výraz na informačné a komunikačné technológie, ekvivalent skratky by bolo IKT.

*ID* – pridelená identita pre identifikáciu.

*IS* – informačný systém.

*login* – tiež *sign in* označuje v počítačovej terminológii proces prihlásenia k účtu pomocou používateľského mena a autentizácie. Pojem *logout, logoff* či *sign out* označujú proces odhlásenia.

*malware* – škodlivý alebo zákerný softvér.

*man in the middle* - skratkou MITM, z angličtiny „človek uprostred“, alebo „človek medzi“. Je to snaha útočníka odpočúvať, prípadne aj meniť správy komunikácie medzi účastníkmi tak, že sa stane aktívnym prostredníkom bez vedomia účastníkov pôvodnej komunikácie.

*OTP* – (one time password), jednorazové heslo.

*passphrase* – sekvencia písmen alebo slov používaná ako tajná informácia.

*password* – heslo anglicky. Reťazec alfanumerických znakov používaný ako tajná informácia.

*phishing* – podvodná technika používaná k získavaniu údajov od obetí útoku, keď je komunikácia predstieraná, že pochádza od oficiálneho zdroja.

*PIN* – (personal identification number) osobné identifikačné číslo. Reťazec numerických znakov používaný ako tajná informácia.

*ROM* – (read only memory) pamäť iba na čítanie.

*rootkit* – je sada počítačových programov, pomocou ktorých možno maskovať prítomnosť *malwaru* v počítači, napríklad prítomnosť vírusov, trójskych koní, spyware a podobne.

*SW* – ustálená textová skratka softvér, či software.

*token* – je fyzické/hardvérové zariadenie určené na autentizáciu. Akýkoľvek predmet, obsahujúci bezpečne uložené informácie (USB pamäť, čipová karta, bezkontaktný čip pod.).

*URL* – (Uniform Resource Locator) univerzálny formát mien používaný na označenie zdroja na internete.

*V.O.* – výskumná otázka.

# 2 Zdôvodnenie a zameranie dizertačnej práce

Trendy novodobých elektronických zaradení svedčia o tom, že ICT sa stali základným kameňom pre zdroj údajov/informácií a prostriedkom pre zdieľanie údajov/informácií ako v prostredí komerčnom, tak aj v osobnom živote (viď kapitolu *3.1 Novodobé trendy v ICT*). Pri elektronickej komunikácii pritom extrémne dôležitú rolu hrá jej zabezpečenie. Dôvodom sú nové ľudské poznatky, ktoré prinášajú hrozby zneužitia a odcudzenia aktív a identity subjektov, a to hlavne pri komunikácii v ICT. Odbúravaním hraníc medzi vnútorným a vonkajším prostredím firmy sa zvyšuje tlak na informačnú bezpečnosť, ktorú novodobé trendy sťažujú a bez zavedenia ochranných prvkov aj ohrozujú. Preto je otázne, kde je tá hranica rentabilnosti novodobých ICT trendov a ako ich začleniť do hodnoty podniku a analyzovať hrozby, ktoré prinášajú. Táto práca sa konkrétne zameriava na biometrické technológie, ktoré sú stále viac a viac populárnejšie a dostupnejšie (z pohľadu technickej aj finančnej stránky). Biometrické technológie sú vhodné na bezpečnú autentizáciu používateľov ale nie sú úplnou náhradou všetkých bezpečnostných riešení.

Spoločnosti pri zaobstarávaní biometrických systémov musia posúdiť primeranosť konkrétneho riešenia (posúdiť účinnosť biometrických systémov) spoločne s rizikami s nimi spojenými, pričom musia vhodne kombinovať biometrický systém s ďalšími bezpečnostnými opatreniami na elimináciu/redukciu hrozieb, ktoré inštaláciou a používaním takýchto systémov úzko súvisia. Spoločnosti okrem zváženia vlastných potrieb, musia paralelne zabezpečiť legislatívne požiadavky danej krajiny, aby predišli zbytočným pokutám a trestnoprávnym záležitostiam. Biometrických technológií pritom existuje niekoľko, a jednotlivé metódy biometrií majú odlišný charakter a sú vhodné na špecifické účely. Táto práca konkrétne skúma metódu autentizácie DBP ako hlavnú autentizačnú metódu pre vnútropodnikovú komunikáciu.

Pre návrh konkrétneho výskumu sa najprv musí zúžiť spektrum možného výskumu, vychádzajúc z vedeckej teórie na špecifické riešenia. Preto ako základ práce je analýza súčasného stavu vedeckého poznania, ktorá argumentuje výhody a úskalia autentizačných technológii a ich efekt na podnikovú komunikáciu. Z tejto analýzy sa potom indukoval konkrétny primárny výskum zameraný na DBP.

# 3 Teoretické východiská a stav vedeckého poznania

Premetom práce je skúmanie konkrétnej autentizačnej metódy ako efektívneho nástroja pre vnútropodnikovú komunikáciu. Na samotné slovo komunikácia nájdeme niekoľko vysvetlení, napr. v latinčine „*communicare"* znamená *„zdieľať"* (Harper, Douglas, 2018). Ako základ je dôležité vymedziť samotný predmet komunikácie (napr. pozemná komunikácia – doprava, zdieľanie informácií apod.) (Korbař et al., 1962). Treba rozlišovať komunikáciu medzi subjektmi (komunikácia človek - človek, človek - stroj, stroj - človek, stroj - stroj), o aký typ komunikácie sa jedná (priamy/prezenčný, nepriamy/distančný) a aké prenosové médium sa používa na komunikáciu (Shannon, 1948). Empiricky je predpoklad pre úspešné fungovanie systému riadenia, či regulovania ale aj pri medziľudských vzťahoch práve efektívna komunikácia (správny subjekt má byť na správnom mieste, správny čas, u správnej entity/osoby). Efektívnosť komunikácie je pritom ovplyvnená niekoľkými činiteľmi (napr. rýchlosťou). Táto práca všeobecne pojem „komunikácia" používa ako proces prenosu a zdieľania údajov či informácií, pričom sa bude jednať hlavne o **elektronickú komunikáciu**.

Zdrojom informácií ako aj nástroj pre zdieľanie informácií sú používané informačné systémy. IS sa preto stali kritickou súčasťou modernej spoločnosti (viď legislatívu ČR, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů) a zastupujú jeden z kľúčových faktorov vo fungovaní spoločností (Koch, Chvátalová, 2017). Na zabezpečenie neustálej funkčnosti IS a prevenciu pred možnými hrozbami, musia byť implementované bezpečnostné prvky.

Kľúčovým predpokladom pre vybudovanie bezpečných informačných systémov je zabezpečenie správnej identifikácie a autentizácie ľudí, majetku a udalostí v systéme (Smejkal, Kodl, 2016). Prvky identifikácie, autentizácie, autorizácie a kontroly prístupu zohrávajú významnú úlohu aj v prípade vyšetrovania počítačovej kriminality pri určovaní spôsobu ako bol trestný čin spáchaný, t. j. ako páchateľ získal prístup k počítačovému systému a informačnému médiu a čo sa v systéme uskutočnilo. (Porada, Smejkal, 2017)

Ľudstvo ako celok, prakticky každý človek je dnes viac ohrozovaný kriminalitou kybernetickou, než násilnou či majetkovou. Kybernetická kriminalita a kyberterorizmus sú čoraz naliehavejšie vzhľadom na rastúcu závislosť civilizácie od informačných a komunikačných technológií. Pre podrobné aspekty kriminality spojenej s počítačmi, sieťami,

internetom, virtuálnym priestorom, sociálnymi sieťami a ďalšími, pre dnešnú dobu tak typickými fenoménmi viď literatúru (Smejkal, 2018).

Trendy zabezpečovacích prvkov a procesov v prostredí informačných a komunikačných technológií zahŕňa širokú oblasť úloh a implementácií. Autentizácia a autorizácia v informačných systémoch a pri elektronických dokumentoch sa stretáva s niekoľkými protichodnými požiadavkami na: používateľskú jednoduchosť, rýchlosť overovania, bezpečnosť, vierohodnosť a náklady (Mates, Smejkal, 2012, str. 273).

## 3.1 Novodobé trendy v ICT

Stabilita IS nadobúda extrémny význam s trendmi postupnou digitalizáciou služieb (napr. viď zákon v SR, Zákon č. 305/2013 Z. z. *Zákon o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)*) a vnútornej štruktúry firmy ako sú IoT, BYOD a Priemysel 4.0, ktoré prinášajú svoje výhody ale aj možné hrozby. IoT (z anglickej skratky „*Internet of Things*“ znamená „*internet vecí*“) je v informatike označenie pre prepojenie vstavaných zariadení s Internetom. Prepojenie zariadení by malo priniesť nové možnosti vzájomnej interakcie nielen medzi jednotlivými systémami, ale aj priniesť nové možnosti ich ovládania, sledovanie a zabezpečenie pokročilých služieb. BYOD (z anglického „*Bring Your Own Device*“) je lukratívnym trendom, ktorý znamená, že si zamestnanci nosia svoje vlastné elektronické či „smart“ zariadenia (ako sú notebooky, tablety, smartphony a pod.) do firemného prostredia. Integrácia BYOD do firemných politík je efektívnou reflexiou súčasného vývoja IT do spoločnosti a môže znamenať zvýšenie jej atraktivity, produktivity a mobility jej zamestnancov s možnosťami virtualizácie aplikácií alebo celých používateľských prostredí – desktopov (umožňujúc home office, teleworking atď.).

Priemysel 4.0 transformuje výrobu zo samostatných automatizovaných jednotiek na plne integrované automatizované a priebežne optimalizované výrobné prostredie. Vzniknú nové globálne siete, ktoré sú založené na prepojenie výrobných zariadení do kyberneticko-fyzických systémov - CPS (Cyber-Physical Systems). CPS budú základným stavebným prvkom „inteligentných tovární“, budú schopné autonómnej výmeny informácií, vyvolaní potrebných akcií v reakcii na momentálne podmienky a vzájomnej nezávislej kontroly. Stroje, senzory a IT systémy budú vzájomne prepojené v rámci hodnotového reťazca presahujúceho hranice jednotlivej firmy. Takto prepojené CPS na seba budú pomocou štandardných komunikačných protokolov na báze Internetu vzájomne reagovať a analyzovať dáta, aby mohli predvídať

prípadné chyby či poruchy, konfigurovať samy seba a v reálnom čase sa prispôsobovať zmeneným podmienkam. (Smejkal, Hortai, Molnárová, 2017a)

Pre koncepčné riešenie projektov Priemysel 4.0 je kľúčovým aspektom to, že autonómnu jednotku v rámci zložitého výrobného systému tvoria nielen výrobné úseky, výrobné stroje a ich nástroje, ale aj transportné vozíky a pásy, roboti, ale najmä výrobky, čiastočne spracované výrobky, dávky vstupného materiálu. Za súčasť výrobného systému sú považovaní aj ľudia, niektorí z nich ani nemusia sedieť vo výrobnom závode. Očakáva sa, že všetky tieto autonómne jednotky spolu môžu nepretržite flexibilne komunikovať, vyjednávať, spolupracovať. Aby k takejto silnej komunikačnej a interakčnej spolupráci mohlo dochádzať aj napriek tomu, že niektoré prvky ani nevedia samy komunikovať, môžu byť všetci aktéri reprezentovaní softwarovými modulmi, agentmi, ktorí konajú za nich a namiesto nich. Vzniká tak predstava o prepojení dvoch svetov - svetu reálnych fyzických objektov (strojov, zariadení, robotov, výrobkov, ľudí) a svetu virtuálneho, kde môže byť každá fyzická jednotka v tej či onej podobe dostatočne virtuálne reprezentovaná, zastúpená a jej správanie simulované softvérovým modulom. Už dnes dochádza doslova k prerastaniu oboch svetov. Predpokladá sa, že prvky fyzického sveta budú prepojené navzájom prostredníctvom napojenia na Internet, kde každý takýto fyzický prvok má svoju individuálnu IP adresu - potom sa hovorí o Internete vecí (Internet of Things - IoT). Softvérové moduly, reprezentujúce fyzické elementy vo virtuálnom priestore spoločne riešia úlohy, koordinujú svoju činnosť a rozhodujú s využitím služieb, ktoré si navzájom poskytujú, či ktoré si vyvolávajú prostredníctvom Internetu služieb (Internet of Services - IoS). Aj keď sa z hľadiska metodického hovorí o dvoch Internetoch IoT a IoS, v skutočnosti sa často fyzicky používa Internet jediný s jedinou chrbticovou infraštruktúrou v rámci celého výrobného úseku a realizovanou vo forme ESB (Enterprise Service Bus). Pre roboty a ľudí je nutné počítať so špeciálnymi rozhraniami, umožňujúcimi mobilnú komunikáciu, a to aj na báze prirodzenej reči, vizuálnej či hmatovej informácie - dochádza teda k napojeniu aj na tretí typ Internetu, Internet ľudí (Internet of People - IoP). (Mařík, 2016)

Odbúravaním hraníc medzi vnútorným a vonkajším prostredím firmy sa zvyšuje tlak na informačnú bezpečnosť, ktorú novodobé trendy sťažujú a bez zavedenia ochranných prvkov aj ohrozujú. Preto je otázne, kde je tá hranica rentabilnosti novodobých ICT trendov a ako ich začleniť do hodnoty podniku a analyzovať hrozby, ktoré prinášajú. (Smejkal, Hortai, Molnárová, 2017b)

Medzi relatívne novými trendmi by sa dali zmieniť používanie biometrických technológií, ktoré sú stále viac a viac populárnejšie a dostupnejšie (z pohľadu technickej aj finančnej stránky) viď napríklad autentizáciu na smartphonoch alebo iných „inteligentných“ zariadený.

Medzi trendmi v ICT v EU by sa dal zmieniť ešte rozruch ohľadne ochrane údajov, ktorý spôsobil GDPR (General Data Protection Regulation). Je to nariadenie Európskej únie, ktoré vstúpilo do účinnosti 25. 5. 2018. Jeho cieľom je zvýšiť úroveň ochrany osobných údajov a posilniť práva občanov Európskej únie v tejto oblasti. Vzhľadom k nadobudnutiu účinnosti GDPR (Nariadenie Európskeho parlamentu a Rady č. 2016/679), je dôležité mať na pamäti, že podľa čl. 83 nariadenia možno uložiť správne pokuty až do výšky 20 000 000 EUR, alebo ak ide o podnik, až do výšky 4% celkového ročného obratu celosvetovo za predchádzajúci finančný rok, podľa toho, ktorá hodnota je vyššia. Tie sumy sú veľkou pravdepodobnosťou likvidačné pre väčšinu podnikov, pričom dôvody môžu spočívať „len” v nezabezpečenom alebo v nesprávnom obsahu informačného systému podniku.

## 3.2 Predpoklady autentizácie

Použité metódy autentizácie by mali spĺňať požiadavky na variabilitu ako z pohľadu použitých technológii a systémov, tak aj z hľadiska samotných používateľov. Navrhované riešenie musí navyše vychádzať z práva jednotlivých strán na komunikáciu medzi oprávnenými účastníkmi a v prípade úradných alebo bankových operácií spĺňať požiadavky na uzavretie riadneho kontraktu či vykonanie transakcie (Mates, Smejkal, 2012, str. 272).

Autentizácia používateľov v oblasti ICT musí zabezpečiť rovnaké podmienky ako pri klasicky realizovaných činnostiach (napr. pri službách a transakciách poskytnutých v písomných formách), t. j. zabezpečiť výmenu dát medzi oprávnenými používateľmi pri zaistení neodmietnuteľnosti vykonaných činností (Smejkal, Kodl, 2008). V prípade priameho osobného styku (na oboch stranách sa vyskytuje človek) je identifikácia a autentizácia postavená na princípe rozoznania subjektu (autentizovanej osoby) posudzovateľom. Tento kognitívny a rozhodovací proces je síce jednoduchý, rýchly a relatívne spoľahlivý, na druhej strane je zaťažený možnými rizikami, vyplývajúcimi zo subjektívneho poňatia celého procesu.

Pri osobnom styku prichádzajú do úvahy predovšetkým nasledujúce varianty s rôznymi rizikami autentizácie a autorizácie (viď *Tabuľka 3.1*):

*Tabuľka 3.1: Varianty rizík pri autentizácii a pri autorizácii v osobnom styku*

| Situácia | Riziko pri autentizácii | Riziko pri autorizácii |
|---|---|---|
| 1. strany sú si osobne známe | Prakticky nulové | Stredné - obe strany môžu predpokladať poverenia, ktoré nemusia byť pravdivé |
| 2. autentizovaná osoba je známa osobe autentizujúcej | Možnosť podvrhnutia autentizujúcej osoby (v skutočnosti ide o účastníka); možno odstrániť preverením (legitimovaním) alebo štatusovým správaním (výskyt na určitom mieste - pracovisku a komunikácie s ďalšími zamestnancami) | Stredné - obe strany môžu predpokladať poverenia, ktoré nemusia byť pravdivé |
| 3. autentizujúca osoba je známa osobe autentizovanej | Autentizovaná osoba sa môže vydávať za niekoho iného; možno odstrániť pomocou dokladov (legitimovaním) alebo svedkov (zaručením sa za totožnosť), pričom v oboch prípadoch je riziko síce nízke, ale nezanedbateľné | Nízke - v rámci preverenia identity autentizovanej osoby je možné získať informácie o jej poverení |
| 4. osoby sa nepoznajú | Autentizácia na základe inej vlastnosti než osobnej známosti, je bezpečnosť autentizačného procesu priamo úmerná bezpečnosti použitej metódy. Bez uplatnenia verifikačných nástrojov je riziko vysoké. | Stredné - obe strany môžu predpokladať poverenia, ktoré nemusia byť pravdivé |

*Zdroj: (Smejkal, Kodl, 2008).*

V prípade komunikácie bez osobného styku, typu komunikácia na diaľku pomocou informačných a komunikačných technológií (človek/stroj/človek, človek/stroj alebo stroj/stroj) nastáva iná situácia. Možnosti podvrhu identity sú rozsiahlejšie, preto je dôležité zabezpečiť dostatočnú bezpečnosť pri autentizácii. Pri určovaní proklamovanej identity informačnými a komunikačnými technológiami je možné používať niekoľko faktorov autentizácie, ktoré zahŕňajú veľa spôsobov a typov. Pri distančnej autentizácii a autorizácii by mali byť dodržané nasledujúce predpoklady (Smejkal, Kodl, 2009):

- *„Byť technologicky neutrálny.*
- *Politiky, ktoré sa vzťahujú k riešeniu autentizácii, by mali byť odlišné od politík týkajúcich sa zaistenia bezpečnosti údajov.*
- *Byť škálovateľný a umožniť prípadné rozšírenie bezpečnostných modelov.*

- *Malo by rešpektovať požiadavky všeobecne záväzných právnych predpisov aj interných dokumentov.*
- *Musí byť pre používateľa jednoducho použiteľné a nesmie klásť vysoké finančné požiadavky na ktorúkoľvek zo strán.“*

## 3.3 Prehlaď autentizačných faktorov

Pri určovaní proklamovanej identity informačnými a komunikačnými technológiami je možné voliť zo základných faktorov autentizácie, ktoré zahŕňajú veľa spôsobov a typov. Základný spôsob autentizácie je jednofaktorová autentizácia. To znamená, že používateľ preukazuje svoju identitu jedným z uvedených troch druhov dôkazov – dôkaz znalosťou, dôkaz vlastníctvom, dôkaz charakteristikou osoby.

Príklady prvkov autentizačného reťazca (**dôkaz faktoru/overenie faktoru**):

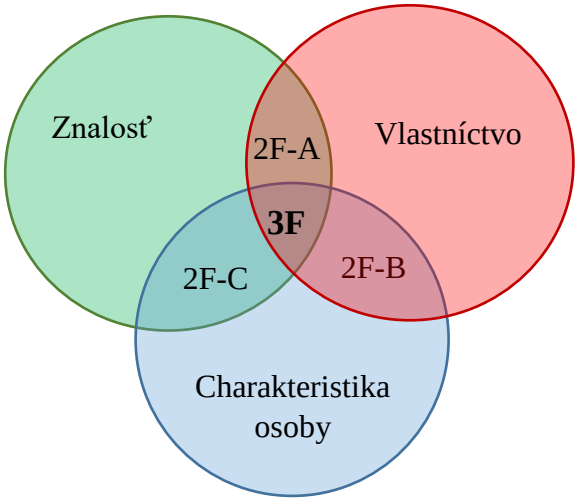
- Heslo/heslo alebo heš hesla (autentizácia znalosťou).
- Karta/snímač (autentizácia predmetom).
- Biometria/opis biometrie (autentizácia žiadateľom).

V literatúre nájdeme aj dodatočné autentizácie údaje (Hortai, 2017), a to napr. polohu (resp. geografická polohu), či miesto kde sa autentizácia odohrá alebo je limitovaná na možné použitie. Pri elektronickej komunikácii pre tento účel môžu slúžiť GPS súradnice zariadenia (zemepisná šírka a dĺžka súčasnej pozície), umiestnenie servera alebo pracovnej stanice (napr. doména či IP adresa zariadenia), atď. (Lenzini et al., 2008). Samotne ale tieto údaje sú pre autentizáciu nedostatočné. Pri vzdialenej komunikácii sa zvyšuje možnosť falšovania týchto údajov (proxy servery, vzdialené hackovanie pomocou interného *rootkit*-u, sfalšované súradnice zariadenia atď.) a tým aj riziko autentizácie. Táto práca pre výslednú komunikáciu predpokladá aj vzdialenú formu komunikácie a z tohto dôvodu sa nezaoberá týmto typom autentizácie konkrétnejšie a uvažuje ju iba ako doplnok autentizácie napr. pre evidenciu.

Každý typ autentizácie má svoje výhody aj nevýhody, a preto sa často kombinujú do takzvanej viacfaktorovej autentizácie (Smejkal, Kodl, 2008; Huang et al., 2011). Viacfaktorovou autentizáciou alebo kombináciami metód sa dá zvyšovať bezpečnosť autentizácie. Jednotlivé faktory autentizácie, ich metódy a ich možná kombinácia je podrobnejšie vysvetlená v podkapitolách (viď príslušné kapitoly ďalej).

### 3.3.1 Kombinácia autentizačných faktorov a viacfaktorová autentifikácia

Pre prehľadné znázornenie kombinácií autentizačných faktorov sa použili Vennove diagramy:




*Obrázok 3.1: Kombinácia autentizačných faktorov*

*Zdroj: vlastné spracovanie.*

Obrázok 3.1 predstavuje základné tri skupiny autentizačných faktorov a ich kombinácie. Separované množiny predstavujú jednofaktorovú autentizáciu, a to faktory množín znalostí (niečím čo vieme), vlastníctva predmetov (niečím čo vlastníme) a charakteristikami osoby (niečím čím sme). Ostatné varianty vzniknú prekrývaním množín, tu sa jedná o viacfaktorovú autentizáciu. Možnosť **2F-A** predstavuje dvojfaktorovú autentizáciu napr. kombináciu autentizačného predmetu a PIN. Je možné teda jednoznačne určiť majiteľa autentizačného predmetu a v prípade snahy o zneužitie pri odcudzení je nutné vedieť vstupný kód/PIN. Dvojfaktorová autentizácia, časť prekrývaním množín **2F-B** je napr. využitie rozoznávania tváre a čipovej identifikačnej karty. Možnosť dvojfaktorovej autentizácie **2F-C** predstavuje použitie snímača odtlačkov prsta spolu s heslom, ktoré je potrebné zadať. Skupina **3F** predstavuje trojfaktorovú autentizáciu (Huang et al., 2011), kde sa využívajú všetky tri autentizačné faktory aspoň jednou metódou.

Dôležité je rozlišovať aj použitie viacnásobných riešení z rovnakej kategórie, keď sa nejedná o viacfaktorovú autentizáciu, ale o typ vrstvenej bezpečnosti (FFIEC, 2005). Podľa počtu základných **faktorov autentizácie** sa autentizácia delí na jeden alebo viacfaktorovú autentizáciu, cudzojazyčne aj prezývanú multifaktorovú autentizáciu (Burr et al., 2013, str. vii.). Viacfaktorová autentizácia používa akékoľvek dve alebo viac autentizačných faktorov. Kľúčovou súčasťou je to, že overovacie faktory musia byť aspoň v dvoch kategóriách faktorov.

Napríklad pomocou čipovej karty a PIN je overovanie viacfaktorové, pretože tieto dva faktory sú „niečo, čo máte“, a „niečo, čo viete“. V prípade, ak by používateľ musel zadať PIN a potom známe heslo, to by podľa tohto prístupu nebolo multifaktoriálne overenie, pretože obe metódy sú z rovnakého faktora (dôkaz znalosťou).

Pri skúmaní pojmu „dvojfaktorová autentizácia“ sa môžeme stretnúť s nezhodu pojmov. Jedna forma dvojfaktorovej autentizácia je niekedy nazvaná „two step Authentication“ (Stanford University, 2016). Tento pojem zväčša používajú webové autentizačné rozhrania. Samotný Google používa pojem „2-Step Verification“, ktorej možnosti pre používateľov ponúka bezplatne. Odlišnosti „overenia dvoch krokoch“ Googlu od dvojfaktorového overovania je, že nie vždy je nutné použiť druhý faktor na overenie. Druhý faktor (nie heslo používateľa) je vyžiadaný iba na overenie vašej identity, pri možných pochybnostiach o identite (prístup z inej krajiny, neznáma MAC adresa zariadenia, atď.), alebo keď vyprší platnosť cookies súborov stanovené v prehliadači používateľa (možnosťou nastavenia). Pre detailné vysvetlenie viď príklad (Google, 2017).

Overenie v dvoch krokoch používa dva typy autentizácií na overenie identity používateľa: na príslušný ID alebo login používateľ zadá jemu známe heslo (1 faktor). Po správnom zadaní hesla je umožnení ďalší krok (2 faktor, je niečo požívateľ má): overovací kód. Z logiky vyplýva, že sa jedná o dvojfaktorovú autentizáciu (v prípade použitia externého zariadenia). Faktor znalosti a druhý faktor je predmet, ktorý používateľovi udeľuje zatiaľ jemu vopred neznámu informáciu pre autentizáciu (minimálne na úrovni potvrdenia). Tento typ overenia sa vyžaduje na prístup k systémom, ktoré majú vyššiu úroveň bezpečnosti (Humphreys, 2011). Okrem toho, overenie v dvoch krokoch zaistí lepšiu ochranu elektronického účtu používateľa, napr. pred odpozorovaním hesla. Pre znázornenie autentizačných možností tohto typu pre webové platformy niektorých firiem viď zdroj (Davis, 2014).

### 3.3.2 Autentizácia pri elektronických systémoch

Empiricky: z historického hľadiska z periférnych zariadení bola zatiaľ najviac využívaná konzolová platforma (monitor a klávesnica). Toto prispelo k tomu, že najčastejším známym spôsobom pri autentizácii v IS je jednofaktorová autentizácia a to dôkaz znalosťou - PIN, heslo, fráza, ktoré sú viazané na identifikačný údaj ako meno používateľa, login alebo ID (Xu et al., 2009). Známe príklady sú prihlásenie do operačného systému na počítači alebo často využívané ako základné prihlásenie na webových stránkach atď.

V súčasnej dobe je ale potrebné orientovať sa na viacparametrovú alebo viacfaktorovú autentizáciu, keď je riešenie postavené na kombinácii dvoch alebo troch autentizačných faktoroch. Na nedostatok jednofaktorovej autentizácie upozorňuje aj príklad zlyhania autentizácie cloudového systému iCloud od známej spoločnosti Apple v lete roku 2014, keď nedbanlivosť tvorcov používateľského IS umožnila hackerom nabúrať sa k dátam používateľov (veľký rozruch spôsobili nahé fotky amerických celebrít) (Arthur 2014; Landi 2014). Pre iné príklady kybernetickej kriminality spojené s prelomením alebo odcudzením hesla viď literatúru (Smejkal, 2018).

ISO (International Organization for Standardization) rezervovala sériu noriem ISO 27000 pre systémy riadenia bezpečnosti informácií v oblasti informačných technológií. Všetky štandardy z rady 27000 definujú jednotnú štruktúru a pravidlá pre začlenenie špecifických požiadaviek a môžu ich využívať organizácie všetkých typov a veľkostí (napríklad obchodné podniky, vládne úrady, neziskové organizácie apod.).

Pre zvýšenie bezpečnosti sa v súčasnej dobe najčastejšie používa dvojfaktorová autentizácie predmet plus znalosť. Jej najbežnejším príkladom je personalizácia mobilného telefónu pomocou SIM karty (token), ktorej obsah, resp. prístup k nemu, je chránený prístupovým PIN-om (Hortai, 2017), alebo príklad bankovej karty s príslušným PIN-om.

Novodobé trendy v ICT (viď kapitolu 3.1) priniesli aj zmeny používaných zariadení. Používateľmi často používané zariadenia ako sú prenosné notebooky a smart zariadenia často obsahujú snímače použiteľné pre biometrické autentizácie (napr. snímač odtlačku prsta). Týmto spôsobom sa dostáva do podvedomia používateľom čoraz viac používaná biometrická autentizácia.

## 3.4 Autentizačný faktor znalosť

Od subjektu je vyžiadaná tajná informácia - dôkaz znalosťou. Užívatelia majú mať túto tajnú informáciu uloženú vo svojej pamäti tak, aby bola ľahko zapamätateľná a nevznikli nepríjemnosti, že na ňu dotyčný zabudne.

Zásadnou nevýhodou sú nároky kladené na pamäť používateľov, ktorí majú tendenciu k zapísaniu si hesla, špeciálne v prípadoch, keď sa heslo v pravidelných časových intervaloch mení a je komplikované si ho zapamätať (He, Wang, 2015). Možnosťou voľby hesla používateľom, môže vzniknúť nevýhoda a to vysoká zraniteľnosť zvoleného hesla z dôvodu buď voľbou príliš jednoduchého hesla (1234, „heslo“), alebo voľby takej kombinácie čísel

alebo písmen, ktorú daný človek najlepšie pozná (dátumy narodenia rodinných príslušníkov, atď.) alebo „recyklácia“ už používaného hesla pri inom systéme apod.

Technika je zraniteľná odpozorovaním znalosti (nezakrytie prstov pri zadávaní PIN-u; malé zabudované kamery; verejné kamerové záznamy; elektronické monitorovanie klávesnice alebo komunikácie; SW typu spyware) alebo útokom: útok hrubou silou, útok prenesením hesla a slovníkový útok (anglicky „dictionary attack“) (Bonneau, 2012). Pri slovníkovom útoku útočník postupne predkladá rôzne heslá zo slovníka najpoužívanejších hesiel (napr. mená, názvy, letopočty apod.), kým na správne heslo nenarazí. Útok hrubou silou (anglicky „brute force attack“) (Alsaleh et al., 2012) je väčšinou pokus o rozlúštenie šifry/hesla bez znalosti kľúča na dešifrovanie. V praxi sa jedná o systematické testovanie všetkých možných kombinácií alebo obmedzenej podmnožiny všetkých dostupných kombinácií.

Ochrana proti útokom:

- V prípade možnosti nastavenia vlastného hesla/PIN-u používateľmi, je potrebné upozorniť požívateľov aby nepoužívali všade tie isté PIN-y alebo heslá (prevencia proti útoku prenesením hesla).
- Nech používateľ používa ťažko odhadnuteľné heslá. Riešenie: systém donúti osobu použiť heslo obsahujúce malé a veľké písmená, čísla, interpunkčné znamienka aj pri vlastnej voľby hesla.
- Obmedzenie prístupu, a to obmedzením počtu pokusov pre nesprávne prihlásenie, alebo systematické predlžovanie doby ďalšieho overenia správnosti hesla (časový zámok).
- Použiť časovo obmedzené heslá (heslo sa musí meniť v daných časových intervaloch).
- Passphrase – heslová fráza, dlhšia sekvencia znakov a väčší počet znakov (alfanumerická a interrupčné znamienka), aby odolala slovníkovému útoku i útoku silou a pritom bola ľahko zapamätateľná.

Metódy založené na znalosti hesla, resp. na báze tajnej autentizačnej informácie sú základom pre všetky autentizačné protokoly. Ak je autentizačná informácia získaná akýmkoľvek spôsobom, vo finálnej podobe bude prevedená do podoby digitálnej – akejsi obdoby hesla. Následne z hľadiska ďalších protokolov nemá zmysel rozlišovať, či sa jedná o skutočné heslo, alebo digitálnu podobu inej autentizačnej metódy (Doseděl, 2004).

### 3.4.1 Diskusia a zhrnutie tejto časti

Autentizácia pomocou znalosti sa v IS používa najčastejšie a tak je dobre známa aj pre laikov. Je to jednoduchá a lacná metóda. Typickými aplikáciami sú prístup k počítaču a prístup k webovým službám. Na ochranu pred zachytením hesla v komunikačnom kanáli sa používa šifrovaný prenos hesla.

- **Výhody**: jednoducho distribuovateľné, lacná implementácia a používateľom známa.
- **Nevýhody**: veľké riziko odpozorovania znalosti. Používateľ dôkaz faktoru môže zabudnúť, a preto variabilita faktoru kvôli zapamätateľnosti je relatívne malá (slabá na možné slovníkové alebo podobné útoky).

## 3.5 Autentizačný faktor vlastníctva

K tejto forme autentizácie sa používajú predmety. Autentizačný predmet je prakticky úložiskom autentizačných informácií. Overenie totožnosti pomocou predmetu pri osobnom styku je pre ľudí známe, napr. pri úradných záležitostiach s občianskym preukazom. Pri možnostiach ICT túto autentizáciu predmetom v literatúre nájdeme aj pod menom „*token*“ (Mayes, Markantonakis, 2008). Táto autentizačná metóda sa v praxi využíva zvyčajne v spojení s predchádzajúcou (znalostnou), existujú však aj techniky založené výlučne na vlastníctve určitého autentizačného predmetu (Ministerstvo financií SR, 2013). Prieskum ukázal, že pre tento účel overovania identity pomocou faktoru vlastníctva je možností niekoľko.

Delenie autentizačných predmetov do kategórií v literatúre nájdeme viaceré (Lorenc, Matyáš, 2007). Rôzne typy majú rozdielne vlastnosti, a tým spojené výhody a nevýhody pri používaní. Kvôli hodnoteniu ich práca delí do vlastných kategórií, podľa:

- **dynamiky informácie:**
  - statický,
  - dynamický;
- **konštrukcie:**
  - klasické (bez elektroniky),
  - elektronické prevedenie;
- **typu realizácie:**
  - hardwarový,
  - softwarový,
  - realizácia pomocou externého zariadenia;

- **integrácii s používateľom:**
  - integrovaný,
  - neintegrovaný.

### 3.5.1 Dynamika pamäte

Jedná sa o jednoduché delenie podľa dynamiky autentizačných informácií. Môže sa deliť na statickú alebo dynamickú informáciu.

- Statická - predmetom obsahovaná informácia pre autentizáciu je nemenná pri používaní.
- Dynamická - predmetom obsahovaná informácia pre autentizáciu sa mení pri používaní (napr. výstup je funkciou aktuálneho dátumu a času alebo spätnej väzby).

### 3.5.2 Delenie podľa konštrukcie

**Klasické** predmety (bez elektroniky) v ICT predstavujú jedinečný zoznam kódov pre autentizáciu konkrétneho používateľa. Tlačený zoznam kódov môže mať niekoľko typov:

- Formu knižky alebo zošita obsahujúci kódy pre jednorazové použitie. Každý kód je použiteľný iba raz a po použití sa stáva neplatným.
- Tlačený zoznam kódov**,** takzvaná „grid karta“ (Entrust, 2018) na overovania dvojstupňovej autentizácie.


*Obrázok 3.2: Ukážka grid karty*

*Zdroj: [online] [cit. 20.08.2018] URL: https://www.entrust.com/gridcard/.*

Po prvotnej autentizácii (napr. ID a príslušné heslo) je vyžiadaný ďalší kód pri nasledujúcom kroku autentizácie napr. kód s príslušnou adresou v knižke alebo v prípade grid karty maticového charakteru sa vyžaduje informácia na kombinácii stĺpca a riadka (napr. používateľovi sa ukáže B1 a on musí zadať príslušné heslo na políčku B1) viď *Obrázok 3.2*.

Z pohľadu typu realizácie sa jedná o hardwarový typ (materiálne existujú, ale neobsahujú funkčnú elektroniku). Z pohľadu dynamiky pamäte by sa dali nazvať pseudo-dynamické, lebo autentizačné kódy sú vopred známe ale ich poradie používania obsahuje dynamiku.

Existujú aj iné typy, ale postupným technologickým vývojom a digitalizovaním sa dostávajú do pozadia a dominujú elektronické predmety pre autentizáciu. Napríklad jednoduchým naskenovaním alebo odfotením grid karty je hotová elektronická softwarová verzia, ktorá je voľne distribuovateľná, a preto jeho používanie reprezentuje nebezpečné riziká. Z tohto dôvodu sa práca s týmito klasickými predmety predmetmi nezaoberá.

**Elektronické** predmety sú buď konštruované funkčnou elektronikou (vlastnou hardwarovou konštrukciou), alebo v elektronickej podobe používané na hostiteľskom systéme (viď ďalšie delenia podľa typu realizácie). Predmety obsahujú elektronicky uložené informácie, ktoré sú pri autentizácii z nich extrahované, alebo vyžiadané spätnou väzbou.

### 3.5.3 Typy elektronických tokenov

Podľa realizácie boli delené na: hardwarový, softwarový, externý.

#### Elektronický hardwarový token

Elektronický hardwarový token je fyzicky zrealizovaný a má charakter predmetu. Primárnou požiadavkou hardwarového autentizačného predmetu obecne je zaistenie vyššieho stupňa bezpečnosti oproti „základnej“ metóde autentizácie – prihlásenie heslom. Jeho charakteristika spočíva vo vlastníctve predmetu používateľom, ktorý ho musí mať k dispozícii, ak sa chce autentizovať do systému. Hardwarové tokeny obvykle existujú v niekoľkých formách: karta, autentizačný kalkulátor a USB kľúč. Často používanými autentizačnými tokenmi sú identifikačné plastové karty (napr. bankové karty). Delia sa na niekoľko typov podľa ich obsahu a schopností. Najjednoduchšie sú karty s magnetickým prúžkom obsahujúce nemennú informáciu (napr. klasické bankové karty). Aktuálne používané karty sú už použiteľné na bezkontaktnú komunikáciu na krátku vzdialenosť (metre), ktorá je zabezpečená technológiou RFID (Radio-frequency identification - identifikácia na rádiovej frekvencii).

Technológia RFID je použiteľná pre viaceré účely: chip-ovanie produktov (napr. na prevenciu krádeži), chip-ovanie domácich zvierat (na identifikačné účely), atď., ale aj použiteľná pre autentizáciu používateľa (viď PayPass bankové karty). Na používanie RFID sa vzťahujú: norma ISO/IEC 29167-1 (2014) definuje architektúru bezpečnostných služieb pre normy rozhrania ISO/IEC 18000 pre zariadenia na rádiofrekvenčnú identifikáciu (RFID).

ISO/IEC 20248 špecifikuje dátovú štruktúru digitálneho podpisu pre RFID a čiarové kódy, ktoré poskytujú autentickosť údajov a metódy snímania. Automatické identifikácie a techniky zachytávania dát sa vykonávajú v rámci ISO/IEC JTC 1/SC 31.

Chipy sú k dispozícii v prevedení pre čítanie alebo pre čítanie a zápis. Delenie **hardwarových** tokenov podľa dynamiky pamäti tokenu:

- **Statické pamäťové tokeny** – napr. statická pamäť ROM.
- **Dynamické pamäťové tokeny** – ktoré sú osadené mikroprocesorom alebo dynamickou pamäťou. Tiež nazývané aj *inteligentné* alebo *smart* tokeny (Mayes, Markantonakis, 2008).

Podľa kontaktu pri extrahovaní informácií:

- **Kontaktný** – tokeny ktoré potrebujú priamy kontakt zo snímacím povrchom alebo vloženie do snímaného zariadenia (napr. magnetické pásky).
- **Bezkontaktný** – tokeny ktoré nevyžadujú priamy kontakt zo snímacím povrchom (napr. RFID).

**Inteligentné/smart-tokeny**

Smart-tokeny rozširujú možnosti pamäťových tokenov využitím mikroprocesora zabudovaného priamo do tokenu. Vďaka zabudovanej elektroniky token môže vykonať určité operácie s údajmi, ktoré sú v ňom uložené. Smart-token môže, ale nemusí vyžadovať zadanie znalosti (napr. PIN-u) pred použitím na autentizáciu (napr.: zariadenie na používanie bankovej karty). Pri podmienke vyžadovania hesla/PIN-u tokenom, je pamäť na čipe smart-tokenu nečitateľná, kým sa nezadá správne heslo/PIN. Využitie zabudovaného procesora môže byť rôzne, zväčša ide o generovanie jednorazových hesiel, generovanie dynamických hesiel, alebo o zapojenie do protokolu výzva – odpoveď. Existuje viacero typov smart-tokenov: typ smart-karty (napr. platobná karta s čipom) alebo môžu vyzerať ako malé kalkulačky s displejom a konzolou, USB kľúče.

**Autentizačné kalkulátory** môžu byť založené na tajomstve uloženom v samotnom zariadení a na autentizačnom serveri, alebo na synchronizovaných hodinách. Kľúčová vlastnosť kalkulátorov spočíva v hardwarovej implementácii kryptografického algoritmu a v možnosti použitia technológie zdieľaného tajomstva komunikačným protokolom na báze výzva - odpoveď. Medzi ďalšie vlastnosti môže patriť rozhranie pre interaktívnu komunikáciu s používateľom, ktoré sa skladá z klávesnice a displeja. Optické rozhranie, infračervený port,

Bluetooth zasa umožňujú komunikáciu s ďalšími zariadeniami bezkontaktne (Krhovják, Matyáš, 2007).

**USB autentizačné tokeny** pracujú na podobnom princípe ako karty obsahujúce čip. Disponujú pamäťovou oblasťou pre ukladanie chránených dát, kde sú typicky ukladané šifrovacie kľúče. Prístup k funkciám je umožnený až po zadaní PIN kódu. Hlavná prednosť USB autentizačných tokenov v porovnaní s čipovými kartami, je spôsob pripojenia a komunikácie s počítačom. Pripojujú sa priamo k USB portu a teda nevyžadujú žiadnu čítačku alebo špeciálny snímač. V praxi to znamená rýchlu inštaláciu a intuitívne používanie. (Mayes, Markantonakis, 2008).

### Softwarový token

Je obdoba hardvérového tokenu v softwarovom vydaní. Softwarový token je uložený na univerzálnom elektronickom zariadení, môže sa jednať o prenosný počítač, stolný počítač, tablet, smartphone a podobne. Hlavná výhoda softwarového tokenu je, že používateľ nepotrebuje ďalšie zariadenie, ktoré musí prenášať, môže ho mať aj vždy pri sebe (Hortai, 2015). Zároveň je to hlavný rozdiel oproti hardwarovému tokenu, ktorý musí byť uložený v špecializovanom zariadení. Softwarový token má podobu aplikácie, ktorá sa inštaluje na zariadenie, ktorého hardware bude pre výpočty vhodný. Token môže byť zabezpečený ďalším faktorom, zväčša sa jedná o heslo/PIN. Ďalšia výhoda je možnosť jednoduchej distribúcie a aktualizácie softwarových tokenov (napr. použitie nového bezpečnejšieho šifrovacieho algoritmu, atď.). Môže podporovať automatizáciu procesov a tým urýchliť proces autentizácie. Náklad na vývoj nového hardvéru je nulový. Nákladom je vývoj, údržba a prevádzka SW na danú platformu.

Úroveň bezpečnosti je priamo úmerná bezpečnosti hostiteľského systému. Softwarový token ale môže implementovať zvlášť bezpečnostné prvky (napr. šifrovanie správ, kontrola odposluchu atď.). Pretože sa jedná o software, je tento typ tokenu vystavený hrozbám, ako napadnutie vírusom, tak aj všetkým druhom softwarových útokov. Tieto hrozby sa dajú eliminovať použitím antivírusových a antispyware softvérov na hostiteľskom systéme (poprípade aplikovaním firewallu). Pri mobilných aplikáciách je doporučené použiť čo najuzavretejší systém alebo aplikovať šifrovacie metódy pre zabezpečenie obsahu.

SW token by sa dal ďalej deliť podľa použitej platformy (PC, smartphone) a podľa kompatibility s operačným systémom (Windows, Mac OS, Linux alebo u smart-zariadení: Android, IOS, Windows, atď.).

**Realizácia pomocou externého zariadenia**

Je podobný ako softwarový token, ale bez použitia špecializovaného softwaru. Tento typ autentizácie zdieľa autentizačné informácie s vopred nastaveným externým zariadením cez jeho vopred definovaný komunikačný protokol. Distribútor autentizačných údajov nevie zabezpečiť ďalšie spracovanie týchto údajov, a je plne závislý na danom zariadení. Úroveň bezpečnosti je daná bezpečnosťou zvoleného komunikačného zariadenia.

Príkladom takejto autentizácie sú **heslové správy prichádzajúce na mobilné zariadenie používateľa**: poslanie raz použiteľného hesla, tzv. OTP (anglicky One-Time Password) na vopred nastavené zariadenie (napr. telefónne číslo SIM karty), pomocou textovej správy obsahujúce toto heslo (napr. prostredníctvom SMS správy). Väčšina bánk podporuje tento spôsob k prístupu na internetbanking.

### 3.5.4 Integrácia s používateľom

**S používateľom neintegrovaný**

Tokeny sú predmetného charakteru a používateľ ich v prípade potreby musí nosiť zo sebou (napr. banková karta, autentizačný kalkulátor atď.) alebo používajú hostiteľské zariadenie, na ktorej sú závislé (napr. softwarové tokeny).

**S používateľom integrovaný**

Na autentizáciu pomocou vlastníctva sa používa predmet, ktorý je do entity integrovaný, v prípade živej bytosti a človeka implementovaný do vlastného tela. Autentizačný predmet sa stáva „súčasťou“ používateľa a tým prináša možné výhody (predmet má používateľ stále zo sebou). I keď prináša podobné výhody ako biometrická autentizácia, predmet sa nestáva biometriou používateľa. Samotná autentizáciu predmetom, i keď je zabudovaná do tela používateľa je jednofaktorová a to autentizáciu vlastníctvom (používateľ vlastní predmet).

Tieto integrované predmety sa dajú deliť podľa dynamiky pamäte (kapitola 3.5.2) a podľa konštrukcie (kapitola 3.5.1).

**Prípad klasickej konštrukcie statickou informáciou** je príklad označenie jazvou dobytka či dokonca aj ľudí otrokov (Higginbotham, 1978, str. 176–184). Toto označovanie je proces, kedy sa vpáli značka, symbol alebo ornament vzoru, do kože žijúcej osoby s úmyslom, aby výsledná jazva bola trvalá a rozpoznateľná. Možné označenie je aj pomocou vytetovanie čísla alebo obdoby čiarového kódu na telo používateľa. Počas Druhej svetovej vojny

fašisti používali tetovanie na telá väzňov pri registrácii a identifikácii v koncentračných táboroch sériovými číslami v Osvienčime (Piper, Świebocka, 1996, str. 60-61). Tieto typy sa v praxi používajú skôr na identifikačné účely pri forenzných aplikáciách napr. pri identifikácii podľa tetovania (Lee et al., 2012).

Sofistikované prevedenie predstavujú **elektronické konštrukcie**. Elektronický hardware sa upraví tak aby ju bolo možné implementovať do tela používateľa. Obsahované informácie závisia od použitej technológie. Známy spôsob je vpichnutie pod pokožku ruky používateľa kapsulu obsahujúcu RFID chip. Tento chip, potom nahradzuje kartu, kľúč, atď. na vstup či login do autentizačného systému. Pri implementácii komplexnejších elektronických konštrukcií musia používatelia podstúpiť chirurgický zákrok. Takéto označovanie sa bežne používa pri zvieratách.

Technoprogresivistické fantázie o prekročení obmedzení ľudského tela, pri prekonávaní (prostredníctvom medicínskych, technologických a výživných prostriedkov) choroby, slabosti, slabosti a konečnosti ľudského života prestavujú priaznivci biohacking-u (Malatino, 2017). Biohacking predstavuje skôr experimentálne prístupy ako vednú disciplínu. Tieto technologické implantáty majú svoje korene v teórii cyborgov (Sato et al., 2008), pri ktorej sa prejavuje radikálne divergentné chápanie cyborgovej realizácie. V praxi má ale čoraz viac podporovateľov a preto je aj čo raz aktuálnejší. Z tohto dôvodu je dôležité sa o nej zmieniť, lebo môže mať vplyv na autentizačné technológie hlavne na tie integrovateľné do používateľov. Návody na tieto technológie viď online na Biohack.me (2018): https://biohack.me/, alebo pre možnú kúpu hotových súprav a príslušných manuálov online na Dangerousthings (2018): https://dangerousthings.com/.

### 3.5.5 Diskusia a zhrnutie tejto časti

Táto autentizačná metóda sa v praxi využíva zvyčajne v spojení s predchádzajúcou (znalostnou), existujú však aj techniky založené výlučne na vlastníctve určitého autentizačného predmetu. Vlastnosti autentizačných predmetov sa líšia v závislosti na použitom type. Výsledné delenie slúžilo na jednoznačné stavovanie vlastností faktoru vlastníctva pre použite v ICT.

#### Výhody faktoru vlastníctva

Výhody oproti faktoru znalosti je, že tajné informácie nemusia byť používateľom zapamätateľné, resp. ich vôbec nemusí poznať. Autentizačné údaje preto môžu byť dlhšie a zložitejšie, ba aj dynamicky sa meniace, teda aj odolnejšie voči možným útokom.

Kombinácia niečoho „čo viem“ s niečím „čo vlastním“ poskytuje podstatne silnejšiu úroveň bezpečnosti ako jednotlivé metódy využité samostatne. Neoprávnená osoba aj po získaní tokenu nezískava kompletnú autentizačnú informáciu, nemôže token použiť ak nemá k nemu príslušnú znalostnú informáciu. Empiricky: získanie tokenu aj PIN/hesla je oveľa ťažšie ako získanie používateľského mena a hesla (samozrejme, pokiaľ si PIN/heslo používateľ nenapísal priamo na token). Používateľ na odpozorovanie hesla si nemusí uvedomiť, ale pri strate tokenu si používateľ môže všimnúť neprítomnosť predmetu a následne ho blokovať, znefunkčniť a tak predísť možných hrozbám.

**Výhoda u hardwarových tokenov** spočíva v tom, že v čase môžu byť použité iba na jednom mieste (napr. ten istý token môže byť použitý aj pre prístup do priestorov aj pre prihlásenie sa do počítača. Ak však používateľ chce opustiť PC, musí si token zobrať aby mohol prejsť cez chránené priestory. Minimalizuje sa tak riziko, že používateľ ostane prihlásený na počítači a nechá ho bez dozoru.) To ale nemusí byť pravda v každom prípade, napr. ak sa vytvorí klón/kópia tokenu (riziko falzifikovania tokenov). Z toho vyplýva, že bezpečnosť daného tokena je úmerná jej bezpečnostnej komplexicite a konštrukcie tokenu.

**Výhody u smart-tokenov je:**

- Smart-tokeny poskytujú značnú flexibilitu a môžu byť použité na riešenie mnohých problémov autentizácie. Všeobecne platí, že poskytujú väčšie zabezpečenie ako statické pamäťové tokeny. Smart tokeny môžu vyriešiť problém elektronického monitorovania s cieľom neoprávnene zachytiť autentizačné údaje aj v prípade, že overovanie sa vykonáva v rámci otvorenej siete, napr. pomocou jednorazových hesiel (Ministerstvo financií SR, 2013).
- Ak má elektronické rozhranie, prenos autentizačného údaja sa môže vykonať automaticky bez zásahu používateľa.
- V prípade interakcie s používateľom je umožnená dodatočná kontrola (napr. používateľ je informovaný o používaní tokena hneď pri používaní, alebo sa eviduje jej používanie)
- Sú komplikovanejšie a tak náročnejšie na falšovanie ako napr. klasické tokeny.

**Výhody softwarových a externých tokenov** je, že používatelia nemusia používať ďalší systém, ale používajú sa zostávajúce zaradenia, na ktorých sa spúšťajú alebo komunikujú s nimi. Tento typ umožňuje aj automatické spracovávanie informácií a uľahčenie autentizácie.

**Nevýhody faktoru vlastníctva**

Nutnosť nosenia bezpečnostného predmetu (tokenu). Okrem nosenia autentizačných predmetov aj ich používanie je prácnejšie, čo sa môže zdať používateľovi ako obťažujúce a komplikujúce pri prístupe (do miestnosti, IS, aplikácie, online služby, atď.). Je však dôležité uvedomovať si, že token slúži k ochrane samotného používateľa a jemu cenným aktívam (voči zväzku kľúčov, ktoré tiež treba nosiť pri sebe zvyčajne nikto nenamieta). Prípad keď sa používa externé zariadenie (napr. pošle sa OTP heslo na telefón používateľa) je nutné použiť dané zariadenie používateľa, ktoré nie je garanciou funkčnosti a je ovplyvnené exogénnymi faktormi (napr. predmet ukradnutý, batéria telefónu môže byť vybitá).

Používateľ autentizačný predmet môže stratiť alebo mu ho ukradnú. Nevzťahuje sa to na prípad integrovaného tokenu do používateľa. Tá však musí byť do neho implementovaná a proces implementácie nemusí byť pre neho prívetivý alebo v prípade technophobie (Rosen et al., 1993; 1995) vôbec prijateľný, ktorý môže vyvrcholiť až do všeobecnej hystérie ohľadne čipovania občanov. Integrované snímače sa ťažko aktualizujú a predstava hrozby krádeže originálu implantátu prináša nebezpečnú záležitosť a to násilné vyňatie z tela používateľa.

Hrozba repliky tokenu, ktorej bezpečnosť je úmerná od komplexnosti použitej technológie. Hrozba replikou môže byť kompenzovaná napr. tak, že sa token doplní ochrannými prvkami, ochranami voči falšovaniu. Tieto ochrany prinášajú ďalšiu nevýhodu a to finančnú náročnosť na technológiu výroby tokenov, snímačov alebo softwarového vývoja.

**Všeobecné nevýhody u hardwarových tokenov:**

- Potreba používania špeciálneho zariadenia (čítačky) extrahovať autentizačné informácie, avšak nie v každom prípade (napr. autentizačný kalkulátor).
- Elektronické zariadenie predstavuje ďalšie finančné náklady. Tieto náklady ale berú v niektorých prípadoch na seba subjekty, ktoré majú záujem o ich používanie (napr. banky alebo štát).
- Smart-token bez automatického rozhrania môže vyžadovať, aby používateľ vykonal niekoľko aktivít (napr. zadal výzvu do tokenu, zadal odpoveď do počítača) a môže takto spôsobiť nespokojnosť používateľa pri práci.

**Príklad použitia na minimalizáciu autentizačných rizík**

Na minimalizáciu rizík je použitý princíp výzva-odpoveď s viacfaktorovou autentizáciou. Vhodné riešenie je použitie hardvérovej autentizačnej kalkulačky (integruje štandardné

nevýhody autentizačných predmetov: používanie predmetu, prácnejšia manipulácia s predmetom a použitie znalosti PIN-u). Pre použitie je potreba mať autentizačný kalkulátor, poznať príslušný PIN zariadenia a kontakt komu volať, v prípade napr. osobných bankárov sa identifikovať hlasom. Príslušný kontakt zadá číslo (výzvu) a po zadaní čísla do kalkulačky sa generujete odpoveď. Autentizačný kalkulátor tak zaistí bezpečnosť aj v prípade skompromitovaného PC (zabezpečenie ochrany pred odpočúvaním, mad-in-the-middle apod.).

## 3.6 Autentizácia charakteristikou používateľa – biometriou

Používateľ svoju identitu dokazuje svojimi vlastnými charakteristikami, biometrickými informáciami (napr. odtlačkom prsta, hlasom a pod). Sledované charakteristiky sa musia najprv u žiadateľa zistiť, dôveryhodným spôsobom nasnímať a potom bezpečne uložiť. Overovanie identity sa dokazuje porovnaním aktuálne zistených biometrických charakteristík overovaného subjektu s dôveryhodnými záznamami týchto charakteristík – etalónom. Podľa miery zhody aktuálne zistených charakteristík a údajov v kontrolných zariadeniach, autentizačný systém rozhodne, či autentizačnú požiadavku prijme alebo odmietne.

Biometrická autentizácia vychádzala z forenzných vied, ktoré umožnili jedinečnú identifikáciu osôb. Dnešné sofistikované metódy pomocou automatizovaného testovania biometrických prvkov s digitálnymi systémami umožňujú používanie biometrie pre autentizáciu používateľov. (Wlodarczyk, 2012)

Pri autentizácii používateľov sú nároky kladené na merateľnú telesnú vlastnosť. Musí sa jednať o vlastnosť, ktorou disponujú všetci užívatelia uvažovaného autentizačného zariadenia. Je vhodné vybrať vlastnosť, ktorá sa ľahko meria a je nemenná v čase (Rak et al., 2008).

Každá biometrická charakteristika má svoju efektívnosť aj nevýhody. Jednotlivé typy biometrií nemusia úspešne spĺňať všetky požiadavky (napr. presnosť, praktickosť a náklady spojené s implementáciou) všetkých aplikácií (napr. kompatibilita rozdielnych hardwarových platforiem, správa digitálnych práv, riadenie prístupu). Konkrétny výber závisí od konkrétnej aplikácie. (Pal et al., 2014)

Kvôli dôvodu rozdielnych vlastností biometrických prvkov, a tým spojené výhody a nevýhody pri používaní ich práca delí do kategórií pre prehľadnejšie hodnotenie:

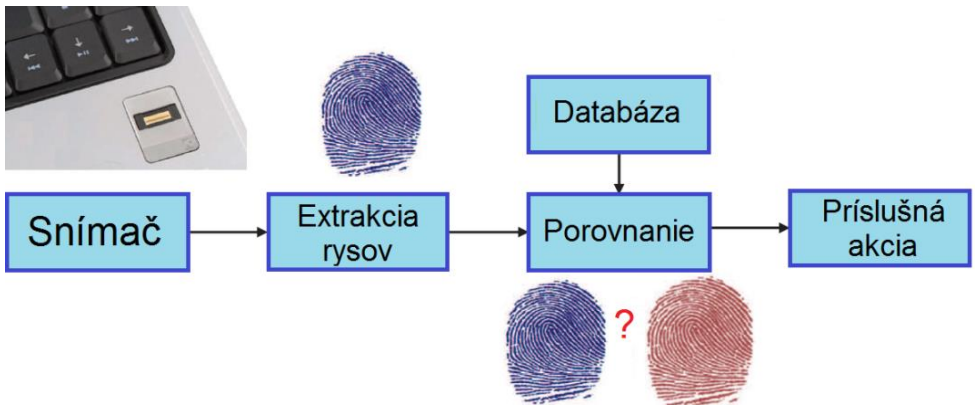
- **Prístup autentizačného systému**: podľa počtu porovnania overovanej biometrickej vzorky (viď kapitolu 3.6.1).

- Zoskupovanie údajov podľa **anatomických a fyziologických vlastností** (statické biometrie) a **behaviorálnych vlastností** (dynamické biometrie) (Galbally et al., 2015; Wang, Liew, 2012). Zhrnutie tejto časti delenia je v tabuľkách: *Tabuľka 3.2* a *Tabuľka 3.3*, kde sú zvolené metódy vysvetlené podrobnejšie.

### 3.6.1 Overovanie vzorky biometrie podľa počtu porovnania

**Porovnania 1 ku mnohým (1:n)**: overovaná vzorka biometrie sa porovnáva s každým etalónom v danej množine databázy (napr. prehľadávanie v databáze otlačkov prstov). Výhodou je, že nie je potrebná predbežná identifikácia overovanej osoby. Nevýhody tohto prístupu sú nároky na výpočtový výkon overovacieho systému ale aj vyššie riziko chybného prijatia pri autentizácii (systém vyhodnotí overovanú osobu ako inú s podobnou biometriou).

**Porovnania 1 ku 1 (1:1)**: overovaná vzorka biometrie sa porovnáva s konkrétnym vzorom danej overovanej osoby. Vyžaduje sa predbežná identifikácia (napr. meno, ID) overovanej osoby, aby sa mohol použiť referenčný etalón. Zabezpečuje vyššiu bezpečnosť a eliminuje autentizačné nezhody overovaného subjektu s inými subjektami.




*Obrázok 3.3: Príklad postupu biometrického autentizačného systému*

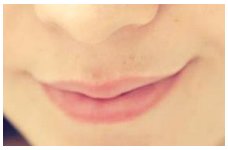
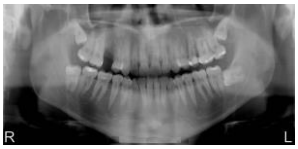
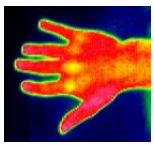
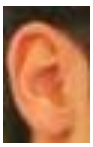
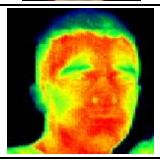
*Zdroj: vlastné spracovanie.*

### 3.6.2 Anatomické a fyziologické biometrické údaje pri autentizácii

Tieto údaje vychádzajú z anatomických vlastností používateľov a majú statický charakter (časovo nemeniaci údaj), v prípade fyziologických vlastností sú to stopy po osobe napr. pach. Ďalšia fyziologická vlastnosť živých ľudí je vyžarovanie tepla z tela. Exogénne vplyvy ako sú počasie apod. a zmeny pri emocionálnych či hormonálnych výkyvoch môžu ale silne vplývať na termogram používateľa. Preto termogram biometrie poslúži skôr ako doplnková, či dodatočná kontrola živosti overovanej biometrie napr. tváre, ruky, ušnice apod.

Táto časť uvádza príklady z možných merateľných biometrií, ktoré by sa dali použiť pre autentizáciu používateľov v rámci ICT. Zhrnuté sú v tabuľke: *Tabuľka 3.2* a zvolené metódy sú vysvetlené podrobnejšie.

*Tabuľka 3.2: Anatomické a fyziologické charakteristiky*

| | | | |
|---|---|---|---|
| Geometria ruky |  | Tvar pier |  |
| Krvné riečisko tela napr. rozloženie žíl na zápästí, prstov apod. |  | Dentálny obraz |  |
| Termogram ruky/dlane |  | Tvar a vlastnosti ucha |  |
| Odtlačky prstov |  | Spektrum kože |  |
| Geometria tváre |  | Necht, nechtové lôžko, ryhovanie nechtov |  |
| Termogram tváre |  | DNA |  |
| Dúhovka oka |  | Pach (odoranty) |  |
| Sietnica oka |  | | |

*Zdroj: vlastné spracovanie (obrázky majú ilustratívny charakter).*

**Odtlačky prstov**

Každý človek má jedinečnú štruktúru odtlačku, a preto môže byť pomocou neho jednoznačne identifikovaný. Snímanie odtlačku prsta patrí k najznámejším biometrickým metódam. (Drahanský et al. 2017)

V oblasti bezpečnosti a autentizácie sa používa bezprostredné snímanie. Osoba usilujúca sa o autentizáciu položí prst na snímací senzor, ten nasníma odtlačok a nasleduje spracovanie údajov. Nasnímané informácie sa porovnajú s referenčným vzorom odtlačkov uloženými v databáze. Môže sa jednať o porovnanie jedna k jednej (etanolom odtlačku danej osoby), alebo porovnanie jedna ku mnohým (všetkým, ktoré sú v danej databázovej množine).

Senzory sa delia na kontaktné a bezkontaktné (snímače optické, termálne alebo odporové). Snímacie prvky sa môžu integrovať do zariadení (smartphone, tablet apod.), do klávesnice stolných počítačov, do korpusu notebooku, alebo sa vyrábajú ako samostatné zariadenia, ktoré sa pripájajú ako periférie (Rak, Matyáš, Říha, 2008).

Výhoda je široká ponuka zariadení a snímačov. Jedná sa o relatívne lacnú technológiu na univerzálne použitie, malou veľkosťou a možnosťou mobilného použitia. Pre pokroky algoritmov rozpoznávania odtlačkov prstov viď napr. (Fan, Yu, Du, Li, Cao, 2012).

Táto metóda je náchylná na útoky falzifikátom. Odtlačok sa dá ľahko získať bez vedomia jeho nositeľa a vytvoriť z neho syntetický falzifikát (vyrobenie modelu odtlačku prsta, podľa nechanej vzorky odtlačku inde, napr. na sklenenom pohári, displeji dotykového telefónu apod.). (Kanich, Drahanský, 2017)

**Geometria ruky/dlane**

Kombinácie dĺžky, šírky a hrúbky, merané na všetkých piatich prstoch jednej ruky, ich tvar, obrys, kontúry a teda rozmery sú špecifické a jedinečné pre každého človeka (Dvořák, Drahanský, 2017). Identifikačné charakteristiky ruky sa od dospelosti relatívne nemenia. Autentizačný vzor sa vytvorí priemerovaním niekoľkokrát nasnímaných údajov, snímačom namerané rozmery potom softvér konvertuje do niekoľkobytovej biometrickej šablóny. Výhodou tejto metódy je malá dátová veľkosť biometrických vzorov (Rak, Matyáš, Říha, 2008). Nízko nákladová verzia rozpoznania dlane sa dá skomponovať pomocou jednoduchého skenera viď (Badrinath, Gupta, 2011).

Nevýhodou môže byť, že používateľom môže prekážať fyzický kontakt so snímačom, obmedzujú sa aj hygienické okolnosti používania. Z pohľadu inštalácie sa jedná o relatívne veľké zariadenie oproti ostatným metódam. Keďže geometria ruky nie je príliš unikátnou biometrickou vlastnosťou, jej aplikácia v bezpečnostnej sfére je obmedzená práve stupňom bezpečnosti, ktorý chceme dosiahnuť (Ščurek, 2008). Nízka miera chybných odmietnutí, ale aj nízka variabilita autentizačného prvku používateľov dokazuje nižšiu úroveň bezpečnosti. Odporúčaná iba pre doplnkovú verifikáciu osôb (kombináciou inými faktormi).

Táto metóda je tiež náchylná na možné útoky s falzifikátom geometrie ruky/dlane (napr. maketa obrysu daného tvaru). Bezpečnosť tejto technológia je úmerná na komplexnosti analýze danej biometrie, napr. či sa jedná o 2D alebo 3D obraz. (Dvořák, Drahanský, 2017)

**Krvné riečisko tela**

Charakteristiky tejto biometrie sú unikátne, dostatočne stabilné v priebehu života dospelosti každej osoby a vhodné pre proces autentizácie. Obraz je odlišný pre pravú a ľavú časť tela. Pomocou vybraných algoritmov sa prevedú obrazové konverzie a nasnímaný obraz je vektorovo uložený vo veľkosti niekoľko stoviek bajtov.

Oproti geometrie ruky je tento typ aj pohodlnejší, keďže orientácia ruky nemusí byť striktne dodržaná – tú identifikuje až software. Výhodou je aj bezkontaktný princíp (používateľ sa nemusí dotýkať povrchu snímača, čo zvyšuje hygienu) a neopotrebovávanie snímača kontaktom používateľov (pravdepodobnosť správneho prijatia používateľa).

**Rozloženie žíl na zápästí** – snímač rozpoznáva jedinca podľa predloženého zápästia (prvé komerčne dostupné systémy sú datované až k roku 2000). Táto technológia sa vyznačuje obťažnosťou falšovania (sieť ciev je ťažké napodobniť, pretože je vo vnútri ruky a nie je teda viditeľná pre napodobnenie, navyše niektoré princípy priamo vyžadujú, aby bola ruka živá, teda aby v nej tiekla teplá krv, alebo sú doplnené technológiou termovízie). Technológia spočíva v snímaní žíl ruky špeciálnou kamerou v infračervenom svetle. Tak je možné získať obraz stromovej štruktúry žíl, ktoré tvoria zreteľný vzorec. Štruktúra krvného riečiska sa navyše v dospelom veku príliš nemení a je výrazná. Jej jedinečnosť ukázali aj niektoré vedecké štúdie medzi jednovaječnými dvojčatami (Ščurek, 2008). Pri autentizácii môžu byť porovnané aj ostatné anatomické tvary zápästia (Kumar, Prathyusha, 2009). Pre bezpečné použitie viď (Wu et al., 2013).

**Rozloženie prstových žíl** - samotný prístup snímaní prstových žíl nemusí byť dostatočne veľkou vzorkou pre jednoznačné určenie biometrie. Snímka rozloženia prstových žíl je ale efektívnym doplnkom pre snímku odtlačku prsta, ktorou sa dá zvyšovať presnosť verifikácie. (Kumar, Zhou, 2012).

**Pre všeobecné znázornenie** úrovne tejto technológie odporúčam pozrieť si zdroj (Christie Medical Holdings, 2016), kde sa táto technológia používa aj v iných oblastiach.

**Rozpoznanie tváre a hlavy**

Empiricky: identifikácia osôb podľa tváre patrí k najprirodzenejším spôsobom rozpoznávania osôb. Ľudia pri osobnom kontakte sa práve rozpoznávajú podľa tváre, a preto je aj intuitívna a prijateľná pre používateľa pri autentizácii - žiadny fyzický kontakt (je možné aj pasívne monitorovanie bez vyzvania používateľa).

Z bezpečnostného pohľadu je dôležitý správny a výstižný popis tváre daného jedinca. Tento údaj sa veľakrát používa aj pri druhom faktore (dôkaz vlastníctvom), kde identifikačné karty obsahujú obraz tváre jedinca.

Z pohľadu biometrie sa predovšetkým popisuje celkový tvar, plnosť a farba. Ako doplňujúce znaky sú uvádzané vrásky okolo očí, nosu, úst, ich dĺžka a hĺbka, kútiky, kozmetické chyby, jazvy a podobne. Pre identifikáciu osoby sa používa analyticko-štatistická metóda na základe fotografického portrétu. Presnosť závisí na komplexnosti vyhodnocovacieho algoritmu, koľko údajov berie do úvahy (2D, 3D). Pri rozpoznávaní tváre sa dajú využiť aj algoritmy umelej neurónovej siete (Wright et al. 2009). Pre robustné rozpoznávanie tváre viď (Ou et al., 2014).

Technologický gigant Apple Inc. na nových zariadeniach prechádza pri autentizácii z rozpoznania z odtlačku prstov (tzv. Touch ID) na rozpoznanie pomocou tváre používateľa (tzv. Face ID). (Apple, 2017)

Tvár je odhalená biometria a preto verejnosťou snímateľná. Výhoda implementácie je ale možnosť využívania bežných kamier. Nevýhodou sú riziká možnými podvrhmi maskou, fotkou, video záznamom apod. napodobňujúcou charakteristiky tváre oprávneného používateľa. Na verejne dostupných stránkach na internete a videá na a www.youtube.com sú mnohé neúspešné ale aj úspešné znázornenia špekulantov ako oklamať jednotlivé „smart“ zariadenia pri autentizácii podľa tváre používateľa. Preto sa odporúča pri autentizácii podľa tváre používateľa sofistikovane overiť živosť snímaného objektu, napr. doplniť zariadenie termovíznou kamerou alebo vhodnou technológiou na redukciu rizika podvrhmi (napr. proti snímkam tvárí použiť snímania tváre v 3D; proti maskovým maketám tvárí je vhodná termovízia), ktoré sú viac a viac sofistikovanejšie.

Riziko spojené s rozpoznaním tváre môže byť aj zneužitie bez vedomia používateľa, napr. odblokovaním daného zariadenia alebo vykonanie nechcenej operácie, keď napr. používateľ spí alebo je omráčený a zariadenie ho bez jeho vedomia prijme autentizačnú požiadavku.

Riziko je aj pri jednovaječných dvojčatách/trojčatách (Wall Street Journal, 2017) alebo osôb, ktoré sú si tvárou veľmi podobné, a preto by ich systém vyhodnotil rovnako.

**Sietnica oka (retina)**

Používateľ sa zameria na špecifikovaný bod optického snímača a infračervený lúčom sa nasníma štruktúru sietnice (vnútorná zadná časť oka) a žiliek podobne ako pri snímaní krvného riečiska. Snímanie je na vzdialenosť niekoľko až desiatok centimetrov (Shikarwar et al., 2014). Vysoká presnosť, štruktúra žiliek sa líši u jednotlivcov a v priebehu života sa nemení, zmena ale môže nastať vplyvom chorôb, napr. diabetes, starnutia alebo úrazu (Koštialik, Maruniak, Drahanský, 2017). Snímanie sietnice je vhodné pre verifikáciu osoby (Lajevardi et al., 2013; Hájek, Doležel, Drahanský, 2014)

Jedná sa o „skrytú“ (na verejnosti nedostupnú) biometrickú vlastnosť, preto menej náchylnú na falšovanie. Nevýhodou sú nepríjemné pocity pre používateľa, bližší „kontakt“ so snímačom – napr. potreba zloženia okuliarov, priblížiť sa ku snímaču veľmi blízko a nechať si svietiť do oka. Relatívne vyššiu cenu snímacieho zariadenia kompenzuje jej presnosť overovanej vzorky.

**Dúhovka oka (iris)**

Nekontaktné biometrické snímanie, kde používateľ sa pozerá do kamery vo vzdialenosti až 1-2 m. Užívateľsky prívetivý, žiadny fyzický kontakt, okuliare neprekážajú. Vhodný aj pri masovom prílive ľudí (závislá od systému). Relatívne vyššiu cenu systému kompenzuje jeho vysoká presnosť rozpoznania vzorky. (Pillai et al., 2011)

Dúhovka oka ako aj tvár je na verejnosti snímateľná. Kamery s optikou a vysokým rozlíšením vedia dobre zaznamenať detaily dúhovky očí a tak výsledne vytvoriť falzifikát originálu (Fox-Brewster, 2015). Vyššia bezpečnosť sa dá docieliť spojením nasnímania dúhovky spoločne aj zo sietnicou oka používateľa (Hájek, Doležel, Drahanský, 2014).

**DNA**

Bunky živých bytostí obsahujú veľa subčastí medzi nimi aj DNA (Obsil, Obsilova, 2011). Existuje veľa možností získania DNA (vlasy, ochlpenie, sliny, krv, atď.). Výhodou je vysoká presnosť analýzy. Nepoužíva sa komerčne, nakoľko je overenie vzorky finančne náročné a časovo neefektívne. Hrozbou môže byť oklamanie systému cudzou vzorkou (eliminované odobratím vzorky pod priamym dohľadom) alebo zámenou odobratej vzorky – tieto okolnosti

sú vylučujúcimi pre distančné používanie v ICT. Vylučuje sa aj použitie v prípade jednovaječných dvojčiat, ktoré majú identické DNA.

**Odoranty – ľudský pach**

Metódou pachovej identifikácie sa môžeme stretnúť ako metódou kriminalistickej techniky a slúži na identifikáciu individuálneho pachu fyzickej osoby s ním vytvorenou pachovou stopou na mieste činu alebo na inom mieste, ktoré so spáchaním činu súvisí. Kriminalistická prax používa s vysokou spoľahlivosťou vycvičených psov. Podstata metódy pachovej identifikácie je subjektívne správanie psa, ktorého správnosť je možné overiť empiricky a za použitia moderných vedeckých metód vzniku pachu a fyziológia jeho vnímania k tomu zvlášť vybraným a vycvičeným psom za podmienok náhodnosti aj opakovania, teda spôsobom potvrdzujúcim alebo vyvrátením možnosti jeho využitia v konkrétnom prípade. (Straus, Kloubek, 2010, s. 9-11)

Ako príklad uvádzam: dôkaz pachovou stopou je prípustný vo väčšine štátov USA (Ensminger, 2010). Pritom súdy vždy prihliadajú v zmysle rozsudku vo veci People v. Kelly (1976) 17 Cal.3d. 24, stanovujúci všeobecné podmienky na vykonávanie dôkazu novou technológiou či vedeckou metódou (Kelly rule), ako aj v ďalších rozsudkoch požadujúcich všeobecné predpoklady rozhodnutia súdu založené na znaleckom skúmaní. Na strane kritiky je, že pes nie je technické zariadenie zostrojené a spôsobilé na účel individuálnej identifikácie ľudského pachu (ako napríklad človekom konštruovaný prístroj), a keď ako živý tvor vníma a identifikuje pachovú stopu svojimi zvlášť vyvinutými zmyslami, nie je neomylný. Na druhej strane americké súdy vnímajú fakt (frekvencia, úspešnosť) výsledkov konkrétnych psov, možné chybovosti pri individuálnej identifikácii a prípadné pochybnosti o jedinečnosti pachu každého jednotlivca výrazne znižujú alebo dokonca vylučujú (Ensminger, 2011, s 99).

Iným príkladom európskej praxe môže byť Spolková republika Nemecko. Obšírne zhodnotenie dôkazného využitia pachových stôp, vrátane kritérií, ktoré pritom zohľadňujú nemecké súdy, je obsiahnuté napríklad v monografii (Neuhaus, Artkämper, 2014, s. 143-146). Dôkaz metódou pachovej identifikácie bol, alebo je použiteľný ako dôkaz v trestnom konaní tiež v Holandsku, Belgicku, Maďarsku, Dánsku, Poľsku, Rakúsku, Rusku, Lotyšsku viď príklady: (Wójcikiewicz, 2000; Schoon, Haak, 2002).

Rozhodnutia v kriminalistike sú založené na konkrétnych požiadavkách. Predovšetkým ide o schopnosť psa správne identifikovať individuálny ľudský pach (certifikovaný výcvik), stabilitu psa a vhodnosť použitých procesov pri identifikácii pre dané účely. Aj keď sa spôsoby

vykonania metódy pachovej identifikácie v detailoch v rôznych krajinách odlišujú, majú spoločný cieľ: určiť individuálny pach osoby, ktorý sa nachádza na mieste činu, alebo na veciach, ktoré so spáchaním činu skutkovo súvisia. Často namietanou slabinou tohto dôkazného prostriedku je údajná nemožnosť overenia výsledkov pomocou vedeckých metód.

Ústav analytické chemie, Fakulty chemicko-inženýrské, Vysoké školy chemicko-technologické v Praze, za podpory Ministerstva vnitra ČR vykonávala od roku 2014 vedecký výskum: *Projekt VF20142015036 - Pachová signatura (2014-2015, MV0/VF),* ktorého cieľom bolo skúmanie molekulovej podstaty tzv. ľudskej pachovej signatúry, o ktorej sa verí, že je pre ľudského jedinca jedinečná, časovo stála a ktorú cvičený pes vie jednoznačne rozpoznať. Výskum je unikátny, pretože v odbornej literatúre predtým nebolo diskutované molekulové zloženie aktívnej ľudskej pachovej signatúry. Pri výskume bola potvrdená existencia skupiny molekúl obsiahnutých v pachovej stope človeka, ktorá má vlastnosti aktívnej pachovej signatúry. Bolo zistené, že tento súbor molekúl je chemicky veľmi stabilný a samotné molekuly majú relatívne malú prchavosť, čo zodpovedá skúsenostiam kriminalistov. Tieto molekuly sa podarilo oddeliť od ostatných molekúl pachovej vzorky, pričom pomocou špeciálne cvičených psov bolo preukázané, že oddelená skupina molekúl umožňuje jednoznačnú identifikáciu človeka. Vykonané pokusy ukazujú, že čuchový orgán psov je na molekuly pachovej signatúry o niekoľko rádov citlivejší ako súčasné možnosti inštrumentálnej chemickej analýzy. Avšak výsledky doterajšieho výskumu pachovej stopy ukazujú, že olfaktronická identifikácia páchateľa podľa pachovej stopy nájdenej na mieste činu je principiálne možná. Prípadný dôkaz takejto objektívnej identifikácie by zrejme mala väčšiu váhu na súde, ako v prípade použitia psa. Aby tento spôsob určenia bol umožnený, je nevyhnutné radikálne zmeniť metodiku odberu pachovej stopy, pričom samotná výmena sorpčnej textílie na čistejšiu nemusí byť pre chemickú analýzu dostatočná. (Doležal et al., 2016; Ústavní soud České republiky 2016)

Ľudský pach sa skladá z niekoľkých chemických zlúčenín, ktorých intenzita či absencia vytvára jedinečný profil u každého človeka. V oblasti civilného nasadenia je ale potrebné porovnávať a správne identifikovať viac ako jednu pachovú konzervu zároveň a preto zatiaľ neexistujú dostatočne presné senzory. Ďalším problémom sú zmeny v skladbe pachových stôp pri emocionálnych či hormonálnych výkyvoch. Reálne nasadenie tejto metódy na autentizačné účely v praxi je zatiaľ otázkou budúcnosti. (Ščurek, 2008; Inbavalli, Nandhini, 2014)

**Dentálny obraz**

Empiricky: pre presné určenie dentálneho obrazu živého človeka je požívaný röntgenový snímok. Kvôli vznikajúcej radiácii pri snímaný je tento typ zatiaľ v praxi nepoužiteľný. V iných prípadoch by sa jednalo o snímanie chrupu používateľa, ktorý by predpokladal snímače pre jedno použitie, kvôli hygienickým záležitostiam.

**Necht, nechtové lôžko, ryhovanie nechtov**

Metóda netradičná pre používanie pri autentizácii používateľov. Pri prieskume literatúry bolo zistené, že došlo iba k málo pokusom, a preto nie je možné jednoznačne stanoviť jedinečnosť nechtovej textúry, informáciách o kontúre a formy nechtového lôžka (Kumar et al., 2014; Bala, 2017).

Empiricky: metódy ktoré pracujú na viditeľných znakoch nechtu sú vystavené riziku podvrhmi falzifikátmi, lebo kvôli manipuláciami rukami máme väčšinou nechty odhalené, a preto sú verejnosťou snímateľné (napr. kamera s optikou a vysokým rozlíšením). Nechty tiež nemusia mať konštantný vzhľad, napr. manikúra, lak apod.

Presnejšia metóda na určenie identity osoby je použitie techniky interferometrie. Metódy založené na tomto jave na vykonanie analýzy nechtového lôžka neidentifikujú priame viditeľné znaky ryhovania nechtov ale štruktúru, ktorá sa nachádza pod ním, teda nechtové lôžko. Nechty obsahujú keratín, ktorý je prírodný polymér a menia orientáciu dopadajúceho svetla. Ak použijeme zdroj polarizovaného svetla pod určitým uhlom a ožiarime ním necht, môžeme zachytiť a analyzovať fázové zmeny lúča po odraze z nechtu na prijímači. Po spracovaní signálu získame číselnú sekvenciu, obdobu čiarového kódu, ktorú možno porovnať s databázou vzoriek (Ščurek, 2008). Manipulácia nechtovým povrchom ale môže mať vplyv na vyhodnotenie (napr. lak, gél na nechtoch, polámanie nechtu apod.) a tak znemožniť autentizáciu.

**Tvar a vlastnosti ucha**

Metóda založená na individuálnom tvare a morfometrickej stavbe ušnice ucha každého jedinca. Všeobecne existujú metódy pre biometrickú identifikáciu podľa ucha a ušnice:

- Podľa odtlačku štruktúr ušnice (podobne ako u odtlačkov prstov) – táto metóda pre prax nie je praktická, jej využitie je vo forenznej oblasti.
- Podľa morfometrických vzťahov - geometria ušnice, v 2D (Kumar, Wu, 2012) nebo 3D forme (Theoharis et al., 2008).

- Podľa odrazu zvuku v ušnom kanáliku. Pri verifikácii osoba priloží ucho k reproduktoru. Zvuk sa odráža od steny zvukovodu a jeho časť sa vracia odrazom ušnej steny späť. Intenzita pohltenia zvuku v ušnom kanáliku je u jednotlivcov individuálna a podľa tejto intenzity možno individuálne identifikovať osobu a overiť jej totožnosť. (Ščurek, 2008).

Použiteľnou metódou pre komerčné využitie, tak aby bola komfortná pre používateľa, je identifikácia podľa morfometrických vzťahov - geometria ušnice. Je to prípad nekontaktného snímania biometrie ušnice používateľa optickým snímacím zariadením zo vzdialenosti. Možné je aj implicitné overenie tvaru ucha pomocou fotoaparátu vo smartphone počas hovoru (Fahmi et al., 2012). Údaje na snímke (morfometrické vzťahy - rozmery, tvary, položenie významných bodov, krivky a pod.) sú potom vyhodnotené a v závislosti na použitom type algoritmu.

**Spektrum kože**

Ľudská koža sa skladá z niekoľkých vrstiev. Každá vrstva má odlišnú hrúbku a táto hrúbka sa u každého človeka mení, je jedinečne zvlnená a vyznačuje sa ďalšími charakteristickými rysmi. U ľudí kolagénové a pružné vlákna sú rozdielne, ako aj kapilárne lôžka sú odlišné vo svojej hustote a rozmiestnením, ďalej sa líšia veľkosťou a hustotou buniek vnútri pleťových vrstiev. Kožná spektroskópia využíva princíp metódy, že vybranú časť pokožky ožiari svetlom o viacerých vlnových dĺžkach (od viditeľného až k blízkemu infračervenému svetlu), každá vlnová dĺžka svetla sa potom láme a odráža v inej vrstve pokožky a od iných štruktúr kože. Odraz svetelných lúčov je zachytený prijímačom a odovzdaný na ďalšie spracovanie. Na tento typ technológii nájdeme niekoľko patentov, kde hlavným reprezentantom je Rowe (2010) taktiež je veľakrát skloňovaný skin spektroskop so senzorom Lumidigm.

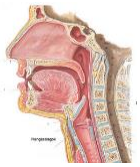
Empiricky: spektrum kože na jednotlivých častiach tela nie je konštantná. Preto pri autentizácii je racionálne testovanú vzorku použiť na konkrétnej časti tela, napr. ako dodatočná kontrola pri snímaní odtlačku prstu.

### 3.6.3 Dynamické biometrické vlastnosti

Dynamické metódy sú založené v zachytení parametrov prejavu (behaviorzimu) konkrétneho človeka v čase. Samotná biometria je statická vlastnosť a prejav subjektu pri vykonávaní činností je dynamická vlastnosť. Niektoré dynamické biometrické meracie systémy vychádzajú zo snímaní statickej aj dynamickej biometrie. Táto časť uvádza niektoré príklady

z možných merateľných biometrií, ktoré by sa dali použiť pre autentizáciu používateľov v rámci ICT. Zhrnuté sú v tabuľke: *Tabuľka 3.3* a zvolené metódy sú vysvetlené podrobnejšie.

*Tabuľka 3.3: Dynamické vlastnosti - charakteristiky behaviorizmu*

| | | | |
|---|---|---|---|
| Pohyb a gestikulácia tváre |  | Dynamika stlačení klávesy |  |
| Zužovanie zreničky/dúhovky, pohyb očí |  | Dynamika dotyku obrazovky |  |
| Pohyby pier |  | Dynamika pohybu kurzoru na displeji |  |
| Hlas/reč |  | Vlastnoručný podpis a jeho dynamika |  |
| Chôdza |  | | |

*Zdroj: vlastné spracovanie (obrázky majú ilustratívny charakter).*

**Pohyb a gestikulácia tváre**

Pri statických biometriách boli spomenuté metódy rozpoznanie tváre. Tie sú mnohokrát kritizované problematikou falšovania tváre. Obísť autentizačný systém v tomto prípade môžeme umiestnením fotografie/videa/masky autorizovanej osoby pred kameru. Tento problém sa môže zredukovať detekciou životnosti osoby pomocou pohybov očí a úst. (Singh, 2014)

Okrem klasického rozpoznania tváre sú snímané aj dynamické prejavy ľudskej tváre, gestikulácie, pohyby očí a úst. Každá z nich musí byť zachytená kamerou po určitú dobu a vyhodnotená špecifickými algoritmami počítačového videnia (Hortai, 2015).

**Chôdza**

Celá metóda pracuje na základe porovnávania kriviek dráh, ktoré opisujú určité body alebo kontúry ľudského tela (Lee, Tan, Tan 2013). Vychádza sa z toho, že každý človek je iný svojim pohybovým, svalovo kostrovým systémom, svojim dynamickým stereotypom, každý chodí inak. Segmentáciu pohybu môžeme snímať v jednoduchej alebo v komplexnej scéne. Detekujú sa dynamiky ťažiska tela a lomových bodov tela (spravidla boky, kĺby: kolenný a členkový). Krivky uvažovaných bodov sú pre jedincov unikátne a vhodné pre porovnávanie a k identifikácii 1:1 (Rak, Porada, 2007).

V literatúre sa môžeme stretnúť pojmom na dynamiku chôdze: „*lokomócia*“ (z anglického *locomotion*) (Straus, Jonák, 2006). Samotná identifikácia na základe chôdze je riešená mnohokrát aj v kriminalistike (Straus et al., 2008).

Tento typ potrebuje vytvoriť vzor časových priebehov pohybu. Výhodou je jednoduché rozmiestnenie kamier na verejných priestranstvách. Nevýhoda je náročné určenie presného biometrického vzoru a možné vplyvy psychického a fyzického stavu jedinca.

**Hlas/reč**

Identifikácia založená na analýze zvuku, vibrácií, výslovnosti a rýchlosti ľudskej reči. Hlasové charakteristiky závisia od veľkosti hlasiviek, úst, nosovej dutiny a ďalších procesoch tvorby hlasu jedinca. Používa sa množstvo príznakov, ktoré možno rozdeliť do dvoch skupín:

- **Štatistické** - nezávislé na texte, pracujú s dlhodobými strednými hodnotami, histogramami, využívajú sa iba znelé segmenty - základný tón (kmitočet) reči, dlhodobé spektrum reči, koeficienty LPC (Linear Predictive Coding), korelačné a kovariančné matice jednotlivých príznakov (Han et al., 2006; Zhu, Yang, 2012 ).
- **Dynamické** - vhodné pre rozpoznanie hovorcu v závislosti od textu, ide o určenie časových priebehov zvolených parametrov reči - základný tón reči, prvé formanty, spektrum, valcový model hlasového traktu atď. (Trevisan et al.,2015).

Niektoré technológie zakladajú rozhodnutie autentizácie na analýze slov i celých viet, ktoré pozná iba autentizovaný hovorca. Dochádza teda k dvojfaktorovej autentizácii na základe rozpoznania reči a overovania znalosti hesla/parafrázy.

**Použitie:**

Používa sa najmä na autentizáciu prostredníctvom zvukovej komunikácie: telefón, prenos hlasu internetovým protokolom VoIP atď. Výhoda je, že netreba implementovať žiadny

dodatočný hardvér. Používateľ hovorí do mikrofónu zariadenia pre neho už známou prijateľnou formou. Nevýhodou je, že verifikácia môže byť ovplyvnená napr. chorobou (prechladnutím, nádchou apod.), psychickým stavom hovorcu, šumom okolia atď.

Možnosti podvrhnutia falzifikátmi: rečové záznamy alebo naučený napodobňovací algoritmus. Rozvoj umelej inteligencie napr. algoritmov umelých neurónových sietí (LeCun, Bengio, Hinton, 2015) okrem rozpoznania reči (Russell, Norvig, 2016. , str. 912-917) umožňujú aj spätné vytvorenie zvukových avatarov osôb, alebo obdobu digitálneho hlasu podľa profilu používateľa. Zo zvukových záznamov sa umelá inteligencia vie „naučiť“ hlas používateľa. Výsledný nastavený algoritmus s napodobneným hlasom používateľa potom umožňuje vysloviť akúkoľvek vetu, ktorú jej zadáme, a to aj s rozličnými intonáciami. Rizikové skupiny sú hlavne tí, ktorých je hlas známy (rádio, TV, apod.). Nedá sa vylúčiť ani záznam na diaľku, kde sa zaznamená dostatočná hlasová vzorka používateľa bez jeho vedomia. Okrem profesionálnych komerčných algoritmov na napodobnenie hlasu človeka sú aj verejne dostupné cez internet, viď napr. Lyrebird (2018) https://lyrebird.ai/

Autor sám má skúsenosti s umelými neurónovými sieťami, a preto aj z vlastnej skúsenosti neodporúča používať túto metódu pre diaľkovú autentizáciu z pohľadu dlhodobého časového horizontu, kvôli neustálemu vývoju umelej inteligencie a špecializovaných HW architektúr (Venkataramani et al., 2018) na ich podporu.

**Dynamika písania na klávesnici**

Technológia sa používala už za druhej svetovej vojny. Britská tajná služba používala túto metódu na overenie autenticity rádiotelegrafických správ svojich špiónov - dynamika úderov pri vysielaní v morzeovke (Ščurek, 2008).

Každý človek píše inak (rýchlosť, čas stlačenia klávesy, dĺžka pauzy atď.) Tento typ je náročný na získanie etalónu – je potrebné vzorku textu opakovane napísať (čím viac slov, čím viackrát, tým sa znižuje chybovosť overenia), tieto metódy sú sumarizované do roku 2011 od autorov (Karnan, Akila, Krishnaraj, 2011).

Výhodou je, že nevyžaduje ďalší hardvér, pretože využíva už implementovaný hardvér (napr. konzola, klávesnica) (Banerjee, Woodard, 2012). Možnosť použitia na verifikáciu používateľa po prihlásení sa do systému a prístupu k chráneným dátam, ochrana počítača pred deťmi, zistenie nezvyčajného chovania sa používateľa.

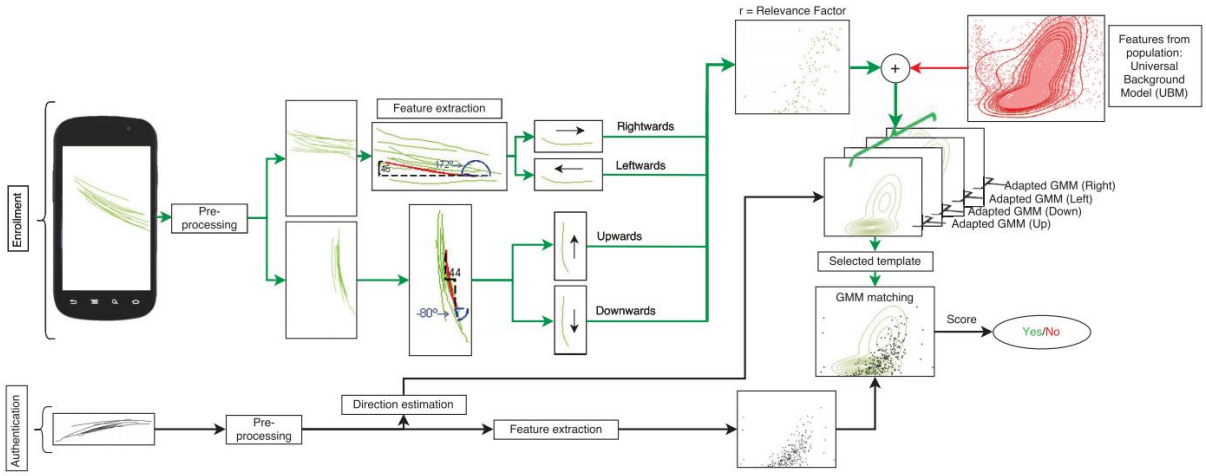
Menej presná metóda (nestálosť písania na klávesnici a vysoké hodnoty FRR). Na dynamiku môže mať vplyv únava alebo stres, pri zranení ruky je táto metóda plne vylúčená (Tresner, Salykin, 2016).

**Dynamika pohybu myší**

Nakreslenie určeného tvaru, ktorý bol nakreslený pri vytváraní etalónu. Obraz je potrebné nakresliť niekoľkokrát. Z nakresleného vzoru sú určené špecifické znaky ako pozícia, rýchlosť ťahu a zaoblenie, ktoré sú následne porovnané s etalónom. Vlastnosti sú podobné ako u dynamiky písania na klávesnici, skôr použiteľné pre dodatočnú verifikáciu (Zheng et al., 2011) po prihlásení.

**Dynamika dotyku obrazovky**

Pri dotykových obrazovkách (napr. pri smartphonoch) sa prejavia behaviorálne znaky osoby pri dotýkaní sa obrazovky (Zhao et al., 2014). Štúdie potvrdili (Pozo et al., 2017; Fierrez et al., 2018), že na základe štatistík interakcií používateľov s dotykovými obrazovkami (napr. frekvencia a trvanie ťahu prstov s dotykovou obrazovkou) by bola možná ich osobitná autentizácia.




*Obrázok 3.4: Ukážka systému vyhodnotenia dynamiky dotyku obrazovky*

*Zdroj: prevzaté zo zdroja (Pozo et al., 2017).*

### 3.6.4 Rukopis, biomechanika pri podpise a dynamický biometrický podpis

Biomechanické procesy podieľajúce sa na produkcii ľudského podpisu sú veľmi zložité a doteraz nie úplne objasnené. Pri značne zjednodušených podmienkach: primárna excitácia je myšlienka vyskytujúca sa v centrálnom nervovom systéme (konkrétne v ľudskom mozgu) pre

cielený pohyb s vopred definovanou intenzitou a trvaním (Bičonský, 1992). Cielený pohyb (alebo plánovaný pohyb) prechádza z miechy na jednotlivé svaly, ktoré sú aktivované v určitom poradí a danou intenzitou. Osoba v dôsledku takýchto aktivácií (sťahovanie a uvoľňovanie) svalov pohybom ramena a rukou držiacou pero hrotom pera zanecháva stopu písacieho nástroja na povrchu papiera – vlastnoručne sa podpíše. Napriek zložitosti a obmedzenému pochopeniu tohto procesu niektoré základné vlastnosti podpisu, konkrétne jeho charakteristické parametre, môžu byť matematicky a výpočtovo popísané a odvodené, a tak čiastočne automaticky reprodukované (Kodl, 2010). Celý dynamický proces podpisu je ale kvôli unikátnosti ľudskej biomechaniky nenapodobniteľný (Smejkal, Kodl, 2014).

Pri analýze podpisu je podstatná skutočnosť, či sa jedná o statické alebo dynamické snímanie vyhodnocovania podpisu. Literatúra rozdeľuje overenie podpisu osôb do dvoch hlavných oblastí. Podľa procesu overenia podpisu sa rozlišujú (Jain et al., 2002; Mates, Smejkal, 2013, str. 316):

- off-line,
- on-line.

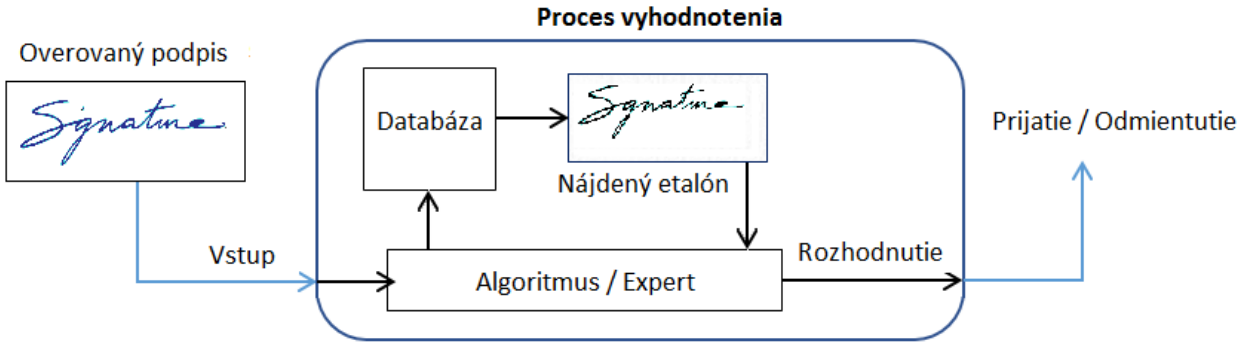
**Off-line systémy pre verifikáciu osôb na základe ich podpisu**

**Postup:** pri off-line metóde sa verifikovaná osoba podpíše klasickým spôsobom na papier. Získaný podpis sa digitalizuje pomocou optického skenera alebo fotoaparátu (Bouamra et al., 2018). Alternatívou digitalizácie podpisu sú tablety alebo iné vhodné nástroje, keď sa verifikovaná osoba podpíše na dotykový display (snímací povrch), alebo príslušným perom (snímač zabudovaný v hrote pera) podobne ako na papier, pričom sa musia zabezpečiť rovnaké podmienky, ako pri klasickom podpise. Z analýzy obrázkov vlastnoručného podpisu (skúmanie vlastností binárnych obrazcov podpisov), sa vyhodnotia jednotlivé charakteristiky podpisu a daným off-line algoritmom sa stanoví jeho pravosť (podobnosť vzorovému podpisu osoby).

**Vytvorenie podpisového vzoru**: každý podpis daného jedinca je jedinečný. To znamená, že každý podpis sa niečím líši a nezhoduje sa na 100 percent s ostatnými podpismi. (Diaz et al., 2015) Preto na vytvorenie referenčného podpisu je doporučené použiť niekoľko vzorov podpisu. Hodnotí sa výsledný tvar podpisu.

**Vyhodnotenie**: vyhodnocuje sa podobnosť obrazu výsledného podpisu overovanej osoby s príslušnou vzorkou podpisu jedinca. Jednotlivé etalóny môžu byť uložené v elektronickej databáze. Pri podpisovaní sa potom hodnotí zhodnosť s referenčným etalónom uloženou

v databáze. Výsledne príslušná aplikácia alebo expert určuje prijatie (zhodu) alebo odmietnutie (nezhodu) podpisu.




*Obrázok 3.5: Off-line vyhodnotenie podpisu*

*Zdroj: vlastné spracovanie.*

**Kritika**: Vyhodnocujú sa výsledné viditeľné informácie a práve to je slabá stránka tohto typu, lebo umožňuje odpozorovanie, napodobnenie podpisu.

Existujú nespoľahlivé metódy, ktoré používajú tento princíp rozpoznávania podpisu a opierajú sa o ľudský faktor v podobe kaligrafického „odborníka“. Bežne sa používajú v oblasti bankovníctva a maloobchodu napríklad na overenie vlastnoručného podpisu osôb (Smejkal, Kodl, 2011).

V posledných rokoch overovacie techniky off-line metód sú postavené na pseudo-dynamických technikách, napr. pomocou umelých neurónových sietí, tzv. „deep learning“ (Bouamra et al., 2018). Výskumníci (Soleimani et al., 2016) použili histogram orientovaných gradientov a diskrétnu Radonovú transformáciu s *Deep Multitask Metric Learning* aby zvýšili výkonnosť overovania podpisov. Iný (Hafemann et al., 2016) zas na základe neurónových sietí typu *Deep Convolutional Neural Networks* (DNN) systém naučili funkcie na vyhodnotenie, ktoré boli výsledne nezávislé od píšucej/podpisujúcej osobe. Táto technika bola potom vyhodnotená na GPDS960 a brazílskych databázach PUC-PR s dôveryhodnými výsledkami. V ďalšej štúdii (Rantzsch et al., 2016) riešili prístup nezávislosti vyhodnotenia od píšucich/podpisujúcich osôb pomocou hlbokého metrického učenia (deep metric learning) a naučili tak vkladanie podpisov do viacdimenzionálneho priestoru. Táto metóda porovnáva triplety: dvoch pravých a jedného falzifikovaného podpisu, za účelom zvýšenia verifikačnej výkonnosti databázy ICDAR SigWiComp 2013. Podobne (Hafemann, Sabourin, Oliveira, 2017) použili konvolučné neurónové siete, aby naučili siete na efektívne reprezentácie z podpisových obrazov v režime nezávislého od píšucich/podpisujúcich osôb. Táto technika

v sebe zahŕňala aj učenie znakov z podskupiny odborných falzifikovaných podpisov. Tento výsledný systém bol vyhodnotený na štyroch súboroch údajov z databáz: GPDS, MCYT, CEDAR a brazílsky PUC-PR, pričom vykazoval konkurencieschopnú výkonnosť z hľadiska miery chybovosti vyhodnotenia.

Zhrnutie známych príspevkov k overeniu off-line podpisu sú prediskutované a hodnotovo reprezentované v (Bouamra et al., 2018, str. 185). Významným výsledkom v citovanom článku je, že pri rozpoznaní pravosti podpisu dosiahli autori touto metódou presnosť približne 93 %, kedy presnosť bola stanovená ako podiel počtu správnych rozhodnutí k celkovému počtu testovaní pri rozhodovaní o pravosti (Malik, 2015). Nimi zistené hodnoty FAR dosahujú cca. 10 % a FRR cca. 4.5 %. Ako konštatujú autori cit. článku, jedná sa o dosiahnutie najlepších výsledkov, získaných s využitím off-line metód overovania podpisov.

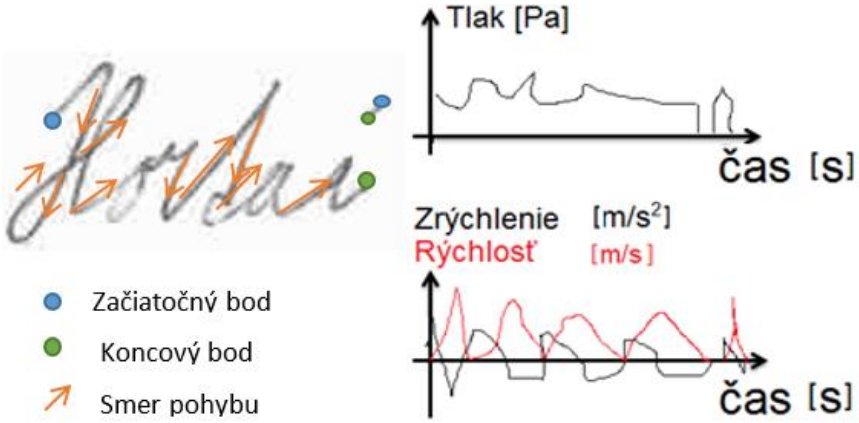
**On-line systémy pre verifikáciu osôb na základe ich podpisu**

Využíva jedinečnosť kombinácie anatomických a behaviorálnych vlastností človeka, ktoré sa prejavia pri podpise. Zahrňuje analýzu viditeľných a neviditeľných informácií podpisu.

On-line systémy využívajú ako statické, tak dynamické informácie o podpise (obraz aj informácie o jeho vytvorení) (Jain et al., 2002; Mates, Smejkal, 2012, str. 316). Z ručného podpisu možno tak elektronicky zistiť napr.: smer, rýchlosť a tlak pri písaní, ktoré sú jedinečné črty každej osoby a dajú sa použiť pre autentizáciu osoby. Na tento druh podpisu sa dá použiť terminológia: **dynamický biometrický podpis** (skratkou **DBP**) a v práci sa používa tento výklad pojmu.

V on-line systémoch sú charakteristiky písaného textu získavané v reálnom čase pomocou špecializovaného tabletu, alebo iného vhodného nástroja (Francis et al., 2015). Verifikovaná osoba sa podpíše na dotykový display (snímací povrch), alebo príslušným perom (snímač zabudovaný v hrote pera) podobne ako na papier. Hodnotí sa dynamika, t. j. celý proces vytvárania podpisu v čase. Základnými dynamickými vlastnosťami podpisu sú rýchlosť, akcelerácia, časovanie, tlak a smer ťahu, ktoré sú zaznamenávané vo viacrozmernom súradnicovom systéme (Galbally et al., 2015). Dva rozmery pohybu podpisu slúžia na určenie rýchlosti a smeru ťahu, tretia súradnica určuje tlak na podložku (Smejkal et al., 2013). Snímacie jednotky od jednotlivých výrobcov sa líšia počtom členov vektoru biometrických informácií (Lopez-Garcia et al., 2014).

Systém po načítaní parametrov podpisu pripojí ďalšie informácie podpísaného dokumentu, ako je používateľské meno, aktuálny čas a dátum atď. Dáta sú potom šifrované a tvoria tzv. biometrickú značku, ktorá je odoslaná na ďalšie spracovanie.




*Obrázok 3.6: Ilustrácia dynamického vyhodnotenia podpisu*

*Zdroj: vlastné spracovanie.*

Technológiou on-line metódou dynamického biometrického podpisu sa zaoberá práca rozsiahlejšie v primárnom výskume. Aby sa obmedzila možná duplicita vysvetlení, je DBP vysvetlený v kapitole zahrňujúcej jej rozsiahlu analýzu (viď kapitoly: 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 a 5.9).

### 3.6.5 Normy ktoré sa vzťahujú na biometrické technológie

Normy, ktoré sa vzťahujú všeobecne na problematiku biometrie sú zhrnuté v nasledujúcej tabuľke:

*Tabuľka 3.4: Zoznam noriem majúce vzťah k biometrii*

| Označenie | Názov | Kat. číslo v ČSN |
|---|---|---|
| ISO/IEC 2382-37 | Information technology –Vocabulary - Part 37: Biometrics | 94239 |
| ISO/IEC 7816-11 | Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods | 71993 |
| ISO/IEC 19792 | Information technology -- Security techniques -- Security evaluation of biometrics | 98483 |
| ISO/IEC 19794-1 | Information technology – Biometric data interchange formats – Part 1: Framework | 92758 |
| ISO/IEC 19794-10 | Information technology -- Biometric data interchange formats -- Part 10: Hand geometry silhouette data | 80434 |
| ISO/IEC 19794-11 | Information technology -- Biometric data interchange formats -- Part 11: Signature/sign processed dynamic data | 98677 |
| ISO/IEC 19794-14 | Information technology -- Biometric data interchange formats -- Part 14: DNA data | 95068 |

| | | |
|---|---|---|
| ISO/IEC 19794-2 | Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data | 93411 |
| ISO/IEC 19794-3 | Information technology -- Biometric data interchange formats -- Part 3: Finger pattern spectral data | 80311 |
| ISO/IEC 19794-4 | Information technology -- Biometric data interchange formats -- Part 4: Finger image data | 77862 |
| ISO/IEC 19794-5 | Information technology -- Biometric data interchange formats -- Part 5: Face image data | 92920 |
| ISO/IEC 19794-6 | Information technology -- Biometric data interchange formats -- Part 6: Iris image data | 92757 |
| ISO/IEC 19794-7 | Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data | 98678 |
| ISO/IEC 19794-8 | Information technology -- Biometric data interchange formats -- Part 8: Finger pattern skeletal data | 94462 |
| ISO/IEC 19794-9 | Information technology -- Biometric data interchange formats -- Part 9: Vascular image data | 92759 |
| ISO/IEC 19795-1 | Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework | 80528 |
| ISO/IEC 19795-2 | Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation | 82417 |
| ISO/IEC 19795-4 | Information technology -- Biometric performance testing and reporting -- Part 4: Interoperability performance testing | 83562 |
| ISO/IEC 19795-7 | Information technology -- Biometric performance testing and reporting -- Part 7: Testing of on-card biometric comparison algorithms | 95291 |
| ISO/IEC TR 19795-3 | Information technology -- Biometric performance testing and reporting -- Part 3: Modality-specific testing | 82418 |
| ISO/IEC 19785-2 | Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority | 89527 |
| ISO/IEC 19785-4 | Information technology -- Common Biometric Exchange Formats Framework -- Part 4: Security block format specifications | 89790 |
| P CEN/TS 16428 | Biometrics Interoperability profiles - Best Practices for slap tenprint captures | 92605 |
| ISO/IEC 24761 | Information technology -- Security techniques -- Authentication context for biometrics | 96250 |
| ISO/IEC 24745 | Information technology -- Security techniques -- Biometric information protection | 96251 |
| ISO 19092 | Financial services -- Biometrics -- Security framework | 82761 |

*Zdroj: vlastné spracovanie.*

### 3.6.6 Diskusia a zhrnutie časti biometrickej autentizácie

Aj keď pri tejto autentizácii používateľ svoju identitu dokazuje svojimi vlastnými charakteristikami vyskytuje sa v nich niekoľko základných problémov. Hrozby predstavujú možné útoky falzifikátmi biometrií. Útočník by mohol predkladať overovacej strane falzifikovaný model (napr. model odtlačkov prstov alebo fotku tváre autorizovaného pracovníka), na ktorom by príslušný senzor zosnímal biometriu, akú má oprávnený používateľ a systém by ho „úspešne“ autentizoval. Autentizácia statickou biometriou ďalej zahrňuje riziko odcudzenia originálu biometrickej vzorky (myslí sa tým napr. odrezanie prstu, ruky alebo iných častí teľa). Ochrana voči takýmto falšovaním/útokom:

- Použiť ťažko vytvoriteľný model biometrie alebo použiť dynamickú biometriu.
- Overiť živosť autentizačného biometrického vzorku (či sa nejedná o maketu). Existuje viacero prístupov, od jednoduchého umiestnenia čítačky do vizuálneho dosahu ľudskej kontroly, až po sofistikované testy živosti – systém vyzve osobu k určitým pohybom alebo meria ďalšie vlastnosti, ako teplotu prstu, tep krvi v žilách alebo elektrický odpor overovanej biometrie.
    - Kontrolou živosti statickej biometrie sa eliminuje riziko používania odcudzeného originálu biometrie. Tu ale ostáva naďalej riziko donútenia použitia hrubou fyzickou silou živej biometrie (napr. pritlačením prstu, ruky alebo hlavy do skeneru). Riziko donútenia použitia hrubou fyzickou silou sa ale nevzťahuje na dynamické biometrie, lebo ich použitie závisí na vôli oprávneného používateľa.

Problémom je aj neexistujúca stopercentná spoľahlivosť a možný vznik chybových stavov. Môže dôjsť chybám, keď je ako platný používateľ vyhodnotený ten, ktorý nemá do systému prístup. Pravdepodobnosť tohto stavu je vyjadrená veličinami:

**FAR - Miera chybného prijatia:**

Pravdepodobnosť, že biometrický systém klasifikuje nesprávne dva odlišné biometrické vzory ako zhodné, a tým zlyhá pri odmietnutí potencionálneho útočníka. Táto chyba patrí k závažnejším, lebo prináša bezpečnostné riziko.

$$FAR = \frac{Počet\ zhodných\ porovnaní\ rozdielnych\ vzorov}{Celkový\ počet\ porovnaní\ rozdielnych\ vzorov} \qquad (1)$$

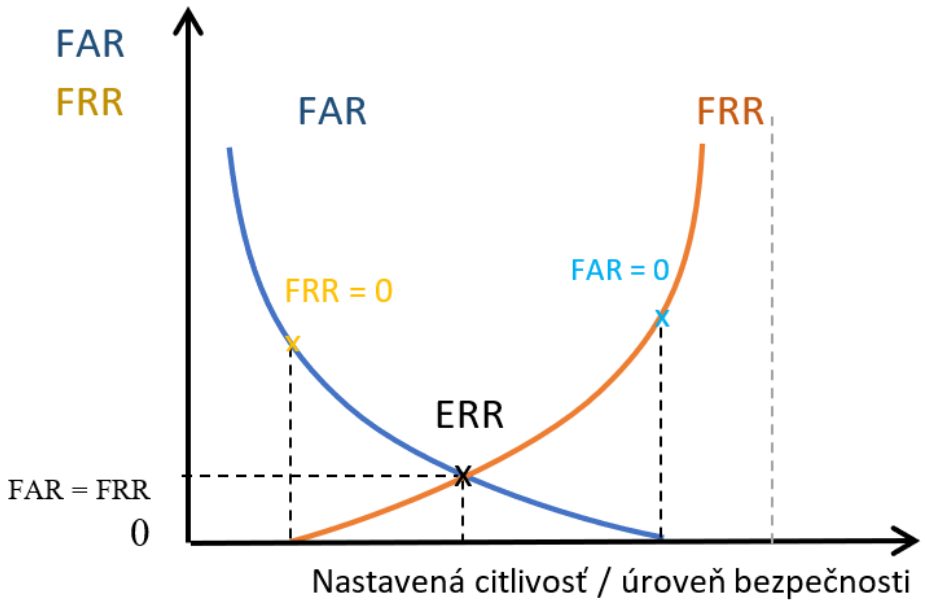
**FRR - Miera chybného odmietnutia:**

Pravdepodobnosť, že biometrický systém klasifikuje nesprávne dva biometrické vzory od rovnakej osoby ako odlišné, a tým zlyhá pri prijatí oprávneného používateľa.

$$FRR = \frac{Počet\ porovnaní\ vzorov\ osoby\ A\ vedúci\ k\ nezhode}{Celkový\ počet\ porovnaní\ vzorov\ osoby\ A} \qquad (2)$$

Každá aplikácia autentizačného zariadenia kladie rozdielne nároky na hodnoty týchto ukazovateľov (Doseděl, 2004). Na predstavu veľkosti týchto čísel som uviedol príklad najnovšej technológie: technológia *Fujitsu PalmSecure* sníma jedinečný obraz krvného riečiska (žíl) v dlani človeka. V internom výskume spoločnosti Fujitsu bola dosiahnutá miera chybného prijatia FAR nižšia ako 0,00008% a miera neoprávnených odmietnutí FRR len 0,01%. Niektoré bankové spoločnosti uvažujú v budúcnosti nahradiť touto technológiou kreditné karty (Fujitsu, 2013).

Mnohé biometrické systémy umožňujú voľbu, alebo nastavenie „úrovne bezpečnosti“. Nastavenie tejto úrovne je pomocou prahovej hodnoty tolerancie prijatia, či citlivosťou systému. Teoretický priebeh závislostí FRR a FAR je znázornený na *Obrázok 3.7*. Reálny priebeh pri konkrétnej technológii sa môže líšiť. Bod ERR (Equal Error Rate) reprezentuje nastavanie, kedy FAR a FRR sú si ekvivalentné. Kde vľavo od ERR je FAR > FAR a vpravo od ERR je FAR < FRR. V praxi FRR a FAR môžu mať síce veľmi malé hodnoty blízkej k 0 ale nikdy nebudú nulové (v reáli je graf na *Obrázok 3.7* FRR a FAR posunutý vertikálne hore a s osou *x* sa nedotýkajú).




*Obrázok 3.7: Teoretický vzťah medzi FRR a FAR*

*Zdroj: vlastné spracovanie podľa* (*Drahanský*, 2007).

Biometrické systémy majú aj ďalšie ukazovatele, napr.:

- **FTA** (Failure to Acquire) – reprezentuje zlyhanie nasnímať vzorku a môže byť vyjadrená mierou neschopnosti nasnímať biometrickú vzorku, t. j. podiel chybných záznamov daného senzora (biometrická charakteristika je prítomná, ale zaznamenanie biometrickej charakteristiky je odmietnuté). Táto hodnota slúži ako miera hodnotenia kvality senzorov.
- **FTE** (Failure to Enrol) (miera neschopnosti zaregistrovania) – reprezentuje zlyhanie úspešne zaregistrovať používateľov a môže byť vyjadrený ako percentuálny podiel používateľov, ktorých systém nebol schopný úspešne zaregistrovať. Miery FTE sa často vyskytujú pri systémoch, ktoré majú kontrolu kvality biometrickej charakteristiky. Nasnímané biometrické charakteristiky s nedostatočnou kvalitou nie sú systémom rozpoznateľné/zaregistrovateľné. V tomto zmysle predstavuje FTE údaj, ktorý hodnotí schopnosť algoritmu pracovať aj s nekvalitnými biometrickými charakteristikami.
- **FTM** (Failure to Match) (miera neschopnosti porovnať vzorku pri používaní, za predpokladu už úspešného procesu zaregistrovania používateľa) – môže byť vyjadrený ako percentuálny podiel biometrických charakteristík, ktoré síce nasnímané boli ale nemohli byť porovnané s etalónom používateľa a/alebo akokoľvek inak zo systémom spracované.

Pre detailnú reprezentáciu indikátorov biometrických systémov viď literatúru napr. (Drahanský et al., 2011; Wayman et al., 2005).

**Výhody biometrií:**

- Odolnosť proti krádeži originálu.
- Niektoré biometrické charakteristiky sa v priebehu života jedinca relatívne nemenia (napr. DNA), alebo prechádzajú len veľmi malou zmenou (žily na ruke).
- Silná metóda, veľké percento spoľahlivosti (v závislosti od metódy a implementácie).
- Žiadateľ má dôkaz identity stále so sebou. Používateľ sa nemusí obávať straty, krádeže karty alebo zabudnutia hesla. Biometriu môže použiť aj negramotná osoba, nie je potrebné pri sebe nič nosiť.
- Možnosť kombinácie s inými faktormi alebo kombinácia viac biometrických metód.

**Nevýhody biometrií:**

- Možná chybovosť systému, vyčíslená hodnotami napr. mierou chybného prijatia (FAR) a mierou chybného odmietnutia (FRR) apod.
- Nutná účasť používateľa pri vytváraní autentizačnej informácie (vytvorenie vzoru biometrie, atď.).
- Možnosti falšovania a slabé miesta biometrických systémov na ktoré treba zabezpečiť:
    - **Na strane senzora**: podvrh falzifikátmi biometrických vlastností. Hlavne statické vzorky (napr. syntetické vzorky odtlačkov prstov, maska napodobňujúca charakteristiky tváre oprávneného používateľa) sú nemenné a dajú sa kopírovať. Neplatí pre skryté dynamické biometrie (viď napr. DBP).
    - **Na strane spracovania/overenia**: modifikácia extraktora (porucha normálnej funkčnosti snímača biometrie); modifikácia šablóny (napr. nastavenie iného tolerančného pásma prijatia ako pri pôvodnom vytvorenom etalóne charakteristiky); zmena porovnania (zmena relácie z pôvodnej charakteristiky na inú charakteristiku v databáze); zámena etalónu v databáze (z pôvodnej charakteristiky na charakteristiku útočníka); blokovanie komunikačného kanála a zmena výsledku overenia (kontrolné zariadenie nemá prístup na databázu etalónov charakteristík a je rušený útokom a zmenou výsledného prijatia, útok napr. „man in the middle“ a pod.)
        - Pre elimináciu tejto hrozby je potrebné zabezpečiť databázu etalónov biometrií, komunikačné kanály overovacích zariadení a snímačov.

# 4 Ciele, výskumné otázky a hypotézy dizertačnej práce

**Ciele dizertačnej práce**

Cieľom dizertačnej práce je návrh konceptu a testovanie metódy autentizácie pre bezpečnú autentizáciu a efektívnu vnútropodnikovú komunikáciu. Ako vhodný nástroj pre túto rolu sa javí technológia, ktorá zahŕňa použitie dynamického biometrického podpisu, preto sa práca s touto tematikou zaoberá podrobnejšie.

Základom daného výskumu bolo navrhnúť relevantné výskumné otázky. Z odpovedí výskumných otázok sa ďalej navrhli špecifické hypotézy a vypracovala sa vhodná metodológia na testovanie hypotéz. Jednotlivé výskumné otázky a hypotézy majú rozdielny charakter, preto aj špecifickú metodológiu a vypracovanie. Výsledným cieľom výskumu je potvrdiť alebo vyvrátiť, že DBP je vhodný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu. Hlavné a výsledné hypotézy práce sú H0.0 a H0.1:

- *H 0.0: DBP je použiteľný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu.*
- *H 0.1: DBP nie je použiteľný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu.*

Odpovede na tieto hlavné hypotézy sú v kapitole *5.10 Súhrn a syntéza primárneho výskumu*. Pre ostatné skúmané hypotézy a výskumné otázky viď referencie v nasledujúcej kapitole.

## 4.1 Výskumné otázky a hypotézy

Výskumné otázky sú zaostrené na význam autentizačných technológií pre podnikovú použiteľnosť a prax. Aby výskum práce mal jednotiaci rámec sú položené výskumné otázky postupne (V.O. s nižším číslom implikovala V.O. s vyšším číslom), a to v nasledovnom poradí:

**V.O. 1. Aké sú možnosti používania autentizačných technológií v organizáciách?**

- Vypracovanie viď v príslušnej kapitole 5.1.2.

**V.O. 2. Čo musia spoločnosti zabezpečiť, aby mohli biometrické systémy používať a sú tieto systémy pre spoločnosti prínosné?**

- Vypracovanie viď v príslušnej kapitole 5.1.3.

**V.O. 3. Sú vhodnejšie použiť statické alebo dynamické biometrie komunikáciu v podniku?**

- Vypracovanie viď v príslušnej kapitole 5.1.4.

**V.O. 4. Ktorá dynamická metóda je najvhodnejšia pre komunikáciu v podniku?**

- Vypracovanie viď v príslušnej kapitole 5.1.5.

**V.O. 5. Aké sú aspekty spojené s používaním DBP?**

Výskumná otázka 5 odpovedá na možné delenie aspektov, ktoré sa vzťahujú konkrétne na dynamický biometrický podpis. Vypracovanie viď v príslušnej kapitole 5.1.6. Jednotlivé podotázky (1 až 7) V.O. 5 formulujú konkrétne hypotézy, ktoré sú testované v časti primárneho výskumu a sú nasledovné:

**V.O. 5.1 Aký je legislatívny aspekt a normy DBP?**

Vypracovanie a metodológia výskumnej otázky viď v príslušnej kapitole 5.3.

**V.O. 5.2 Aký je aspekt operačnej analýzy DBP?**

Vypracovanie a metodológia výskumnej otázky je v príslušnej kapitole 5.4, kde bola zodpovedaná ako aj nasledujúca hypotéza:

- H 5.2.I: DBP je možné zefektívniť podnikové procesy a urýchliť komunikáciu.

**V.O. 5.3 Aký je ekonomický aspekt DBP?**

Vypracovanie výskumnej otázky viď v príslušnej kapitole 5.5.

**V.O. 5.4 Aký je spoločenský a používateľský aspekt DBP?**

Vypracovanie výskumnej otázky viď v príslušnej kapitole 5.6, kde boli zodpovedané ako nasledujúce V.O. a hypotézy:

- H 5.4.I: Subjektívne je kybernetická bezpečnosť dôležitá pre ľudí alebo pre spoločnosti.
- H 5.4.II: Subjektívne si ľudia myslia že majú znalosti o kryptografických technológiách.
- H 5.4.III: Ľudia majú reálne znalosti o kryptografických technológiách.
- H 5.4.IV: Ľudia vedia aký je rozdiel medzi elektronickým rozpoznaním vlastnoručného podpisu ako obrázka a DBP.
- V.O. 5.4.1: Je potrebné oboznámiť ľudí v prípade implementácie DBP?

- V.O. 5.4.2: Po neutrálnom oboznámení je pre ľudí DBP prijateľný?

**V.O. 5.5 Aký je technologický aspekt DBP?**

Merania a vypracovanie indukovaných hypotéz prosím viď na príslušnej kapitole 5.7. Nasledujúce hypotézy boli formulované:

- I. časť predpokladala, že pokusné osoby sa rôzne ťažko vyrovnávajú s meniacimi sa okolnosťami podpisu v závislosti na technickom prevedení snímača:
  - H 5.5.I.0 - stabilita podpisov pre danú osobu na jednotlivých zariadeniach sa podstatne nemení (priemer a rozptyl miery zhody podpisov pre každé zariadenie patrí do rovnakého základného súboru),
  - H 5.5.I.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri jednotlivých zariadeniach pre danú osobu.
- II. časť predpokladala, že stabilita podpisov dosahovaná na jednotlivých zariadeniach sa bude štatisticky významne odlišovať.
  - H 5.5.II.0 - priemerná miera a rozptyl zhody podpisov pre jednotlivé snímače sa podstatne nemení (priemer a rozptyl miery zhody podpisov pre každé zariadenie patrí do rovnakého základného súboru),
  - H 5.5.II.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri jednotlivých zariadeniach.

**V.O. 5.6 Aký je technologicko-používateľský aspekt pri DBP?**

Táto časť sa zameriava na možné vplyvy okolností na používateľov pri vytváraní DBP (viď kapitolu 5.8) . Nasledujúce hypotézy a výskumné otázky boli formulované:

- I. časť predpokladá, že celková stabilita podpisov dosahovaná pri jednotlivých pozíciách tela signatára sa budú štatisticky významne odlišovať.
  - H 5.6.I.0 - priemerná miera a rozptyl zhody podpisov pre jednotlivé pozície sa podstatne nemenia (priemer a rozptyl miery zhody podpisov pre každú pozíciu patrí do rovnakého základného súboru),
  - H 5.6.I.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri niektorých pozíciách.
- II. časť V prípade prijatia alternatívnej hypotézy sú skúmané výskumné otázky:

- V.O. 5.6.I Ktoré pozície sú si ekvivalentné z pohľadu podpisovej stability? Pozície, kde priemer a rozptyl miery zhody podpisov patrili do rovnakého základného súboru.
- V.O. 5.6.II Aký exogénny faktor spôsobil rozdiel pri stabilite podpisu u signatára?
- V.O. 5.6.III Je stabilita skôr závislá na exogénnych faktoroch, alebo skôr na individuálnych charakteristikách signatára?

**V.O. 5.7 Aký je aspekt možných rizík zneužitia DBP?**

Táto časť skúma aspekt možných rizík zneužitia a používania DBP (viď kapitolu 5.9). Konkrétne sa zameriava na riziká falšovania DBP a použiteľnosť v praxi. Nasledujúce hypotézy a výskumné otázky boli formulované:

- Hypotézy časti I. predpokladajú, že miera schopnosti napodobňovania podpisov je u každej osoby rovnaká pre všetky podpisy.
  - H 5.7.I.0 – Každý podpis je pre jednotlivcov rovnako ťažké napodobniť.
  - H 5.7.I.1 – Každý podpis je pre jednotlivcov rôzne ťažké napodobniť.
- Hypotézy časti II. predpokladajú, že rozdielne podpisy je rôzne ťažké napodobniť.
  - H 5.7.II.0 – Podpis A a B sú rovnako ťažko napodobniteľné.
  - H 5.7.II.1 – Podpis A a B sú rôzne ťažko napodobniteľné.
- Hypotézy časti III. predpokladajú, že miera zhody medzi pravým podpisom a jeho falzifikátom je priamo úmerná počtom pokusov o napodobnenie.
  - H 5.7.III.0 – Existuje štatisticky významná korelácia a regresia medzi počtom pokusov o napodobenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho napodobnením.
  - H 5.7.III.1 – Korelácia a regresie medzi počtom pokusov o napodobnenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho falzifikátom nie sú štatisticky významné.
- Výskumná otázka na stanovenie miery zhody podpisu.
  - V.O. 5.7.II.1 – Aká má byť stanovená miera zhody podpisu aby bol DBP považovaný za pravý?

# 5 Vyhodnotenie analýzy a výskumu

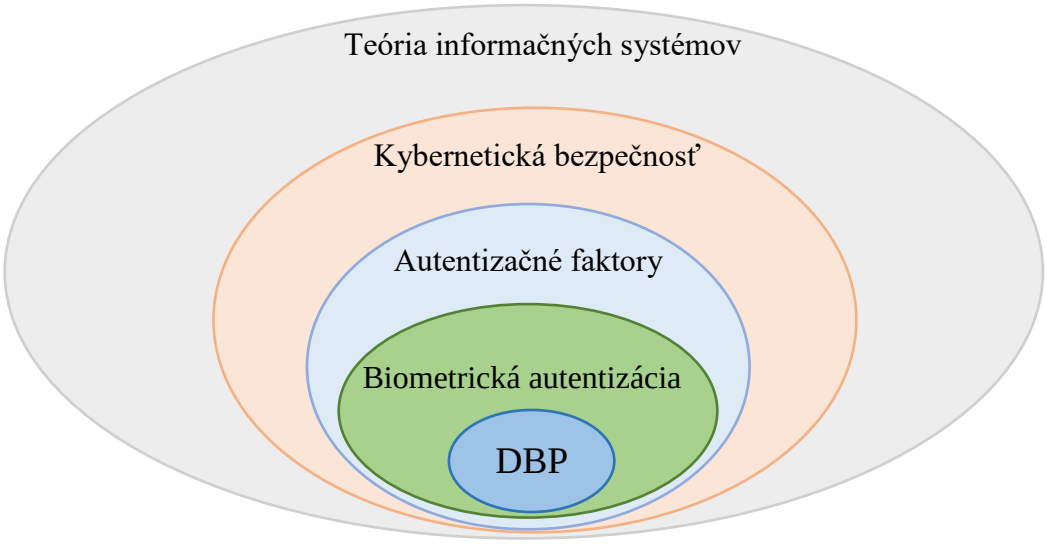
## 5.1 Vypracovanie sekundárneho výskumu V.O. 1 až 5

### 5.1.1 Metodológia sekundárneho výskumu

Nové ľudské poznatky prinášajú hrozby zneužitia a odcudzenia aktív a identity subjektov, a to hlavne pri komunikácii v ICT. Sekundárny výskum čerpá z viac ako zo dvesto zdrojov publikácií a vedeckých prác na objasnenie možností IS a bezpečnej autentizácie používateľov. Popisné štúdie definujú vzory a trendy v ICT a vnútropodnikovej komunikácie. Vzhľadom na charakter témy sú získavané poznatky zo zahraničnej a tuzemskej vedeckej literatúry, zo svetovej a tuzemskej legislatívy a súvisiacich noriem.

Sekundárny výskum je syntéza analyzovaných zdrojov a odpovedá na výskumné otázky číslom: 1, 2, 3, 4, 5 a z časti indukuje V.O. 6 (ktorá je ďalej riešená v primárnom výskume). Práca vychádza zo všeobecnej teórie informačných systémov. Výskum skúma autentizačné možnosti používateľov, autorizáciu a riadenie prístupu. Analyzujú sa možnosti autentizácie, ich zdroje údajov a typ použitej technológie. Analýza tiež zahrňuje varianty rizík u autentizácii a u autorizácie pri osobnom styku a v prípade komunikácie bez osobného styku typu komunikácia na diaľku pomocou informačných a komunikačných technológií. Všeobecné prístupy k možnostiam autentizácie sú pomocou informácií na základe znalosti, na základe vlastníctva, na základe charakteristiky používateľa. Autentizačné faktory a ich typy možno kombinovať medzi sebou pri autentizácii. Základ práce tvorí analýza výhod a úskalia autentizačných faktorov, ktoré sú výsledne vyhodnotené komparatívnou metódou.

V teoretickej časti sa vychádza zo širšieho pojmu a postupne sa zužuje spektrum na rozpoznávanie subjektu na báze signatúry a použitia dynamického biometrického podpisu (viď *Obrázok 5.1*).




*Obrázok 5.1: Metafora cibule a nastoľovanie agendy*

*Zdroj: vlastné spracovanie.*

**Topológia sekundárneho výskumu**

Pre vypracovanie sekundárneho výskumu sa použila nasledujúca topológia metodiky v logicky nadväzujúcom poradí:

- Deskripcia pojmov a vysvetlenie použitých skratiek.
- Fáza rešeršného a analytického prístupu:
    - Zber dostupných a relevantných údajov a informácií.
        - Analýza autentizačných faktorov a metód autentizácie.
        - Viacfaktorová autentizácia.
        - Výhody, nevýhody a praktické použitie autentizačných systémov.
        - Pochopenie problematík autentizácie.
    - Analýza údajov a informácií.
        - Filtrácia dôležitých informácií podľa relevancie (vzťah k téme, impakt zdroja, aktuálnosť zdroja).
        - Komparácia autentizačných faktorov a metód.
        - Skúmanie relevantnej legislatívy a noriem.
        - Skúmanie z hľadiska praktického využitia.
        - Dedukcia analýzy.
        - Odpovede na výskumné otázky.

### 5.1.2 V.O. 1. Aké sú možnosti používania autentizačných technológií v organizáciách?

Možnosti autentizácie sú rôznorodé. Hlavné delenie by mohlo byť do autentizačných faktorov, ktoré ich delia podľa charakteru vyžiadaných údajov. Jednotlivé autentizačné faktory združujú veľa rôznych metód, ktoré sa dajú navzájom kombinovať. Pri voľbe autentizačnej metódy je dôležité použiť vhodnú technológiu, ktorá je na daný cieľ primeraná. Dôležitosť autentizácie používateľov závisí od toho, o aké aktívum sa jedná a aké riziko znáša zneužitie alebo strata daného aktíva. Zvyšujúcim rizikom by sa mala zvyšovať aj bezpečnosť autentizácie.

Pri rozhodovaní autentizačného systému treba mať nadhľad na celok systému a brať ohľad na: autorizáciu, možnú identifikáciu entít a bezpečnostné politiky organizácií. Zvolené metódy autentizácie by mali spĺňať požiadavky na variabilitu ako z pohľadu použitých technológii a systémov, tak aj z hľadiska samotných používateľov. Navrhované riešenie musí navyše vychádzať z práva jednotlivých strán na komunikáciu medzi oprávnenými účastníkmi a v prípade úradných alebo bankových operácií spĺňať požiadavky na uzavretie riadneho kontraktu či vykonanie transakcie.

Autentizácia a autorizácia v informačných systémoch a pri elektronických dokumentoch sa v praxi stretáva s niekoľkými protichodnými požiadavkami: na používateľskú jednoduchosť, rýchlosť overovania, bezpečnosť, vierohodnosť a náklady. Preto nasledujúca argumentácia vysvetľuje výber autentizačnej technológie.

Heslá sú ľahko distribuovateľné. Možno sa ich relatívne ľahko zmocniť, sú prenositeľné a odpozorovateľné. Heslá možno použiť iba na najnižší stupeň zabezpečenia. Doporučené je pri ich používaní v časových intervaloch meniť. Tokeny možno použiť pre vyššie stupne zabezpečenia. Je možné sa ich zmocniť alebo stratiť. Kombináciu tokenu a hesla je možné použiť pre pomerne vysoký stupeň zabezpečenia. Kombinácia je značne odolná pri odcudzení alebo strate tokenu, avšak opäť môže zlyhať ľudský činiteľ a dôjsť k „nechcenému“ prezradeniu hesla alebo zapožičaniu tokenu (sú prenositeľné). Predmety môžu byť zabudovateľné do ľudí, ale tento spôsob neprináša žiadne výhody čo by nemala autentizácia pomocou biometrie. Biometrické znaky človeka sú neprenosné, a tak ich nemožno stratiť ani odovzdať. Pri používaní biometrie je potrebné biometriu najprv nasnímať a vytvoriť vzor biometrie. Autentizačné implantáty a statické biometrie prinášajú životu nebezpečnú hrozbu krádeže originálu. Preto pri statickej biometrii je doporučené kontrola živosti vzorky. Táto

hrozba je eliminovateľná použitím dynamickej biometrie, ktorá je neprenosná, kvôli unikátnosti biomechaniky neukradnuteľná.

Z analýzy práce je možno konštatovať, že každý typ zabezpečenia je možné podrobiť útokom. Tieto hrozby možno znížiť použitím jednotlivých autentizačných metód vo vzájomných kombináciách. Z týchto dôvodov je dôležité sa zamerať na multifaktorovú autentizáciu s použitím biometrických metód. Kombinácia mnohých metód autentizácie ale povedie k rastu nákladov a zvýšenej miere interakcie používateľa.

### 5.1.3 V.O. 2. Čo musia spoločnosti zabezpečiť, aby mohli biometrické systémy používať a sú tieto systémy pre spoločnosti prínosné?

Nároky pri biometrickom autentizovaní sú kladené na merateľnú telesnú vlastnosť. Musí sa jednať o vlastnosť, s ktorou disponujú všetci používatelia uvažovaného autentizačného systému. Je vhodné vybrať vlastnosť, ktorá je ľahko merateľná, je relatívne nemenná v čase a jeho meranie je používateľsky prívetivé (komfortné, známe) a prijateľné (súhlas s používaním).

Pre požitie v praxi je ale potrebné prihliadnuť na platnú legislatívu aby správcovia osobných údajov mali informácie o správnom postupe, ktorý nebude v rozpore so všeobecným nariadením a aktuálnym stanoviskom krajiny k biometrickým údajom. Používanie biometrických informácií je regulované v tuzemsku (v SR aj v ČR) zákonom o ochrane osobných údajov a v Európskej únii všeobecne s GDPR (General Data Protection Regulation) (viď kapitolu *1.2.1 Biometria a biometrický údaj*)

Biometrické technológie, sú stále viac a viac dostupnejšie (z pohľadu technickej aj finančnej stránky) ale nie sú úplnou náhradou všetkých bezpečnostných riešení. Spoločnosti pri zaobstarávaní biometrických systémov musia posúdiť primeranosť konkrétneho riešenia (posúdiť účinnosť biometrických systémov) spoločne s rizikami s nimi spojenými, pričom musia vhodne kombinovať biometrický systém s ďalšími bezpečnostnými opatreniami na elimináciu/redukciu hrozieb, ktoré inštaláciou a používaním takýchto systémov úzko súvisia.

Preto voľba zavedenia/používania biometrických systémov musí byť opodstatnená (napr. rýchlejšia prevádzka) a súčasne musia byť vyriešené ďalšie vplyvy dotknutých osôb (napr. zamestnanci, klienti). Pri používaní biometrie je potrebné venovať osobitnú pozornosť napr. u detí v školách. Tu sa jedná o výnimočné prípady, keď nie je daný zákonný titul pre

spracovanie údajov a bude nutné dodržať pravidlá pre získanie súhlasu so spracovaním osobných údajov od každej dotknutej osoby. (Úřad pro ochranu osobních údajů, 2018)

Pri biometrickej autentizácii je prvotné určiť šablón/vzor vzorky používateľa (zaregistrovať biometriu ku konkrétnej identite), ktorá vyžaduje účasť a súhlas používateľa pri vytváraní autentizačnej informácie nasnímaním originálu (vytvorenie vzoru biometrie). Ďalej pri používaní biometrických systémov je potrebné používať kompatibilný HW (napr. snímače, overovacie algoritmy). Jednotlivé biometrie sa dajú kombinovať pri autentizácii. Pri kombinácii veľkého množstva biometrických charakteristík pri autentizácii sa celková chybovosť overenia (hodnoty FAR, FRR apod.), môže kumulovať. Ako príklad uvádzam dvojnásobnú autentizáciu pomocou rozpoznania tváre a hlasu, kde sa chybovosti rozličných biometrických metód (napr. pravdepodobnosť nesprávneho odmietnutia) snímačmi či nesprávnym vyhodnotením môže kumulovať (je prijatá prvá biometria ale druhá bola odmietnutá/nerozpoznaná).

Celkovo ale zavedenie/používanie biometrických technológií môže byť prínosné v organizáciách. Odôvodnenia:

- Biometrickými údajmi disponujú všetky živé bytosti. Biometriu môže použiť aj negramotná osoba, nie je potrebné pri sebe nič nosiť, lebo používateľ má dôkaz identity stále so sebou. Biometrické znaky človeka sú neprenosné, a tak ich nemožno stratiť ani odovzdať (za predpokladu štandardného používania).
- Sú odolné proti krádeži originálu (výnimkou sú extrémne prípady, preto je doporučená kontrola živosti biometrie, alebo použitie dynamickej biometrie).
- Niektoré biometrické charakteristiky sa v priebehu života jedinca relatívne nemenia (napr. DNA), alebo prechádzajú len veľmi malou zmenou (napr. odtlačky prstov, žily na ruke).
    - Niektoré biometrie sa ale môžu meniť, napr. vplyvov chorôb (napr. diabetes vplýva sietnicu oka), zmenou priezviska pri podpise apod. Výskumy ale kvôli časovej náročnosti sa k tomu aktívne nevenujú a z pohľadu praxe sa to dá kompenzovať znovu nasnímaním a zaregistrovaním aktuálnej biometrickej vzorky (etalónu).
- Silná metóda umožňujúce veľké percento spoľahlivosti (v závislosti od metódy a implementácie).

- Možnosť kombinácie s inými faktormi alebo kombinácia viac biometrických metód. Biometrické znaky človeka možno použiť ako autentizáciu pre najvyšší stupeň zabezpečenia.

**Praktický príklad použiteľnosti:**

Spoločnosti z rôznych oblastí môžu používať napr. biometrický dochádzkový systém. Zamestnanci so svojim súhlasom si vďaka nemu môžu evidovať dochádzku napr. priložením prsta k dochádzkovému terminálu (napr. namiesto zamestnaneckej karty). Takáto evidencia dochádzky je veľmi pohodlná a spoľahlivá. Zamestnanci si nemusia pamätať heslá a PIN-y, nosiť zamestnanecké karty dokonca ani kľúče. Biometrická autentizácia vie rýchlo overiť, či je zamestnanec oprávnený vstúpiť do budovy, zaznamená jeho príchod alebo odchod a vykoná následný úkon, napr. otvorí mu dvere. Systém môže spravovať, merať a vykazovať všetky aspekty týkajúce sa dochádzky do zamestnania, pracovnej doby, potenciálnych služobných ciest, plánovania dovolenky, dĺžka obedňajšej prestávky a mnoho ďalšieho.

### 5.1.4 V.O. 3. Sú vhodnejšie použiť statické alebo dynamické biometrie?

Statické biometrické vzorky je dnes možné pomerne ľahko falšovať (podvrhy falzifikátmi/kópiami originálnych biometrií). Autentizácia statickou biometriou zahrňuje riziko odcudzenia originálu biometrickej vzorky (myslí sa tým napr. odrezanie prstu, ruky alebo iných častí teľa). Toto drastické autentizačné riziko nemusí byť prijateľné pre používateľov. Toto riziko by sa dalo eliminovať sekundárnou kontrolou živosti autentizačného biometrického vzorku. Kontrolou živosti subjektu problém ostáva naďalej, a to riziko donútenia použitia statickej biometrie hrubou fyzickou silou (napr. pritlačením prstu, ruky alebo hlavy do skeneru).

Kvôli zmieneným rizikám sa do centra pozornosti dostali metódy dynamické (Tabuľka 3.3), ktoré spočívajú v zachytení parametrov prejavu konkrétnej osoby v čase. Tieto charakteristické znaky sú dané fyziomotorickými vlastnosťami osoby, nie sú od nich oddeliteľné a ich odpozorovanie je vzhľadom ku skrytosti jednotlivých parametrov prakticky nemožné.

### 5.1.5 V.O. 4. Ktorá dynamická metóda je najvhodnejšia pre komunikáciu v podniku?

Jednoduchá otázka sa rozuzlila na komplexnú odpoveď: každá autentizačná metóda má svoje silné stránky (napr. jednoduchosť používania, lacná implementácia) a slabé stránky (napr. riziká prelomenia, konkrétne napodobniteľosť alebo možnosti odcudzenia identifikátora).

Z V.O. 3 vyplýva, že výsledné rozhodnutie zvolenej hlavnej autentizačnej metódy bude z množín dynamických biometrií (viď: Tabuľka 3.3).

Výskumná otázka nedefinuje konkrétne okolnosti používania, preto sa stanovili empirické podmienky pre použitie v organizáciách v praxi. Z teoretického východiska sa usudzuje optimálny prístup pre autentizáciu a použitie jedného z najvýznamnejších prírodných biometrických metód autentizácie. Pre okolnosti pre použitie na vnútropodnikovú komunikáciu sa postupne argumentovali a eliminovali metódy podľa nasledujúcich empirických podmienok:

- Proces nepretržitosti pri procesu autentizácie.
- Použiteľná nezávisle od priestoru a miestnosti.
- Používateľsky prívetivá a prijateľná metóda.
- Test živosti subjektu a možnosť automatizovaného testovania na diaľku.
- Vhodná na elektronickú aj na listinnú formu komunikácie.

**Proces nepretržitosti pri procesu autentizácie:**

Všeobecne: pri statických systémoch môžu byť veličiny jednoznačne určené okamžitými hodnotami riadiacich/vstupných veličín, na rozdiel od toho pri dynamických systémoch, ktorého výstup (stav) je závislý nielen na okamžitých hodnotách vstupov ale aj na predchádzajúcich hodnotách vstupov a stavov (závislá na hĺbke pamäte) (Strogatz, 2001).

Čím väčší čas je snímaný, tým presnejšie by mohol byť systém (v tomto prípade osoba) identifikovaný. No predstava že by používateľ mal byť dlhší čas sledovaný pri autentizácii je absurdita (časová náročnosť). Dlhší čas sledovanosti naviac integruje chybu okolitých podmienok, a tak sa prejavujú známky prerušenia rutinných správaní autentizovanej osoby, ktorého by systém vyhodnotil ako falošného používateľa (v prípade neznalosti okolností). Pretržitý proces by mohol byť pri chôdzi zakopnutie (metóda už eliminovaná), alebo oslovenie inou osobou, náladové prejavy, nápad neštandardnej myšlienky: písanie na klávesnici, dynamika pohybu myší, dynamika dotyku obrazovky sú metódy, ktoré sa týmto spôsobom eliminujú. Z časti by sa mohli eliminovať aj metódy: gestikulácia tváre, zužovanie zreničky/dúhovky, pohyb očí, pohyby pier, na ktoré majú okolnosti tiež veľký vplyv. Zmienené metódy v praxi tiež vykazujú väčšiu chybovosť a preto sú skôr doporučené ako doplnkové (napr. kontrola živosti subjektu) a nie ako hlavné autentizačné metódy.

Preto ako hlavnú autentizačnú metódu pre vnútropodnikovú komunikáciu je vhodné použiť metódu autentizácie, ktorá sa dá uskutočniť naraz a nevyžaduje dlhšiu dobu pozorovania, napr. DBP, ktorý je daný dobou podpisovania (niekoľko sekúnd).

**Použiteľná nezávisle od priestoru a miestnosti:**

Presné určenie dynamiky chôdze je potrebné doladiť okolnosti snímania (napr. miestnosť a uhol snímania kamery) aby bola chôdza osoby snímateľná v dostatočnej kvalite. Empiricky: predstava požiadať zamestnanca aby vstal v kancelárii a pred kamerou chodil hore-dole je absurdné, pričom kancelárske miestnosti nie sú prispôsobené na snímanie chôdze pre jednoznačné určenie identity osoby a preto nevhodné na snímanie tejto biometrie. Dynamika chôdze je preto eliminovaná ako možná hlavná autentizačná metóda pre používanie na komunikáciu v podniku.

Interaktívne použitie hlasu/reči je nepoužiteľné pri šume/hluku (napr. open space office) a zbytočne by spôsoboval ďalší hluk, ale aj znemožnil diskrétne jednanie pri autentizácii. Pre presné určenie identity je táto metóda náchylná na zdravotný stav subjektu (napr. nádcha, kašeľ). Samotné rozpoznanie reči by mohla byť používaná na operatívne úkoly (napr. rozkazovanie, alebo písanie namiesto klávesnice), pri autentizácii by mohla byť použiteľná napr. na kontrolu oprávnenia vstupu do miestnosti. Táto metóda autentizácie je skôr nevhodná pre použitie na vnútropodnikovú komunikáciu pri distančnej komunikáciu skrz IS.

DBP sa dá použiť nezávisle od priestoru (interiér, exteriér). Stačí sa na snímač podpísať, kde neruší okolitý hluk a je zaručená diskrétnosť pri podpise (napr. pri možnosti open space office).

**Používateľsky prívetivá a prijateľná metóda:**

Jedná sa o subjektívnu záležitosť každého jedinca. Empiricky: vyzývať používateľov robiť grimasy (gestikulácia tváre), vyplazovať jazyk, robiť pohyby pier alebo reagovať očami nemusí byť prívetivé (napr. môže predstavovať neseriózność). Tieto metódy by sa dali použiť skôr ako doplnkové (hlas/reč + snímanie kamerou pohyb pier ako kontrola živosti používateľa).

Metódy rozpoznania hlasu/reči sú dobre známe pre ľudí, lebo sa používa pri komunikácii v priamom styku (napr. pri rozhovore u viac ľudí). Táto metóda je pri nemých ľudí alebo pri ľuďoch s problémami s hlasivkami nepoužiteľná.

Podpis je dobre známy pre širokú verejnosť a ľudia sú zvyknutí na túto formu potvrdenia identity (napr. podpísanie zmluvy, prevzatie balíka apod.).

**Test živosti subjektu a možnosť automatizovaného testovania na diaľku:**

Všetky dynamické biometrie v prípade overenia na diaľku sú vystavené riziku falšovania/napodobnenia identity. Kvôli skrytým a neviditeľným parametrom sú ale ťažko reprodukovateľné, lebo potenciálni falšovatelia nemajú dostupné údaje na napodobnenie (napr. ako verejne snímateľné statické biometrie tvár, apod.), viď V.O. 3. Nad rámec tohto všeobecného rizika je hlas/reč verejne nahrateľná a prenášateľná cez komunikačné kanály, a preto umožňuje podvrhy zvukovými záznamami, softwarovým napodobnením atď., ktoré predstavujú vysoké bezpečnostné riziko. V tomto prípade test živosti by sa dal uskutočniť interaktivitou autentizujúcej sa osoby. Táto interaktivita ale je na vzdory vyššie uvedených podmienok (použiteľná nezávisle od priestoru – okolitý šum, hluk; proces nepretržitosti – môže byť prerušený; prijateľnosť pre používateľov – odpovedať na otázky osobného charakteru dokazovaním faktoru znalosti a v tomto prípade aj časová náročnosť).

V prípade písaného textu je test živosti daná písaným osoby. Riziko skôr predstavujú možné falzifikáty podpisov.

**Vhodná na elektronickú aj na listinnú formu komunikácie.**

Autenticitu obsahu elektronických dokumentov vie IS zabezpečiť (za predpokladu že IS je zabezpečení proti útokom). V tom prípade keď je potrebné mať obsah dokumentu aj v listinnej podobe je potrebné ho vytlačiť. V prípade keď je potrebné zabezpečiť autenticitu dokumentu aj naďalej, je možno ho evidovať evidenčným číslom dokumentu (aj číslom verzie dokumentu) a sprístupniť ho cez internet napr. cez cloud systém. V prípade podpísaného dokumentu na znázornenie identity používateľa okrem mena a priezviska vie DBP znázorniť napr. výsledný obraz podpisu. Listinná podoba v prípade znázornenia hlasu sú možnosti limitované a je absurdita predložiť snímku tváre podpísanej osoby namiesto jeho podpisu.

**Voľba optimálnej dynamickej biometrie pre vnútropodnikovú komunikáciu**

Všeobecne: všetky biometrické autentizačné metódy majú svoje výhody aj úskalia. Kvôli zmieneným rizikám V.O. 3 (viď kapitolu 5.1.4) sa do centra pozornosti dostali metódy dynamické (Tabuľka 3.3). Preto pre vnútropodnikovú komunikáciu ako hlavná autentizačná metóda bola zvolená z množiny dynamických biometrických metód.

Z argumentácie tejto V.O. vyplýva, že pre vnútropodnikovú komunikáciu je racionálne zvoliť práve DBP v on-line režime, ktorý je pre organizácie ideálny nástroj pre autentizáciu pri právnych rokovaniach a dokumentoch.

Podpis je prirodzený, ľahko dostupný, používateľom dobre známy nástroj pre preukázanie svojej identity. Výhoda DBP oproti ostatným dynamickým autentizáciám je, že podpis môže byť použitý hneď pri autentizácii. Na autentizáciu nie je potrebný špeciálny priestor alebo dlhší čas pozorovania (ako napr. pri dynamike písania na klávesnici, dynamika pohybu myší apod.). Proces podpisu je pri podpisovaní nepretržitý, osoba sa podpíše a ostatné procesy pokračujú po dokončení podpisu. Pri osobnom styku je živosť pri podpise samozrejmá. Pri komunikácii na diaľku môžeme predpokladať axióm, že každý podpis je jedinečný (empiricky: aj 2 podobné podpisy pri vytváraní nikdy nebudú 100% identické). Raz použitý a evidovaný podpis sa už nedá použiť ešte raz, vždy sa predpokladá odchýlka v rámci tolerancie.

K zabezpečeniu vyššej bezpečnosti a kvôli eliminácii autentizačných nezhôd iným subjektom ako overovaným sa predpokladá porovnanie biometrického podpisu 1 ku 1. Overovaný podpis sa porovnáva konkrétnym podpisom danej overovanej osoby. Predbežná identifikácia overovaného subjektu je daná menom podpisujúcej osoby, alebo s menom prihláseného používateľa pracovnej stanice (PC, tablet apod.). Alternatívou je automatické rozpoznania používateľa: načítanie ID z karty, tokenu alebo iného autentizačného premetu (dosiahnutie dvojfaktorovej autentizácie).

Ako všetky biometrie sú vystavené riziku podvrhmi falzifikátom pri autentizácii. Podpis, v zmysle výsledný obraz podpisu je odpozorovateľný, a preto napodobniteľný. Empiricky je ale možné predpokladať, že napodobniť celý dynamický proces podpisu je omnoho ťažšie, ako napodobniť iba výsledný obraz podpisu. Riziko optického odpozorovania výsledného obrazu podpisu je preto eliminovateľný použitím DBP v on-line režime. On-line režim sníma charakteristiky písaného textu v reálnom čase, t. j. sú snímané behaviorálne vlastnosti človeka (dynamická biometria), ktoré sa prejavia pri podpise. DBP v on-line režime sníma celý proces vytvárania podpisu, ktorý z výsledného obrazu podpisu nie je zrejmý. Preto stanovenie falzifikovateľnosti sa indukoval výskum v primárnom výskume na skúmanie možností napodobnenia DBP v on-line režime.

### 5.1.6 V.O. 5. Aké sú aspekty spojené s používaním DBP?

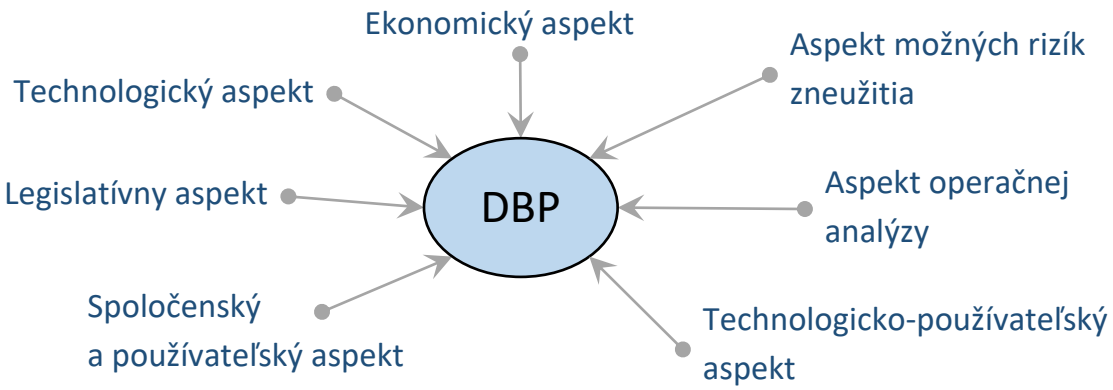
Výskumná otázka 5 je komplexného charakteru, a preto odpovedá iba na možné delenie aspektov, ktoré sa vzťahujú konkrétne na dynamický biometrický podpis. Pre komplexnú analýzu je problematika efektívnej podnikovej komunikácie cez DBP rozdelená do niekoľkých

aspektov, a to podľa možnej logiky prístupu: legislatíva, podnik, management, technológia, používateľ a riziká zneužitia. Dedukcia syntézy sekundárneho výskumu bol základ indukcie primárneho výskumu. Vychádzajúc z analýzy aktuálneho vedeckého poznania jednotlivé podotázky (1 až 7) V.O. 5 formulujú konkrétne hypotézy, ktoré sú testované v časti primárneho výskumu. Jednotlivé aspekty DBP skúmané v primárnom výskume sú formulované výskumnými otázkami:

- VO. 6.1 Aký je legislatívny aspekt a normy DBP?
- VO. 6.2 Aký je aspekt operačnej analýzy DBP?
- VO. 6.3 Aký je ekonomický aspekt DBP?
- VO. 6.4 Aký je spoločenský a používateľský aspekt DBP?
- VO. 6.5 Aký je technologický aspekt DBP?
- VO. 6.6 Aký je aspekt technologicko-používateľský DBP?
- VO. 6.7 Aký je aspekt možných rizík zneužitia DBP?

## 5.2 Vypracovanie primárneho výskumu

Dedukcia syntézy sekundárneho výskumu bola, že dynamický biometrický podpis by mohol byť adekvátny nástroj na efektívnu a bezpečnú vnútropodnikovú komunikáciu. Toto potvrdzuje aj argumentácia vo V.O. 4., kde sa pri daných stanovených podmienkach zvolilo použitie dynamického biometrického podpisu v on-line režime ako hlavná autentizačná metóda pre použitie v podniku na komunikáciu. Samotné rozhodnutie pre implementáciu a používanie DBP v organizáciách prináša aj mnoho ďalších otázok (viď vypracovanie V.O. 4 a V.O. 5). Preto primárny výskum sa zameriava práve na túto technológiu DBP v on-line režime a skúma, či je DBP efektívny nástroj pre podnikovú komunikáciu. Skúmané aspekty majú rozdielny charakter (viď Obrázok 5.2), preto pri primárnom výskume na každý skúmaný aspekt DBS sa použila metodológia zvlášť (viď príslušné kapitoly ďalej).




*Obrázok 5.2: Skúmané aspekty dynamického biometrického podpisu.*
*Zdroj: vlastné spracovanie.*

## 5.3 Legislatívny aspekt a normy DBP

### 5.3.1 Metodológia legislatívneho aspektu

Je silne deskriptívna štúdia, bez formulácie hypotéz. Základ tejto časti tvorí prieskum vzťahujúcej sa legislatívy a normy na daných technológií. Hlavný cieľ je podrobne zhromaždiť, pochopiť a vysvetliť danú legislatívu a normy vzťahujúce sa na problematiku technológie a používania DBP.

### 5.3.2 Vypracovanie

Používanie biometrických údajov je v Európskej únii regulované všeobecným nariadením EÚ o ochrane údajov - GDPR (Nariadenie Európskeho parlamentu a Rady č. 2016/679). GDPR začal v celej EÚ platiť jednotne s účinnosťou 25. 5. 2018. Aby členské štáty EU spĺňali všeobecné podmienky GDPR si museli adaptovať vlastnú legislatívu, viď kapitolu 1.2.1 Biometria a biometrický údaj.

Nariadenie GDPR vo svojom článku 9 upravuje spracovanie biometrických údajov s cieľom jedinečnej identifikácie fyzickej osoby. Pretože nariadenie aktualizovalo doteraz platné zákony členských štátov o ochrane osobných údajov, boli doteraz prezentované názory, podľa ktorých už nie je možné naďalej postupovať v medziach doterajšieho legislatívneho stanoviska. Od konca mája 2018 je teda na mieste otázka, či GDPR mení nejakým spôsobom postavenie DBP v legislatíve, prípadne či treba urobiť nejaké opatrenia.

Podľa (Smejkal, 2017) DBP sníma „surové“ biometrické údaje, ktoré sú využívané len pre podpísanie dokumentu, ich využitie nebude spojené s ďalším automatickým spracovaním

biometrických údajov. DBP nie je používaný pre identifikáciu subjektu údajov, lebo je to práve daná osoba, ktorá podpisom potvrdzuje svoju identifikáciu (uvedením mena signatára, prípadne ďalších údajov, ku ktorým je podpis pripojený) pri určitom úkone, čo dokladá vytvorením svojho podpisu. V prípadoch, keď DBP bude slúžiť ako prejav právneho konania, alebo v iných situáciách, kedy je prítomnosť podpisu dôležitá (zdravotnícke dokumentácie), potom je nasadenie DBP jednoduchá a neobťažujúca forma autentizácie podpisu používateľa vysoko prínosná ako pri rutinnom využívaní, tak pri zabezpečení integrity spracovávaných podpísaných elektronických dokumentov. Biometrické údaje sú šifrované, chránené proti neoprávnenému prístupu a sú sprístupnené tretej osobe (súdnemu znalcovi) iba v prípade sporu o pravosť podpisu, a to veľmi formalizovaným postupom obsahujúcim vysoké záruky.

DBP bude preto využívaný rovnako ako podpis klasický, tzv. jeho využitie nebude spojené s ďalším automatickým spracovaním biometrických údajov a nebude používaný pre identifikáciu subjektu údajov. (Smejkal, 2017)

**Možnosti použitia u elektronického podpisu**

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 zo dňa 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie eIDAS“) je kľúčovým a svojím spôsobom aj prelomovým právnym predpisom EÚ. Kľúčovým je najmä s ohľadom na jeho ambiciózne ciele a prelomovým preto, lebo prichádza v čase, keď už krajiny EÚ mali túto problematiku v širšej či užšej miere upravené národnými zákonmi. Cieľom nariadenia eIDAS je posilniť dôveru pri elektronických transakciách na vnútornom trhu vytvorením spoločného základu pre bezpečné elektronické interakcie medzi občanmi, podnikmi a orgánmi verejnej správy, čím sa zvýši účinnosť verejných a súkromných on-line služieb, elektronického podnikania a elektronického obchodu v EÚ. Nariadenie eIDAS pre tento účel vytvára podmienky pre vzájomné uznávanie kľúčových cezhraničných prostriedkov komunikácie, ako sú elektronická identifikácia, elektronické dokumenty, elektronické podpisy a elektronické doručovacie služby. Nariadenie eIDAS nadobudlo účinnosť ako v ČR tak v SR a dňom jej účinnosti sú jeho ustanovenia týkajúce sa dôveryhodných služieb priamo aplikovateľné a priamo záväzné vo všetkých členských krajinách EÚ. Znamená to, že dôveryhodné služby už viac nie sú upravené národným právom ale Nariadením eIDAS.

Dynamický biometrický podpis je v súlade s nariadením eIDAS (Nařízení Evropského parlamentu a Rady č. 910/2014), ktoré nadobudlo účinnosť 17. 9. 2014. DBP nie je náhradou

kryptografického elektronického podpisu, ale je významnou alternatívou. Túto alternatívu možno použiť v prípadoch, keď implementovanie certifikátov, bezpečné ukladanie a „stráženie“ privátnych kľúčov apod., by významným spôsobom narušilo rutinné a ustálené procesy. Myslí sa napr. spôsobené bariéry odrádzajúce bežných používateľov a významné organizačne technické problémy pri nasadení zaručeného alebo kvalifikovaného elektronického podpisu (Advanced Electronic Signature, Qualified Electronic Signature) podľa Nariadenia eIDAS. Výhodou DBP oproti kryptografickému elektronickému podpisu je tiež existencia uvedenej „vlastnoručnosti“.

**Aktuálne normy týkajúce sa priamo dynamického biometrického podpisu sú:**

Táto časť vychádza z: *Tabuľka 3.4: Zoznam noriem majúce vzťah k biometrii* a vypracováva normy, ktoré sa týkajú priamo DBP:

- *ISO/IEC 19794-7: 2015 Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data.* Českou verziou tejto medzinárodnej normy je: ČSN ISO/IEC 19794-7, Informační technologie - Formáty výměny biometrických dat - Část 7: Data časových řad podpisu/značky. Katalogové číslo: 98678.
- *ISO/IEC 19794-11: 2014 Biometric data interchange formats - Part 11: Signature/sign processed dynamic data).* Českou verziou tejto medzinárodnej normy je: ČSN ISO/IEC 19794-11 Informační technologie - Formáty výměny biometrických dat - Část 11: Zpracovaná dynamická data podpisu/značky. Katalogové číslo: 95083.

**Norma ISO/IEC 19794-7**

Norma špecifikuje formáty výmeny dát pre behaviorálne biometrické dáta podpisu/značky zachytené vo forme multidimenzionálnych časových radov v zariadení. Táto časť ISO/IEC 19794-7 obsahuje:

- Opis dát, ktoré môžu byť zachytené.
- Tri formáty dát pre uchovanie dát: 1. plný formát pre všeobecné použitie, 2. kompresný formát schopný udržať rovnaké množstvo informácií ako plný formát, ale v komprimovanej podobe, a 3. kompaktný formát pre použitie s čipovými kartami a inými tokeny, ktorý nevyžaduje kompresiu/dekompresiu, ale odovzdáva menej informácií než plný formát.
- Príklady obsahu dátových záznamov a osvedčených postupov pre zachytenie dát.

Druhé vydanie z roku 2015 reviduje prvé vydanie (ISO / IEC 19794 7: 2007). Kapitoly 7 a 8 boli technicky revidované a doplnené kapitolou 10 a prílohou A. Takisto zahŕňa technickú opravu ISO / IEC 19794 7: 2007 / Cor.1: 2009.

Podľa normy ISO / IEC 19794-7 sú zaznamenané nasledujúce kanály (v účinnosti parametrov DBS):

*Tabuľka 5.1: Kanály v súlade s normou ISO / IEC 19794-7*

| Channel name | Interpretation |
|---|---|
| X | x coordinate (horizontal pen position) |
| Y | y coordinate (vertical pen position) |
| Z | z coordinate (height of pen above the writing plane) |
| VX | velocity in x direction |
| VY | velocity in y direction |
| AX | acceleration in x direction |
| AY | acceleration in y direction |
| T | time |
| DT | time difference |
| F | pen tip force (pressure) |
| S | tip switch state (touching/not touching the writing plane) |
| TX | tilt along the x axis |
| TY | tilt along the y axis |
| Az | azimuth angle of the pen (yaw) |
| El | elevation angle of the pen (pitch) |
| R | rotation (rotation about the pen axis) |

*Zdroj: ISO / IEC 19794-7*

Počas zaznamenávania údajov podpisu zariadenie získava biometrické informácie overovaného subjektu. Kanály X a Y tvoria povinný záznam pohybu pera. K zaznamenaniu dynamiky musia byť kanály T alebo DT prítomné, alebo uvedený jednotný odber vzoriek (konštantný časový rozdiel medzi dvoma susednými okamihmi vzorkovania). Začlenenie ďalších kanálov (parametrov) je voliteľné (Smejkal, Kodl, 2011).

Formáty výmeny dát sú všeobecné v tom, že môžu byť uplatnené a použité v širokej rade oblasti aplikácií, ktoré zahŕňajú ručne písané značky a podpisy. Táto časť ISO / IEC 19794-7 sa nezaoberá požiadavkami alebo vlastnosťami špecifickými pre aplikáciu.

**Norma ISO / IEC 19794-11**

Norma obsahuje odporúčania a základné požiadavky, ktoré navrhovaný systém musí spĺňať. Norma opisuje povinné parametre a formáty biometrických údajov. Norma špecifikuje

formát pre vzájomnú výmenu dát vytvorených pri podpise, vrátane priestorových a dynamických vlastností, ktoré môžu byť použité pre verifikáciu podpisu/značky.

Definovaný formát dát umožňuje interoperabilitu bez kompromitácie akýchkoľvek práv vývojárov duševného vlastníctva. Aby bola zaistená interoperabilita, je identifikovaná skupina vlastností, mandatórnych pre všetky vyhovujúce implementácie, navyše formát záznamu biometrickej výmeny tiež podporuje proprietárne dáta. Použitie proprietárnych dát je upravené podobným spôsobom ako v ISO/IEC 19794-7, zaisťujúcim dosiahnutie porovnateľnej výkonnosti medzi mandatórnymi a proprietárnymi vlastnosťami.

Táto norma berie ohľad na biometrické údaje definované normou ISO/IEC 19794-7, ktoré môžu byť použité pre výpočet ďalších parametrov. Zaznamenané vlastnosti reprezentujú podstatné dynamické udalosti počas procesu podpisu a tak predstavujú inteligentnú kompresiu formátu ISO/IEC 19794-7. Formát normy 19794-7 použitím podstatných udalostí môže byť extrapolovaný, a teda môžu byť vypočítané ďalšie údaje vlastností podpisu/značky.

Popísaný formát je založený na vlastnostiach dynamických udalostí podpisu v komparácii okamžitého vzorkovania podpisu, ako je popísané v ISO/IEC 19794-7.

Norma ISO/IEC 19794-11 nešpecifikuje analýzu, ktorá má byť vykonaná konkrétnymi porovnávacími algoritmami. Vlastnosti podpisu/značky zaznamenané vo formáte dát môžu byť použité pre analýzu rôznymi porovnávacími algoritmami.

## 5.4 Aspekt operačnej analýzy

### 5.4.1 Metodológia aspektu operačnej analýzy

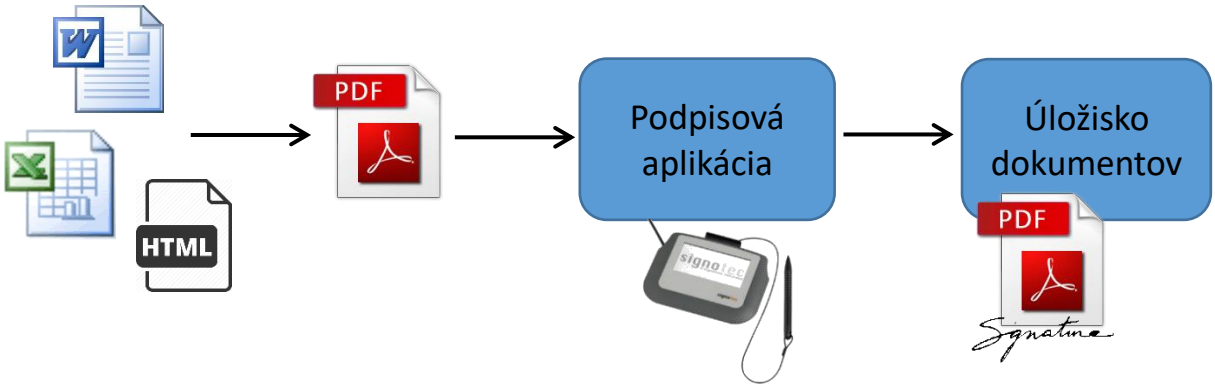
Empiricky: tlak na neustále zvyšovanie efektívnosti podnikových procesov vyžaduje implementáciu nových technológií. Implementácia novej, či doteraz v podniku nepoužitej technológie bude mať následok aj v zmenách podnikových procesov.

Vychádzajúc z empirickej úvahy, implementácia DBP do podnikových procesov prináša aj možné zmeny, kvôli tomu je DBP skúmaný aj z pohľadu operačnej analýzy a použiteľnosti v podnikových procesoch. Táto časť v sebe zahŕňa niekoľko praktických prístupov, ktoré sú si navzájom prepojené. Cieľom tejto časti je nájsť a sumarizovať hlavné prínosy, možné oblasti využitia, výhody a nevýhody DBP na podnikové procesy a všeobecne pre organizácie.

### 5.4.2 Vypracovanie

Proces DBP je najprv analyzovaný, vysvetlený a potom skúmaný z pohľadu uplatnenia pre dané ciele. Cieľom tejto časti je nájsť a sumarizovať hlavné prínosy, možné oblasti použitia, výhody a nevýhody DBP vyplývajúce z komparačnej analýzy na podnikové procesy a všeobecne pre organizácie.

Obrázok 5.3 graficky ilustruje jednoduchý postup použitia DBP. Ako prvý krok je vyhotovenie finálnej verzie dokumentu, ktorý chceme podpísať. Závisí od použitej aplikácie aké formáty sú podporované, kvôli kompatibilite je odporúčané previesť dokument do výsledného formátu *.pdf. PDF bol štandardizovaný ako otvorený medzinárodní formát ISO 32000 v roku 2008 a nevyžaduje žiadne poplatky za jeho implementáciu. Výsledný dokument sa potom načíta do danej podpisovej aplikácie a s príslušným hardwarovým ústrojenstvom používateľ ho podpíše pod svojím menom. Podpísaný dokument je potom podľa potreby uložený a sprístupnený.




*Obrázok 5.3: Ukážka procesu DBP používateľa pri dokumente*

*Zdroj: vlastné spracovanie.*

V prípade nezhody nasnímaného podpisu a vzorového podpisu používateľa, aplikácia nedovolí podpísať daný dokument. DBP obsahuje informácie o tom, ako bol podpis vytvorený, odráža teda charakteristické znaky podpisujúcej sa osoby, tzv. biometrickú stopu, ktorá je unikátna pre každého jednotlivca. Prvky DBP nie sú viditeľné, a preto nemôžu byť falšovateľom reprodukované, na rozdiel od samotného obrázku podpisu, ktorý tu tvorí len jeden z parametrov biometrickej stopy.

Dokument vo formáte PDF je predpokladaný ako finálny, ale napriek tomu sú aplikácie, ktoré umožňujú naďalej finálny dokument modifikovať. Aby bola zabezpečená integrita obsahu dokumentu je dôležité ju zabezpečiť kontrolnými prvkami, ďalej zabezpečiť opatrenia proti zneužitiu údajov DBP používateľa.

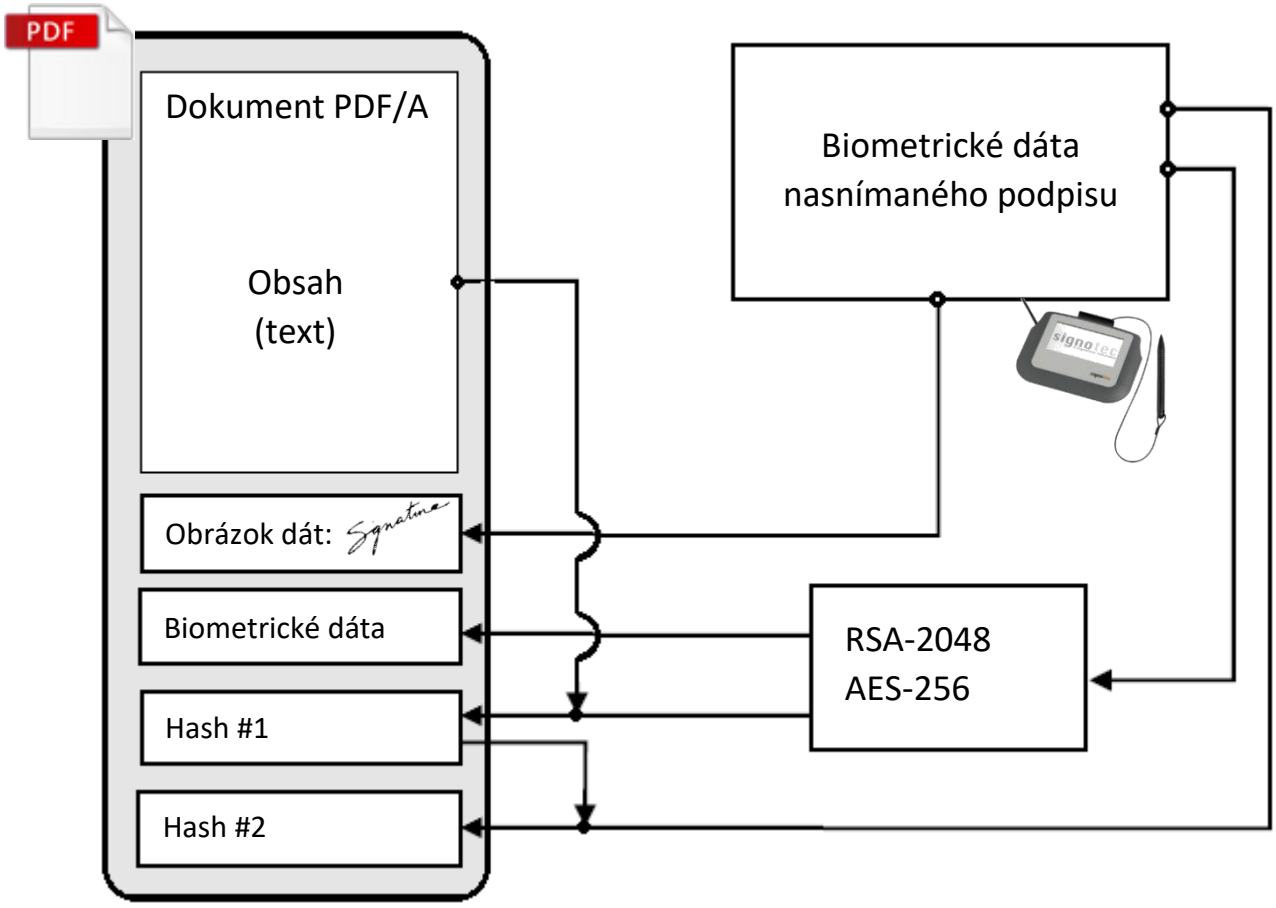
**Zabezpečenie DBP**

Vektor dát, reprezentujúcich DBP, opustí snímacie zariadenie len v zašifrovanom tvare. Zabezpečený prenos biometrických dát zo snímača do počítača bezprostredne nadväzuje na požiadavku na jednoznačné a zabezpečené spojenie DBP s podpisovaným dokumentom. Pre tieto účely je možné použiť kryptografickú metódu pre vytvorenie hashu dokumentu, tak pre ochranu integrity podpísaného hashu štandardným (kryptografickým) elektronickým podpisom. Podstatným rozdielom je, že použitie asymetrickej kryptografie (teda vytvorenie podpisu pomocou súkromného kľúča) nie je požadované na strane klienta (používateľa), ale je otázkou riešenia celého systému. Používateľa (podpisovateľa) nezaťažuje žiadnymi technicko-organizačnými požiadavkami.

Výrobcovia zariadenia zaisťujú bezpečnosť DBP vytváraním radou hashov a vykonávajú podpisovanie a šifrovanie. Príklad takéhoto postupu je reprezentované na schéme: Obrázok 5.4, s nasledujúcim postupom (Smejkal, 2017):

1. Aplikácia zriadi šifrovanú komunikáciu s podpisovacím zariadením (v tomto prípade algoritmom AES-256). Výmena kľúča prebehne pomocou Diffie-Hellman-Merkle protokolu. Počas podpisu sú týmto zabezpečeným kanálom prenášané biometrické údaje do aplikácie.
2. Používateľ sa podpíše na pole podpisovacieho zariadenia. Vytvorené dáta reprezentujúce podpis sú šifrovaným kanálom (viď krok 1) prenesené do pamäti počítača.
3. Na základe biometrických dát aplikácia vytvorí (viditeľný) obrázok podpisu a vloží ho do dokumentu.
4. K biometrickým údajom sú pripojené ďalšie údaje (sériové číslo zariadenia, časová pečiatka), čo zaistí, že biometrické údaje nemôžu byť umiestnené do iného dokumentu, resp. že toto zneužitie je možné zistiť.
5. V zariadení sú zašifrované biometrické údaje symetricky (AES-256) a symetrický kľúč potom aplikácia zašifruje pomocou verejného kľúča asymetricky (RSA-2048).
6. Aplikácia vloží zašifrované biometrické údaje do PDF dokumentu.
7. Aplikácia spočíta HASH1 (algoritmom SHA-256) z obsahu dokumentu a zašifrovaných biometrických dát. HASH1 slúži na kontrolu integrity dokumentu a zašifrovaných biometrických dát. HASH1 je podpísaný verejným kľúčom.
8. Aplikácia vloží podpísaný HASH1 a príslušný verejný kľúč do dokumentu.

9. Aplikácia spočíta HASH2 (algoritmom SHA-256) z HASH1 a nešifrovaných biometrických dát a uloží ho do dokumentu. HASH2 zaisťuje prepojenie dokumentu a biometrického podpisu.
10. Aplikácia zmaže z pamäte počítača nezašifrované biometrické údaje a vypočítané hash-e (HASH1 a HASH2).




*Obrázok 5.4: Schéma previazania DBP s dokumentom typu PDF*

*Zdroj: prerobené zo zdroja (Smejkal, 2017)*

Dodatok k postupu a ku schéme *Obrázok 5.4*:

- PDF/A je oficiálna archivačná verzia formátu PDF definovaná normou ISO 19005-1 (2005) a ISO 19005-2 (2011), ktorá špecifikuje vlastnosti elektronického dokumentového formátu súborov pre dlhodobé uschovávanie. Cieľom týchto súborov je, aby boli kompatibilné s budúcimi verziami softvérových nástrojov a mali nezávislosť na použitej platforme. Verzií PDF/A je definovaných niekoľko, pre konkrétny prehľad viď zmienené normy.

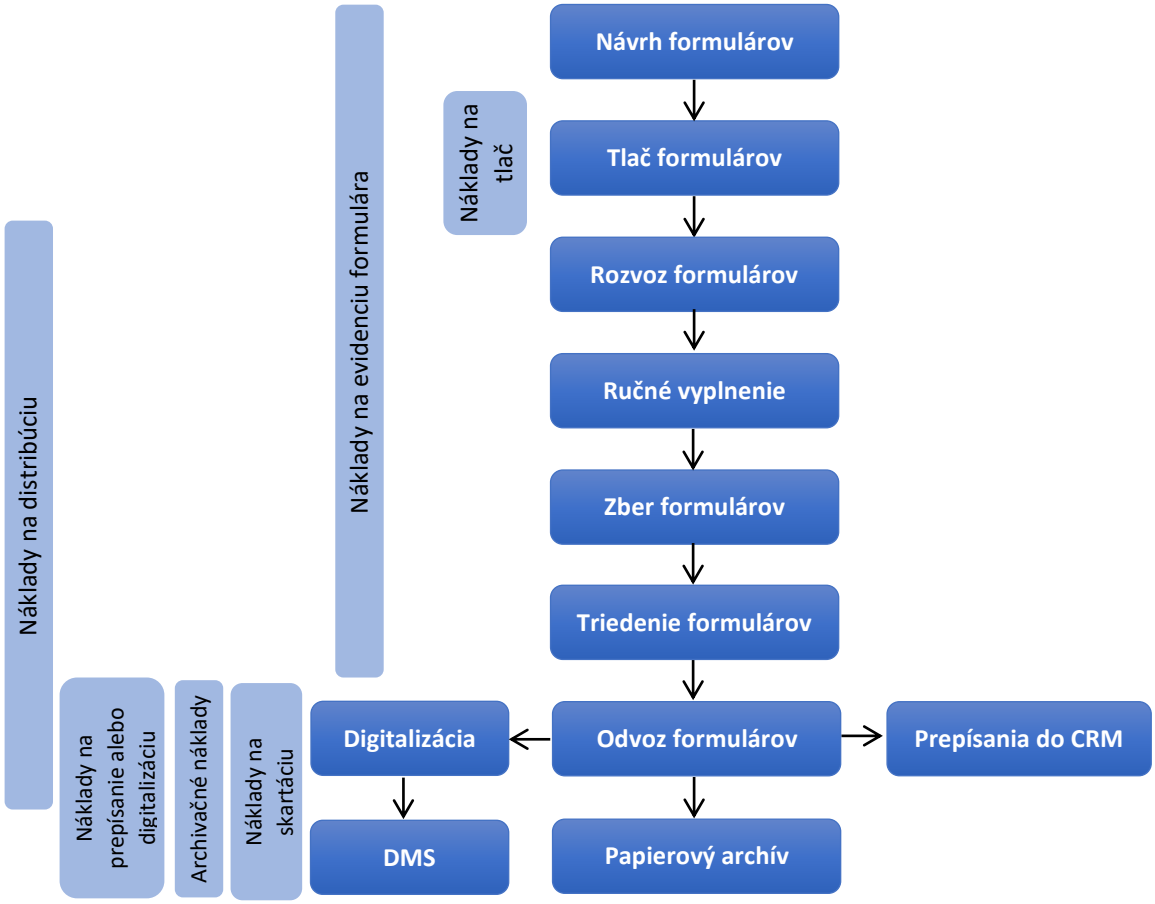
- AES-256 je algoritmus používaný na symetrické šifrovanie dát, pri ktorom sa šifruje a dešifruje rovnakým kľúčom na oboch stranách, s dĺžkou kľúča 256 bitov.
- Diffie-Hellman-Merkle protokol je kryptografická metóda, ktorá umožňuje cez nezabezpečený kanál vytvoriť šifrované spojenie medzi komunikujúcimi stranami a to bez nutnosti predchádzajúceho dohodnutia šifrovacieho kľúča. Výsledkom je vytvorenie symetrického šifrovacieho kľúča, ktorý je efektívnejší a môže byť použitý pre šifrovanie ďalšej komunikácie.
- RSA je algoritmus používaný na asymetrické šifrovanie dát, ktorý sa dá používať pre podpisovanie i šifrovanie dokumentov. Na šifrovanie sa používa súkromný a verejný kľúč nazývaný aj ako šifrovací kľúč a dešifrovací kľúč. Oba kľúče sú rozdielne a majú vopred definovanú dĺžku, pričom pri dostatočnej dĺžke kľúčov sú považované za bezpečné. Dôvodom je fakt, že dané kľúče musia byť matematicky zviazané, avšak nevyhnutnou podmienkou pre užitočnosť šifry je praktická nemožnosť zo znalosti šifrovacieho kľúča vypočítať ten dešifrovací. RSA algoritmus v prípade elektronického podpisu používa tento princíp. Majiteľ súkromného kľúča vie „podpísať“ a poslať elektronickú správu (napr. dokument), ku ktorej ešte pripojí hash danej správy pomocou svojho tajného/súkromného kľúča. Osoby, ktoré dostanú správu vedia autenticitu správy skontrolovať príslušným verejným kľúčom. Kontrola prebieha hashovaním prijatej správy príslušným verejným kľúčom a porovnaním priloženého hashu, ktorý bol vytvorený súkromným/tajným kľúčom. Ak správa nebola zmenená, vyjde ekvivalentná hodnota hashov a správa sa môže považovať za dôveryhodnú. Keďže jediný, kto pozná súkromný/tajný kľúč je jeho majiteľ, je zaručené, že správa bola zašifrovaná/podpísaná majiteľom tajného/súkromného kľúča. Pre každého oprávneného majiteľa sú kľúče unikátne.
- RSA-2048 je RSA algoritmus, ktorý používa súkromný a verejný kľúč s dĺžkou 2048 bitov. Aktuálne používaný v praxi a kvôli dostatočnej dĺžke kľúča je považovaný za bezpečný.

Pre viac informácií ohľadne kryptografických metód a počítačovej ochrane dát pozri zdroje od autora Singh (2003) a Doseděl (2004).

**Využiteľnosť DBP**

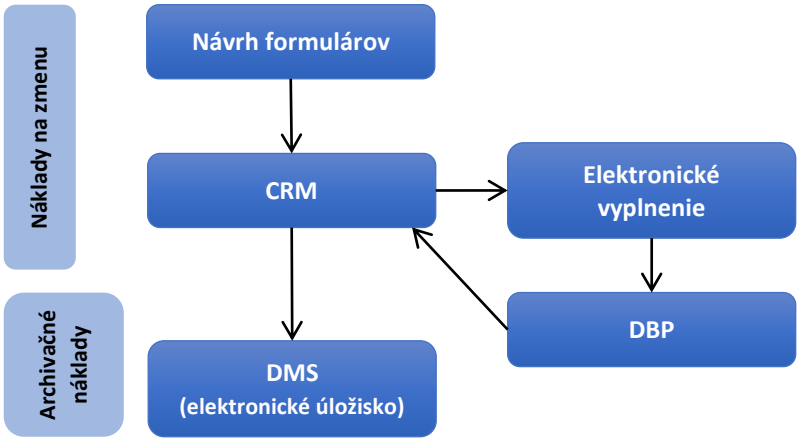
Využiteľnosť DBP narastá s trendmi v ICT a všeobecnou digitalizáciou v spoločnosti. Využitie DBP je možné v prípadoch, keď bude DBP slúžiť ako prejav právneho konania alebo v iných situáciách, keď je prítomnosť podpisu dôležitá (obchodné, pracovnoprávne a zdravotnícke dokumentácie), potom je nasadenie tejto formy autentizácie dokumentu vysoko prínosné ako pre rutinné využívanie, tak pre zabezpečenie integrity spracovávaných podpísaných elektronických dokumentov.

Využiteľnosť DBP v prípade podnikov a organizácií sa dokáže na reprezentačnom príklade, kde sa porovnáva proces pri podpisovaní formulárov v prípade modelu „klasického" papierového podpisovania formulárov (viď: *Obrázok 5.5*) a v prípade použitia DBP s elektronickým obsahom (viď: *Obrázok 5.6*).




*Obrázok 5.5: Schéma procesu pri papierovej verzii podpisovania formulárov*

*Zdroj: vlastné spracovanie.*




*Obrázok 5.6: Schéma procesu podpisovania formulárov s DBP*

*Zdroj: vlastné spracovanie.*

Dodatok ku schémam *Obrázok 5.5* a *Obrázok 5.6*:

- CRM – (Customer relationship management), riadenie vzťahov so zákazníkmi, pre viac viď zdroj: Buttle (2004).
- DMS - Document management system, je správa dokumentov alebo tiež systém pre správu dokumentov alebo Electronic Document management (EDM), je počítačový systém určený na spravovanie elektronických dokumentov a/alebo digitalizovaných papierových dokumentov, napr. dokumentov prevedených do digitálnej podoby skenovaním. pre viac viď zdroj: Meurant (2012).
- Reprezentačný príklad vychádza z reálnej analýzy, ktorá je založená na spracovaní dotazníka (viď kapitolu 5.6.1) pri papierovej verzii a pri elektronickej verzii spracovania. Pri spracovaní dotazníka bolo jednoznačne potvrdené, že plne elektronická verzia umožňuje rýchlejšie procesné spracovanie ako jej ekvivalent v papierovej verzii. Tento konkrétny prípad dotazníka síce nepoužíva DBP, kvôli anonymite dotazníka, ale použiteľnosť v podnikovej praxi s DBP by mala preukázať tú istú analógiu zjednodušenia spracovávania vychádzajúcej z automatických procesov pri používaní elektronických formulárov.

Z reprezentačného príkladu sa dá odvodiť, že výsledná práca s digitálnymi dokumentmi je jednoduchšia ako s papierovými verziami dokumentov. Digitalizácia papierového obsahu je spravidla skenovaná a archivovaná len ako skenované „obrázky“, ktoré v tejto surovej forme nemožno následne efektívne používať a automaticky spracovávať. Pre umožnenie spracovania údajov na papierových dokumentov je potrebné buď prepísanie ich obsahu manuálne do

elektronického systému, alebo použiť počítačové algoritmy na optické rozpoznávanie znakov a textu - OCR (z anglického Optical Character Recognition) viď (Forsyth, Ponce 2003; Hortai, 2015), ktoré ale nezabezpečia 100 percentné opätovné rozpoznanie údajov: strata dokumentov (zlyhanie ľudského faktory), strata informácií (napr. prípady pošpinených dokumentov alebo papiere so znehodnoteným obsahom, kvôli citlivosti na teplo apod.).

**Možné oblasti využitia DBP v podniku**

Pri analýze využiteľnosti boli určené možné využitia a zefektívnenia podnikových procesov vymenovaných a kategorizovaných podľa:

- Všeobecné využitie DBP pri práci s digitálnymi dokumentmi:
    - DBP je možné používať ako alternatívu pre elektronický podpis v rámci vnútropodnikovej komunikácie pre interné záležitosti.
    - Podporuje diaľkovú komunikáciu cez ICT.
    - Urýchľuje archiváciu dokumentov a umožňuje automatického spracovania dokumentov.
    - Umožnenie hromadného podpisu a viac dokumentov súbežne.
    - Umožnenie znázornenia podpisu na vylačnenom dokumente, tým pádom je zabezpečená aj možnosť listinného obehu dokumentov v prípade potreby.
    - DBP je možné používať súbežne s elektronickým podpisom (kvalifikovaným certifikátom). Tu je ale potrebné brať ohľad na platnú legislatívu danej krajiny. Napr. v ČR sa vzťahuje na elektronické podpisovanie dokumentov *Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce*, kde je definované možnosť používania DBP v *§ 7* a prípady, v ktorých sa DBP nedá použiť *§ 5* kvalifikovaný elektronický podpis a *§ 6* uznávaný elektronický podpis.
- Využitie v rámci interných procesov:
    - podpisy faktúr, ponúk, objednávok, dodacích listov, servisných protokolov, podpisy interných materiálov, interné oznámenie, žiadanky, vyjadrenia, a ďalšie využitia.
- Využitie pri styku so zákazníkmi:
    - v rámci pokladničných operácií,
    - pri podpisovaní zmlúv,
    - pri vypĺňaní formulárov,

- pri vybavovaní reklamácií,
- apod. využitia.

**H 5.2.I: DBP je možné zefektívniť podnikové procesy a urýchliť komunikáciu.**

Z vypracovania výskumnej otázky 5.2 je **prijatá** hypotéza H 5.2.I.

**Hlavné prínosy riešenia DBP:**

- umožňujú zrýchlenie procesov pri dokumentoch,
- zvyšujú bezpečnosť pri elektronických dokumentoch,
- zvyšujú produktivitu práce (napr.: komunikácia na diaľku – home office apod.),
- kompenzácia nákladov po implementácii (pre viac o ekonomickej rentabilite viď kapitolu 5.5.)

## 5.5 Ekonomický aspekt

Analýza ekonomického aspektu v sebe zahŕňa nákladovosť a rentabilitu DBP ako zvládnutia kybernetickej bezpečnosti a z úspor vyplývajúcich zo zavedenia systému s DBP.

### 5.5.1 Metodológia ekonomického aspektu

Zo sekundárneho výskumu bolo zistené, že tlak na neustále zvyšovanie bezpečnosti je celosvetovou záležitosťou, čomu korešpondujú aj vysoké náklady. Napr. z verejne dostupných zdrojov možno získať nasledujúce informácie:

- Výdavky Spojených štátov na kybernetickú bezpečnosť z roka na rok rastú. V rozpočte na rok 2016, ktorý predložil ešte prezident Barack Obama, bolo vyhradené 14 miliárd dolárov na túto záležitosť. (Shalal, Selyukh, 2015)
- V júli 2016 NATO oficiálne vyhlásilo kyberpriestor, ako ďalší z operačných dimenzií vedľa vzduchu, zeme a mora. NATO 27. marca 2017 potvrdilo, že na vývoj satelitnej a výpočtovej techniky v nasledujúcich troch rokoch investuje 3 miliardy eur. (Robin, 2017)
- Británia posilnila boj s kybernetickou kriminalitou, na zlepšenie svojej bezpečnosti vydá v najbližších piatich rokoch 1,9 miliardy libier v rámci národnej stratégie kybernetickej bezpečnosti 2016 – 2021. (HM Government, 2016)

V podniku náklady takéhoto charakteru, straty a potenciálne straty nemožno jednoznačne vyčísliť. Predpisy a metodiky často neriešia ako postupovať ekonomicky alebo nestanovia časovo najefektívnejšie riešenia problematiky kybernetickej bezpečnosti.

Pokiaľ sa na to pozrieme z hľadiska účtovníctva, tak zabezpečenie kybernetickej bezpečnosti znamená určitú investíciu pre firmu, ktorá sa v účtovníctve objaví napr. ako dlhodobý nehmotný majetok – software. V tomto prípade sa oceňuje obstarávacou cenou, a táto investícia sa stáva súčasťou účtovnej hodnoty firmy. Bezpečnostné opatrenia nemusia byť nevyhnutne investície, v prípade outsourcingu (napríklad službami externou špecializovanou spoločnosťou) to budú náklady na tieto služby. Tieto hodnoty ale majú veľmi nízku vypovedaciu schopnosť, lebo zavedený systém kybernetickej bezpečnosti predstavuje obrovskú konkurenčnú výhodu oproti firmám, ktoré sa tejto problematike nevenujú.

V našich predošlých publikáciách sme už riešili s kolektívom autorov (Smejkal, Hortai, Molnárová, 2017) otázku kybernetickej bezpečnosti a jej začlenenia do hodnoty podniku. Zistené bolo, že kybernetická bezpečnosť sa stáva faktorom v každej firme a jednoznačne zvyšuje hodnotu firmy, tak účtovnú ako aj trhovú. Všeobecne pre meranie hodnoty podniku možno v podstate využiť tri základné skupiny metód, a to metódy **majetkové, výnosové a metódy tržné** (Kislingerová, 2001).

Keď berieme do úvahy skutočnosť, že kybernetická bezpečnosť zvyšuje efektivitu a konkurenciu schopnosť podniku, tak je jasné, že účtovná hodnota a trhová hodnota podniku sa budú odlišovať. Pri stanovení trhovej hodnoty spoločnosti, treba najprv vyčísliť hodnotu systému kybernetickej bezpečnosti, pričom vychádzame z prínosov, ktoré nám tento systém prinesie. V týchto prípadoch sa používajú metódy výnosového prístupu oceňovania nehmotných aktív.

Otázne je pritom, kde je tá hranica ekonomickej rentabilnosti novodobých ICT a technológií kybernetickej bezpečnosti. Táto časť sa preto zameriava na ekonomickú optimalizáciu technológií. Hlavný cieľ je navrhnúť metódu pre stanovenie horného prahu nákladov pre kybernetickú bezpečnosť z pohľadu ekonomickej rentability. DBP spadá do problematiky kybernetickej bezpečnosti, preto navrhnutá metóda sa dá aplikovať na technológiu DBP. Analýza ekonomického aspektu v sebe zahŕňa rentabilitu DBP ako zvládnutia kybernetickej bezpečnosti a z úspor vyplývajúce zo zavedenia systému s DBP.

Výskum vychádza z vedeckej teórie na konkrétne príklady a vlastné modely. Výsledok sa potom aplikuje na ekonomickú efektívnosť DBP.

### 5.5.2 Vypracovanie

**Zvládnutie kybernetickej bezpečnosti a jej ekonomická rentabilita**

Zvládnutie kybernetickej bezpečnosti má vplyv na stabilitu firmy (zníženie nákladov pri kybernetických útokoch, zvýšenie prínosov znížením rizika pokút napr. podľa GDPR, zaistenie business continuity a pod.). Firmy, ktoré sú náplňou činností aj ekonomickými výsledkami veľmi podobné, sa môžu napriek tomu významne líšiť, a to svojou stabilitou. Stabilita v tomto zmysle je súhrnný pojem pre schopnosť riadiť riziká a zabezpečiť kontinuitu činností. Táto otázka nadobúda extrémneho významu s postupnou digitalizáciou vnútornej štruktúry firmy aj ich vonkajšieho okolia, najmä s trendmi ako IoT, BYOD a Priemysel 4.0. Mierou zvládnutia kybernetickej bezpečnosti by mohla byť zníženie jej rizika. Potom je logické, že stabilná firma má vyššiu trhovú hodnotu, aj keď jej účtovná hodnota môže byť zhodná s menej stabilnou firmou. (Smejkal, Hortai, Molnárová, 2017a)

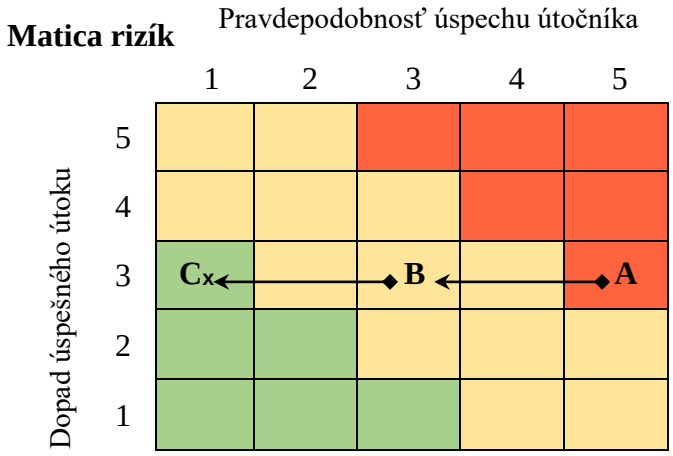
Základným príkladom môže byť samotná povinnosť či zodpovednosť právnických osôb na vynaloženie všetkého úsilia aby spáchaniu protiprávnych činov zabránila. Tie vyplývajú z tuzemských zákonov, v Slovenskej republike trestnú zodpovednosť právnických osôb upravuje *zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov* (účinnosť od 01. 07. 2016) a Českej republike upravuje zákon *č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim* (účinnosť od 01. 01. 2012).

Pre znázornenie hrozby je reprezentačný príklad podvodu, kde útočník používa ukradnutú alebo napodobnenú identitu a dezinformáciu.

- Ukradnúť identitu napr. mailovú adresu oprávneného používateľa je možné metódami sociálneho inžinierstva, napr. metódou „phishing“, ktorá je technika podvodu používaná na internete k získavaniu citlivých údajov (heslá, čísla kreditných kariet apod.) pri elektronickej komunikácii.
- Napodobnená identita je napr. technika poslania správy z podobnej e-mailovej adresy ako pôvodnej. Predstavme si komunikáciu medzi dvoma zahraničnými spoločnosťami kde prvá spoločnosť financuje spoločnosť druhú. Finančné oddelenie prvej spoločnosti dostane mail akoby od 2 spoločnosti, kde namiesto pôvodnej e-mailovej adresy *partner@Menoorganizácie.com* sa uvádza podobný originálu napr.: *partner@Menoorganizácie.org*, kde je iba zmenená doména.

Útočník v oboch prípadoch sa javí ako kompetentný človek z pôvodného mailu. Správa obsahuje inštrukcie a prílohu vo forme dokumentu napr. „podpísanú“ žiadosť, či faktúru a žiada

o preplatenie sumy na účet útočníka/hackera v zahraničí. Správa vyzerá ako dôveryhodná, používa formátovanie ako spoločnosť 2 aj logo atď. Nepreškolený personál od spoločnosti 1 preplatí danú sumu na účet útočníka. Kým sa zistí podvod, má útočník čas na efektívne zahladenie stôp. Takýmto typom útoku vznikne výdaj ukradnutej sumy a aj možné poškodenie dobrého mena spoločnosti atď. Takéto hrozby je možné eliminovať napr. preškolením personálu, kontrolou autenticity príloh, atď. Príklad je znázornený i graficky pomocou matice rizík (viď: Obrázok 5.7), kde sa z pôvodného rizika znázornený bodom A sa pomocou preškolenia personálu vieme dostať do bodu B a s doplnením technológií kontrolou autenticity správy sa vieme dostať do cieľového bodu C. Dopad úspešného skutku je v tomto prípade konštantný, so zmienenými protiopatreniami znižujeme jej pravdepodobnosť aby daná možnosť nastala.




*Obrázok 5.7: Matica rizík a posun znižovaním rizika*

*Zdroj: vlastné spracovanie.*

Opísaný prípad je jednoduchý pokus o podvod, ale možné variácie a spôsoby kybernetických útokov je mnoho (viď Smejkal, 2015). Bez bezpečnostných opatrení je toto riziko riešené iba retenciou rizika. Môžeme teda konštatovať, že protiopatrenia či zabezpečenie kybernetickej bezpečnosti spôsobí zníženie rizika. Takáto možná kvantifikácia sa dá napr. porovnaním ukazovateľov nákladov na zníženie rizika a prínosov zo zníženia rizika, ktorý je na ďalšom reprezentačnom príklade:

Za nesplnenie požiadaviek na GDPR môže spoločnosť platiť pokutu až vo výške 20 miliónov eur alebo 4% z celkového obratu za uplynulý finančný rok. Ukážková spoločnosť je priemerná stredná firma s obratom 5 mil. eur (cca. 130 mil. Kč). Predpokladajme že na začiatku je riziko pokuty napr. 80% riešená iba retenciou rizika, a po vykonaných opatreniach (splnenie požiadaviek na GDPR) sa zníži riziko na 10 %. Týmto spôsobom sa z hroziaceho vyššieho

rizika z 4 % × 5 mil. × 80 % sa zníži na 4 % × 5 mil. × 10 %, t. j. o 4 % × 5 mil. × 70 % = 140 tisíc eur (cca 3,6 mil. Kč). Náklady takéhoto charakteru na vytvorenie systému na zvládnutie požiadaviek vyplývajúcich z GDPR sú 70 tis. eur. (reálna ponuka pre strednú firmu o 500 zamestnancoch). V tomto prípade dôjde k zvýšeniu nákladov o 70 tis. eur jednorazovo, plus k tomu môžeme predpokladať maximálne 20 tisíc eur ročne na pozíciu poverenca pre spracovanie osobných údajov. Pozíciu poverenca je možné aj outsourcovať s nižšími nákladmi.

Pri predpoklade vynaloženia maximálnych nákladov na zníženie rizika sú predpokladané prínosy zo zníženia rizika väčšie. (Smejkal, Hortai, Molnárová, 2017a) Z toho vyplýva vzťah nižšie:

*(Väčšia bezpečnosť ) => (Väčšie náklady) a (Nižšie riziko)* *(3)*

Zo vzťahu vyššie je logické definovať hornú hranicu nákladov, do ktorej sa ešte oplatí znižovať riziko u bezpečnosti IS:

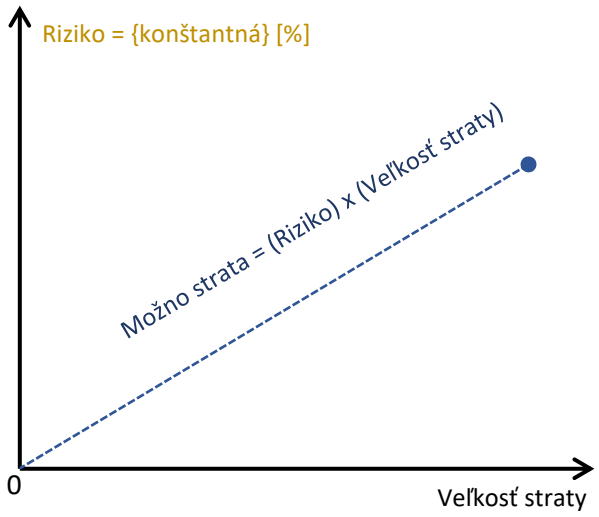
*Náklady vzťahujúce sa na znížení rizika ≤ (menšie alebo rovné ako)*
*Náklady pri vzniku potenciálnej škody a na obnovu kontinuity činností, pokiaľ sa udalosť, s ktorými je riziko spojené, nastane* *(4)*

Rovnice 3 a 4 sú založené na predpoklade o dôležitosti aktív, ktoré závisia na tom, o aké aktívum sa jedná a aké riziko predstavuje zneužitie alebo strata daného aktíva. Z toho vychádza, že je racionálne vynaložiť náklady na zabezpečenie daných aktív až do hranice, kým tieto náklady sú menšie alebo rovné ako čiastka, ktorá reprezentuje stratu daných aktív a vyplývajúce možné zneužitie týchto aktív. Potom je logické, že zvyšujúcou sa hodnotou aktív a rizika by sa mala zvyšovať aj jej zabezpečenie. Náklady na zabezpečenie aktív a na protiopatrenia proti zneužitiu majú vplyv na pravdepodobnosť uskutočnenia vťahujúcich sa hrozieb. Preto rovnice 3 a 4 síce dávajú logickú podmienku, ale kvôli dynamickým vplyvom koeficientov táto hranica nemusí byť optimálny bod, t. j. môžeme predpokladať, že táto podmienka bude mimo hľadaného optima. Preto je ďalej skúmaná funkcionálnou analýzou vzťah medzi rizikom a nákladmi vynaloženými na zabezpečenie aktív a protiopatreniami proti zneužitiu týchto aktív.

Riziko vyjadruje mieru ohrozenia aktív, mieru nebezpečenstva, že sa uplatní hrozba a dôjde k nežiaducemu výsledku vedúcemu k vzniku škody (nežiaducemu následku) (Smejkal, Rais, 2013, str. 99). Pojmy „viac rizika“ a „menej rizika“ v tomto prípade označujú meradlo možnej veľkosti straty. Predpokladaná (očakávaná) hodnota straty v danej situácii je pravdepodobnosť tejto straty násobená veľkosťou potenciálnej straty. Ak je ohrozené desať eur

a pravdepodobnosť straty je 0,2 (20%), bude predpokladaná hodnota straty dve eurá. Pokiaľ je objem postihnutý rizikom sto eur a pravdepodobnosť straty predstavuje 0,02 (2%), bude predpokladaná hodnota straty rovnako dve eurá (Smejkal, Rais, 2013, str. 107).

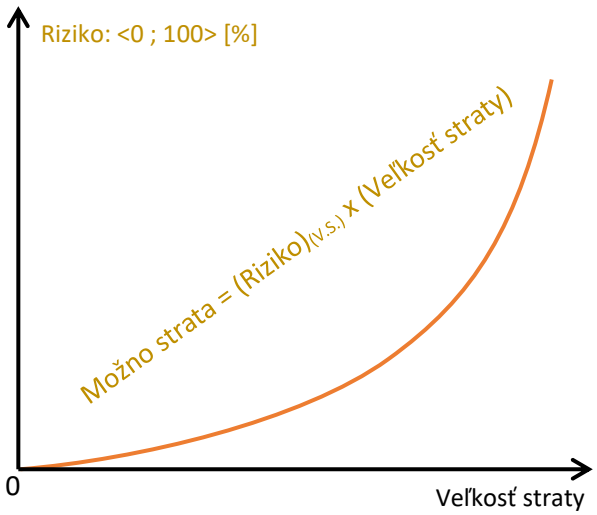
Keď predpokladáme lineárnu závislosť je riziko konštantnou hodnotou v rozpätí: <0 ; 100> % a „možná strata“ je závislá od aktíva, ktoré je ohrozované týmto rizikom (viď Obrázok 5.8), kde:




*Obrázok 5.8: Vzájomný vzťah potenciálnych škôd a rizika*

*Zdroj: prerobené zo zdroja (Smejkal, Hortai, Molnárová, 2017b)*

Môžeme ale predpokladať že táto závislosť má silne nelineárny charakter. Dôsledok je napr. vplyv aktív s vyššou hodnotou, ktoré majú lukratívnejší charakter na možné útoky. Preto zvyšovaním hodnoty aktív sa zvyšuje aj ich riziko ohrozenia/útoku. Empiricky: napr. hacker je motivovanejší kybernetickému útoku tam, kde má možný väčší subjektívny zisk. Kyberterorista sa snaží spáchať čím väčšie škody. Z toho vyplýva že riziko je funkciou hodnoty ohrozovaných aktív/veľkosť straty. Riziko takto naberá dynamický charakter (viď Obrázok 5.9):




*Obrázok 5.9: Dynamický vzťah potenciálnych škôd a rizika*

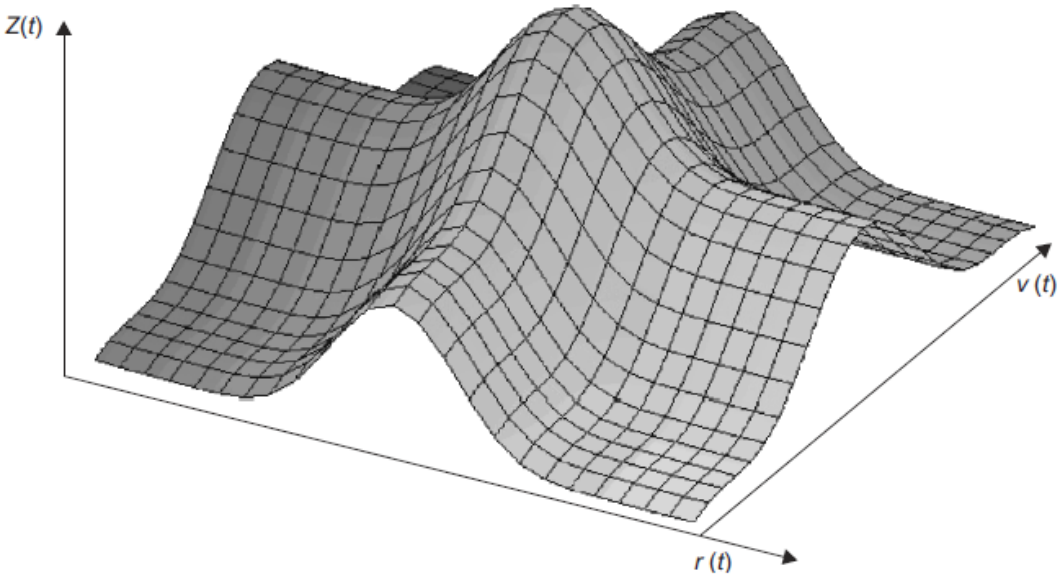
*Zdroj: prebraté z (Smejkal, Hortai, Molnárová, 2017b)*

Zaistenie bezpečnosti systému je nepretržitý proces. Dôvodom sú nové technológie a rozvoj ľudského poznania. Obe totiž umožňujú nové typy útokov a vyžadujú nutnosť priebežných inovácií ochrán. Práve preto čas môže vstupovať do výpočtu ako tretí faktor. Hodnota straty (aktív) sa časom mení a menia sa aj pravdepodobnosti výskytu udalostí spôsobené hrozbami. Ak by sme si na tretiu os vyniesli čas, môžeme modelovať predpokladanú veľkosť straty a jej veľkosť možno vypočítať, ako Z(t) v časovom intervale <0; $T_1$> ohraničeným integrálom, viď rovnicu nižšie a Obrázok 5.10:

$$Z_{(t)} = \int_0^{T1} r(t) \cdot v(t) \cdot d(t) \qquad (5)$$

Kde:

- r(t) je funkcia rizika v čase, vyjadrená pravdepodobnosťou z intervalu <0; 1 >,
- v(t) je funkcia straty alebo rizikového aktíva v čase.



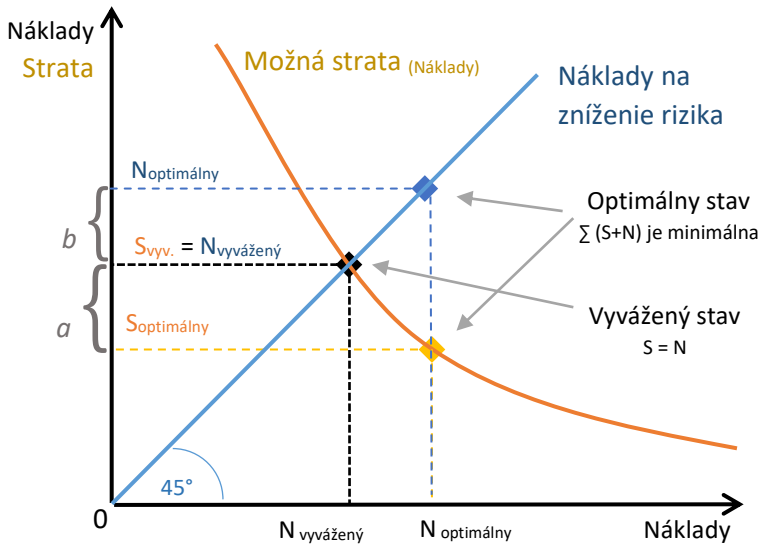

*Obrázok 5.10: Veľkosť predpokladané straty Z(t) v časovom intervale < 0 ; T0 >*

*Zdroj: (Smejkal, Rais, 2013, str. 108)*

Z(t) je veľkosť predpokladanej straty v časovom intervale <0; T1>, ktorú sa snažíme optimalizovať tak, aby bola jej výsledná hodnota minimálna. (Smejkal, Rais, 2013, str. 108)

Dôležitou súčasťou procesu rozhodovania o zníženia identifikovaných rizík sú náklady na zníženie rizika (Smejkal, Rais, 2013, str. 170). Súčasťou projektu na zníženie rizík teda musí byť aj cost-management (riadenie nákladov). Obrázok 5.11 zobrazuje ideálny či teoretický priebeh, ktorý sa v konkrétnom prípade môže trochu líšiť. Platí závislosť, že zvyšovanie nákladov na zníženie rizika znižuje kvantifikovanú možnú stratu. Podľa tejto závislosti existuje vyvážený stav medzi nákladmi na zníženie rizika a jeho výškou resp. škodou, ktorú môže hrozba spôsobiť (definované rovnicou 4 pri dosadnutí hranice, t, j. náklady sa rovnajú potenciálnej strate). Z pohľadu rentability sa ale do opatrení na zníženie alebo odstránenie rizika je vhodné investovať toľko, aby tieto investované náklady mali väčší efekt na znižovanie potenciálnej hroziacej škody, t. j. hľadá sa optimálny stav, kde suma nákladov a možnej straty je minimálna (definované rovnicou 6).

$$\sum(min) = Možná\ strata_{(Náklady)} + Náklady\ na\ zníženie\ rizika \qquad (6)$$




*Obrázok 5.11: Vzájomný vzťah nákladov na odstránenie rizika a potenciálnych škôd*

*Zdroj: vlastné spracovanie.*

Kde:

- Oranžová krivka znamená teoretický priebeh funkcie možnej straty, ktorá je závislá na vynaložených nákladoch na zníženie rizika.
- Modrá krivka reprezentuje náklady na zníženie rizika, ktorá vychádza z 0 (x=0 ; y=0) a osou x uzaviera 45 stupňový uhol.
- $N_{vyvážený}$ – reprezentuje hodnotu vynaložených nákladov na zníženie možnej straty na dosiahnutie stavu, keď sú si tieto hodnoty rovné ($S_{vyv.} = N_{vyvážený}$).
- $S_{vyv.}$ – reprezentuje hodnotu vyváženej potenciálnej straty, ktorá je ekvivalentné s tou hodnotou nákladov ($N_{vyvážený}$), ktoré boli vynaložené na dosiahnutie tohto stavu.
- $N_{optimálny}$ – sú optimálne náklady na zníženie rizika. Po tomto bode je rast nákladov na zníženie rizika väčší ako pokles možnej straty.
- $S_{optimálny}$ – je optimálna hodnota možnej straty. Po tomto bode je pokles možnej straty menší ako rast nákladov vynaložených na zníženie rizika.
- a > b; úsek *„a“* značí rozdiel medzi $S_{vyv.}$ a $S_{optimálny}$ a je menší ako úsek *„b“*, ktorý značí rozdiel medzi $N_{vyvážený}$ a $N_{optimálny}$ .

Z grafu (Obrázok 5.11) sa dá tiež odvodiť:

- nie je možné predpokladať nulové náklady na odstránenie rizika,
- 100 percentné odstránenie rizika môže vyžadovať až „nekonečne“ veľké náklady, ktoré sú nerentabilné z pohľadu investície. (Smejkal, Rais, 2013, str. 109)

Nezvládnutie kybernetickej bezpečnosti môže mať u firmách až likvidačný dopad. Napr. banky, pri ktorých by bolo zistené, že nie sú bezpečné, by to spôsobilo následné poškodenie dobrého mena banky, t. j. masový odliv klientov a cudzieho kapitálu. Iný príklad by mohol byť únik osobných údajov z personálnej agentúry, kde by existujúci a potenciálni klienti stratili motiváciu o kooperáciu s touto agentúrou, nehovoriac o možnej pokute vyplývajúcej z nedostatočného zapečenia osobných údajov v IS.

**Úspory nákladov vyplývajúce zo zavedenia systému**

Empiricky: tlak na neustále zvyšovanie efektívnosti podnikových procesov vyžaduje implementáciu nových technológií. Implementácia novej, či doteraz v podniku nepoužitej technológie bude mať za následok aj zmeny v podnikových procesoch. Vychádzajúc z empirickej úvahy, implementácia DBP do podnikových procesov prináša aj možné zmeny, viď kapitolu 5.4, kde DPB bol skúmaný z pohľadu operačnej analýzy a použiteľnosti v podnikových procesoch. Táto časť v sebe zahŕňa niekoľko praktických prístupov, ktorých cieľom bolo nájsť a sumarizovať hlavné prínosy, možné oblasti využitia, výhody a nevýhody DBP na podnikové procesy a všeobecne pre organizácie.

Náklady spojené so zavedením novej, či doteraz v podniku nepoužitej technológie (nákup, náklady pri implementácii, prevádzka atď.) pritom závisia na type použitej technológie, veľkosti spoločnosti, počte zamestnancov, atď. Empiricky: náklady na plne elektronický obeh dokumentov sa predpokladajú nižšie, než náklady na ich vedenie a obeh v listinnej forme. Na základe operačnej analýzy (kapitola 5.4.1) je úspora založená na znižovaní nákladov vyplývajúca zo zavedenia systému DBP:

- Pri spotrebných nákladoch:
    - znížená spotreba papiera,
    - znížená spotreba tonerov,
    - znížené vyťaženie skenerov,
    - znížené vyťaženie tlačiarní.
- Pri prevádzkových nákladoch (úspory procedurálne):
    - znížená tlač papierových dokumentov a používaní skenerov,
    - logistika (distribúcia, zber papierových dokumentov),
    - zrýchlenie procesov pri dokumentoch (zníženie nákladov pre ľudské zdroje),
    - eliminácia nákladov na prepísanie alebo digitalizáciu papierových dokumentov,

- náklady na skartáciu papierových dokumentov,
- archivačné náklady listinných dokumentov.

- Skryté náklady: straty pri kvalite spracovania listinných dokumentov.

Pre výpočet na porovnanie nákladov papierovej a digitálnej varianty obehu dokumentov alebo návratnosť investície je určený reprezentačný príklad z praxe pre jednu anonymnú spoločnosť. Pre výpočet návratnosti sa použil index ROI - Return on investment (Erdogmus et al., 2004; Phillips, 1997, str. 7-13):

$$ROI = \frac{diskontované\ výnosy}{diskontované\ náklady} \qquad (7)$$

Reprezentačný výpočet prípadovej štúdie viď v elektronických prílohách tohto dokumentu. Tento „business case study“ bol vypočítaný pre jedno centrum zdieľaných služieb, a to s významným prispením spoločnosti. Vypočítanie ROI bolo v prípade zaobstarania technológií a služieb pre *AP (Invoice) Processing* (procesy platenia účtov, faktúr a pohľadávok) oproti súčasnému stavu nákladov na spracovanie *AP* bez potrebnej technológie. Rentabilnosť tejto zmeny prípadovej štúdie je zhrnutá v nasledujúcej tabuľke:

*Tabuľka 5.2: Súhrnné výsledky rentabilnosti prípadovej štúdie*

| Rok | n+1 | n+2 | n+3 | n+4 | n+5 | n+6 |
|---|---|---|---|---|---|---|
| ROI | 107% | 132% | 142% | 148% | 151% | 153% |
| Relatívne | +7% | +32% | +42% | +48% | +51% | +53% |

*Zdroj: vlastné spracovanie podľa tabuľky v elektronických prílohách: „Business Case_scanservice_Shared service center.xlsx“.*

Tento reprezentačný príklad je orientačný a znázorňuje ekonomickú rentabilitu technológie podporujúcu elektronický obeh dokumentov. DBP vie plne podporiť elektronický obeh dokumentov. V prípade výpočtu návratnosti zavedenia DBP, je potrebné počítať aj s nákladmi na zaobstaranie a možný servis DBP systému, no v tomto prípade treba brať ohľad aj na rentabilnosť vyplývajúce z kybernetickej bezpečnosti. Prípadová štúdia bola doplnená teoretickým výpočtom s nasledovnými výsledkami:

*Tabuľka 5.3: Súhrnné výsledky rentabilnosti s rozšíreným výpočtom (s DBP)*

| Rok | n+1 | n+2 | n+3 | n+4 | n+5 | n+6 |
|---|---|---|---|---|---|---|
| ROI | 103% | 129% | 141% | 147% | 151% | 153% |
| Relatívne | +3% | +29% | +41% | +47% | +51% | +53% |

*Zdroj: vlastné spracovanie podľa tabuľky v elektronických prílohách: „Business Case_scanservice_Shared service center.xlsx“.*

Tento teoretický príklad vychádza z reálnej prípadovej štúdie ukázal, že DBP vie byť pre podnik rentabilný. Pre index ekonomickej efektívnosti, či celkový efekt rentability DBP viď diskusiu ďalej.

**Diskusia a zhrnutie tejto časti**

Reprezentované bolo na niekoľkých ukážkových príkladoch, že zvládnutie kybernetickej bezpečnosti má vplyv na dlhodobú stabilitu firmy (zníženie nákladov pri kybernetických útokoch, zvýšenie prínosov znížením rizika pokút napr. podľa GDPR, zaistenie business continuity apod.). Stanovená metóda pre horný prah nákladov pre kybernetickú bezpečnosť bola založená na základe rizikového managementu, kde mierou zvládnutia kybernetickej bezpečnosti je zníženie rizika.

**Náklady všeobecne:** náklady spojené so zavedením novej, či doteraz v podniku nepoužitej technológie (nákup, náklady pri implementácii, prevádzka atď.) závisia na type použitej technológie, veľkosti spoločnosti, počte zamestnancov, atď. V prípade zabezpečenia hlavnú úlohu hrá dôležitosť zabezpečených aktív, napr. či sa jedná o citlivé dáta alebo nie. Nemá zmysel zavádzať silne bezpečnú technológiu na údaje, ktoré ak by sa stratili alebo zneužili, tak by vznikli menšie škody ako samotný náklad na zavedenie tohto zabezpečovacieho systému (viď vzorec 6). Preto bol stanovený optimálny bod, do ktorého sa ešte oplatí znižovať riziko u firiem, t. j. rentabilne investovať.

Aplikovaním zistených znalostí je navrhnutý vzorec 7, kde $EE_{KT}$ prestavuje koeficient ekonomickej efektívnosti technológie kybernetickej bezpečnosti. V prípade rentabilnej investície $EE_{KT}$ má byť väčší alebo rovný 1. Keď $EE_{KT}$ má hodnotu menšiu ako 1 je prípad, pri ktorom je jednoznačné, že investícia bude nerentabilná. Keď je koeficient okolo hodnoty 1 treba zohľadniť časovú periódu, počas ktorej bude technológia používaná a tak doladiť jednotlivé hodnoty vzorca.

$$EE_{KT} = \frac{\begin{array}{c}(\text{Úspory zo zmien v podnikových procesoch vyplývajúce zo zavedenia systému}) + \\ (\text{Úspory vyplývajúce zo zvládnutia kybernetickej bezpečnosti}) + \\ (\text{Úspory zo zníženia daní dôsledkom investície})\end{array}}{\text{Celkové náklady vyplývajúce zo zavedenia systému}} \qquad (8)$$

DBP spadá pod problematiku kybernetickej bezpečnosti a preto je vzorec 7 aplikovateľný. Pri podniku investované náklady na DBP predstavujú kúpu softvéru, príslušného hardvéru, náklady súvisiace zo zaškolením personálu pre používanie a náklady na údržbu. Výsledná suma nákladov je závislá od všeobecných podmienok (viď

vyššie). Z operačnej analýzy bolo zistené a vymenované úspory vyplývajúce zo zavedenia systému DBP. Pri rozhodovaní musí management sám analyzovať pri ktorých konkrétnych procesov z vymenovaných vie použiť DBP. Podľa rozhodnutia implementácie je potrebné v podniku stanoviť „zmeny v podnikových procesoch vyplývajúce zo zavedenia systému“, ktoré v prípade DBP sú vymenované úspory nákladov vyplývajúce zo zavedenia systému. Všeobecne bolo ale dokazené že plne elektronická komunikácia zefektívňuje procesy a urýchľuje spracovanie údajov (kapitola 5.4).

Podľa implementácie treba vykalkulovať aj možné úspory vyplývajúce zo zvládnutia kybernetickej bezpečnosti. Tiež bolo dokázané, že DBP je výborná alternatíva pre zabezpečenie vnútropodnikovej komunikácie (pre viac viď ostatné aspekty).

Preto pri racionálnej implementácie pri DPB sa predpokladá hodnota $EE_{KT}$ väčšia ako 1.

## 5.6 Spoločenský a používateľský aspekt

Výskum má dve hlavné motivácie:

- Empiricky: výskumníci a profesionáli často strácajúcu „reálny“ pohlaď verejnej mienky na vlastný odbor. V konečnom dôsledku sa môže stať, že sa dištancujú od mienky laikov na danú tému.
- Metóda spätnej väzby prijímania technológie s používateľom a skúsenosti používateľov s danou technológiu.

Z vyššie uvedených dôvodov časť primárneho výskumu má za cieľ skúmať možný spoločenský aspekt DBP a zohľadniť aktuálnu mienku používateľov DBP a laikov. Výskum má tiež vyhodnotiť vedomosti respondentov ohľadne autentizačných systémov a zistiť ich stanovisko k autentizácii na báze podpisu.

### 5.6.1 Metodológia spoločenského a používateľského aspektu

Prijímanie informačných technológií používateľom prinieslo mnoho konkurenčných modelov, z ktorých každá má rôzne sady rozhodujúcich faktorov akceptácie (Venkatesh et al., 2003). Dotazníkový prieskum verejnej mienky a používateľov technológie vie výskumníka „opätovne zoznámiť“ s mienkou laikov a je priamy zdroj používateľských skúseností. Môže byť aj výborným nástrojom pre distribuovaný brainstorming na danú tému.

Preto bol zrealizovaný dotazníkový prieskum verejnej mienky. Nezávislý a anonymný výskum skúmal znalosti a mienky ľudí ohľadne kryptografie, kyberbezpečnosti

a elektronického snímania vlastnoručného podpisu. Výskum sa zameriaval na spoločenský vplyv kryptografických a autentizačných systémov ako v súkromnej, tak v podnikovej komunikácii. Súčasťou skúmania spoločenského aspektu boli aj otázky zamerané na používateľskú prívetivosť, t. j. ako sa používatelia cítia pri používaní. Dotazník navádzal respondentov, aby odpovedali na niekoľko otázok nasledujúce za sebou. Dotazník bol vyhotovený v niekoľkých jazykoch ako v papierovej verzii tak aj online.

Jazyk dotazníka bol voliteľný z nasledujúcich jazykov:

- český,
- slovenský,
- anglický.

Rôzne jazykové verzie sú si obsahovo ekvivalentné. Papierové a online verzie sú si obsahovo ekvivalentné, ale formátovo sú upravené pre danú kompatibilitu platformy. Papierové verzie dotazníka sú dostupné v elektronických prílohách vo forme dokumentu. Online dotazník je dostupný cez internet na nasledujúcej hlavnej webovej stránke, po ktorej nasleduje voľba jazyka dotazníka:

https://sites.google.com/view/dbs-survey/main

Online verzia bola distribuovaná cez iný skrátený a sledovateľný URL.

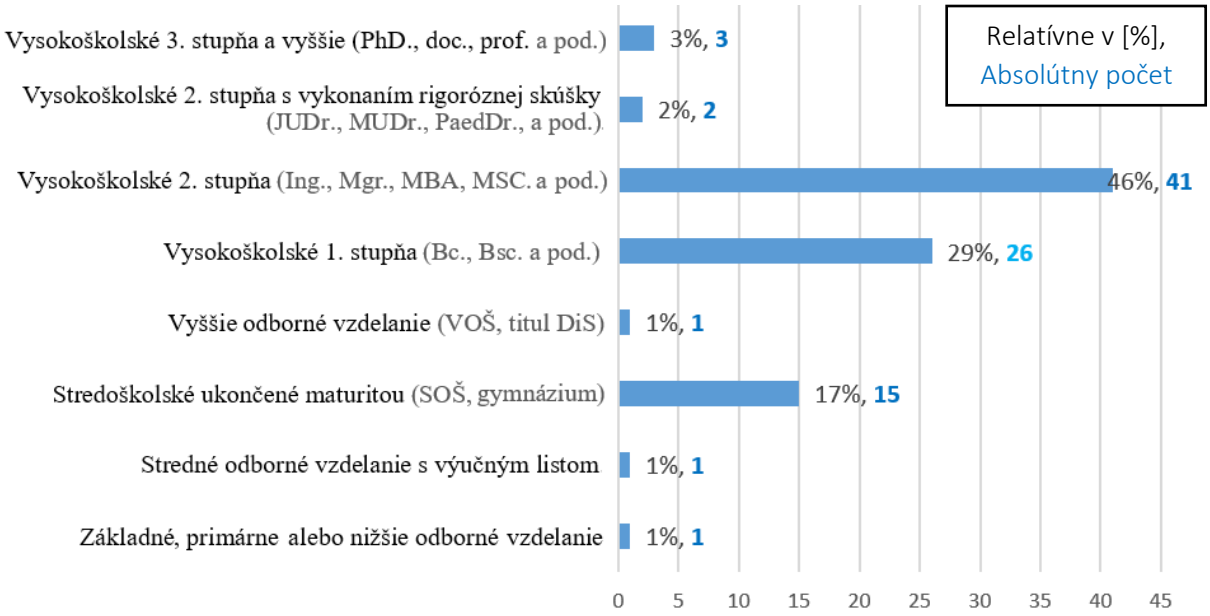
**Použitá vzorka**

Cieľová skupina sa snažila byť čo najviac heterogénna (rozdielne vekové skupiny, rozdielne povolania apod.).

Do 25. 06. 2018 samotný URL na webové rozhranie dotazníka bol otvorený 200 krát (stanovený míľnik kliknutí). Cez sociálne siete Facebook bol kliknutý 169-krát, cez e-mail 30-krát. Kliknutie cez servery na Slovensku 96-krát, v Česku 64-krát, v Maďarsku 16-krát a v ostatných krajinách EU 24-krát (z tých je 1 kontrolný). Dotazník do výsledku v online podobe bol vyplnený iba 87-krát (z výsledných 199 je relatívne 43,7 %) a 3-krát v papierovej verzii na Slovensku. Dotazník celkovo vyplnilo 90 osôb, s nasledujúcimi parametrami:

- Delenie podľa verzie dotazníka:
    - počet Online-CZ = 18
    - počet Online-SK = 49
    - počet Online-ENG = 20
    - počet Papier-SK = 3

- Vek respondentov:
  - priemer veku = 30.16
  - maximálny vek = 65 minimálny vek = 16
  - medián = 28 výberová odchýlka σ = 9.64
- Pohlavie respondentov:
  - počet žien = 47 relatívne 52 %
  - počet mužov = 42 relatívne 47 %
  - nebolo zistené = 1 relatívne 1 %
- Počet podľa najvyššieho dosiahnutého vzdelania:




- Podľa zamestnania: jednotlivci boli pracujúci manuálne alebo psychicky (akademik, administratívny pracovník, policajt, psychológ, právnik, robotník, študent, zamestnanec ministerstva apod.).

**Globálne platí na respondentov:**

U všetkých respondentov bolo zistené, že počítače a internet ovládajú minimálne na používateľskej úrovni.

**Hypotézy a priebeh vypracovania**

Výsledky dotazníkov boli sumarizované do jedného excelovského zošita (viď v elektronických prílohách) a vyhodnotené v príslušnej kapitole (viď kapitolu 5.6).

Zodpovedanie príslušnej výskumnej otázky, je výsledným argumentom nasledujúcich hypotéz a podotázok tejto časti:

- H 5.4.I: Subjektívne je kybernetická bezpečnosť dôležitá pre ľudí alebo pre spoločnosti.
- H 5.4.II: Subjektívne si ľudia myslia že majú znalosti o kryptografických technológiách.
- H 5.4.III: Ľudia majú reálne znalosti o kryptografických technológiách.
- H 5.4.IV: Ľudia vedia aký je rozdiel medzi elektronickým rozpoznaním vlastnoručného podpisu ako obrázka a DBP.
- V. O. 5.4.1: Je potrebné oboznámiť ľudí v prípade implementácie DBP?
- V. O. 5.4.2: Po neutrálnom oboznámení je pre ľudí DBP prijateľný?

### 5.6.2 Vyhodnotenie dotazníka

Prvých niekoľko otázok slúžilo na zber údajov o respondentovi. Potom nasledovali otázky, ktorých bolo niekoľko:

**Otázka 1:** *„Je kybernetická bezpečnosť dôležitá pre Vás alebo pre Vašu spoločnosť?“*

Respondenti mohli vybrať jednu odpoveď s nasledujúcou architektúrou:

({hodnota}. „*slovná odpoveď*“ ) = {počet odpovedí}

- (1. *Nedôležitá*) = 0
- (2. *Málo dôležitá*) = 2
- (3. *Neutrálny postoj*) = 17
- (4. *Dôležitá*) = 40
- (5. *Veľmi dôležitá*) = 31

Výsledný priemer hodnôt odpovedí je 4,11. Hodnota reprezentuje, že táto problematika je subjektívne pre respondentov medzi parametrom „*Dôležitá*“ a „*Veľmi dôležitá*“.

**Otázka 2:** *„Máte znalosti o kryptografických technológiách a viete aký je rozdiel medzi štandardným kryptografickým elektronickým podpisom a elektronickým rozpoznaním vlastnoručného podpisu?“*

Respondenti odpovedali v 27 % (24) ÁNO a 73 % (66) NIE. V prípade že odpovedali NIE, mali preskočiť na ďalšiu otázku s číslom 3. V prípade že odpovedali ÁNO, respondenti boli vyzvaný na kontrolu znalostí s nasledujúcimi otázkami *„a“* až *„i“*, na tieto otázky odpovedali 33. Z 33 boli vyfiltrovaní tí 24, ktorí odpovedali ÁNO na otázku 2:

- *a. Symetrická šifra, niekedy nazývaná aj konvenčná, je taký šifrovací algoritmus, ktorý používa k šifrovaniu a dešifrovaniu jediný kľúč.*

  Správna odpoveď tejto otázky je **Áno**. Odpovedali:

  Áno = 20 Nepravda = 0 Neviem = 4 Relatívne správne = 83 %

- *b. Asymetrické šifrovanie má dvojicu kľúčov - tajný a verejný.*

  Správna odpoveď tejto otázky je **Áno**. Odpovedali:

  Áno = 21 Nepravda = 0 Neviem = 3 Relatívne správne = 88 %

- *c. Kvalifikovaný elektronický podpis je ekvivalentom vlastnoručného podpisu, ktorým sa potvrdzujú právne úkony v listinnej podobe.*

  Správna odpoveď tejto otázky je **Áno**. Odpovedali:

  Áno = 18 Nepravda = 1 Neviem = 5 Relatívne správne = 75 %

- *d. Z klasického podpisu (perom na papieri) sa dá dospieť k všetkým dynamickým údajom procesu vytvárania (rýchlosť, tlak atď.) daného podpisu.*

  Správna odpoveď tejto otázky je Nepravda. Odpovedali:

  Áno = 13 Nepravda = 7 Neviem = 4 Relatívne správne = 29 %

- *e. Šifrovací kľúč a dešifrovací kľúč musia byť matematicky zviazané, avšak nevyhnutnou podmienkou pre užitočnosť šifry je praktická nemožnosť zo znalosti šifrovacieho kľúča vypočítať dešifrovací.*

  Správna odpoveď tejto otázky je Áno. Odpovedali:

  Áno = 16 Nepravda = 2 Neviem = 6 Relatívne správne = 67 %

- *f. Elektronickú značku môže v dátovej správe označovať aj právnická osoba alebo organizačná zložka štátu ako zaručený elektronický podpis.*

  Správna odpoveď tejto otázky je Áno. Odpovedali:

  Áno = 13 Nepravda = 1 Neviem = 10 Relatívne správne = 54 %

- *g. Elektronický podpis a elektronický dynamický biometrický podpis je tá istá technológia.*

  Správna odpoveď tejto otázky je Nepravda. Odpovedali:

  Áno = 1 Nepravda = 14 Neviem = 9 Relatívne správne = 58 %

- *h. Kvalifikovaný certifikát je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný (držiteľ certifikátu).*

  Správna odpoveď tejto otázky je Áno. Odpovedali:

Áno = 20 Nepravda = 0 Neviem = 4 Relatívne správne = 83 %

- *i. Kvalifikovaný certifikát nie je časovo obmedzený.*

  Správna odpoveď tejto otázky je Nepravda. Odpovedali:

  Áno = 4 Nepravda = 9 Neviem = 11 Relatívne správne = 17 %

Celkový percentuálny priemer správnych odpovedí je 62 %, tých ktorí odpovedali áno na otázku 2.

**Otázka 3:** *„Máte skúsenosti s elektronickým podpisom alebo kvalifikovaným certifikátom?“*

Respondenti odpovedali v 53 % (48) ÁNO a 47 % (42) NIE. Keď odpovedali áno, tak 3 najčastejšie odpovede v poradí frekvencie boli: bankový sektor alebo finančné služby; úrady a štátna správa; pracovné a Document Management System.

**Otázka 4:** *„Myslíte si, že používanie elektronického podpisu je dôveryhodným nástrojom na komunikáciu alebo autentizáciu?“*

Respondenti odpovedali v 70 % (63) ÁNO, 19 % (17) NEVIEM a 11 % (10) NIE.

**Otázka 5:** *„Máte skúsenosti so zariadením, ktoré skenuje váš vlastnoručný podpis?“*

Respondenti odpovedali v 43 % (39) ÁNO a 57 % (51) NIE. Keď áno, tak 3 najčastejšie odpovede v poradí frekvencie boli: banky, polícia, mobilné operátory.

**Otázka 6:** *„Myslíte si, že používanie elektronického zachytenia vlastnoručného podpisu je dôveryhodným nástrojom na komunikáciu alebo autentizáciu?“*

Respondenti odpovedali v 59 % (53) ÁNO, 24 % (22) NEVIEM a 17 % (15) NIE.

**Otázka 7:** *„Viete aký je rozdiel medzi technológiami, ktoré slúžia na zachytenie vášho vlastnoručného podpisu, napríklad pri podpise na zariadení, ktoré využíva iba obrázok podpisu (bežne používaná pri doručovaní zásielok) a snímaním dynamického biometrického podpisu?“*

Respondenti odpovedali v 40 % (36) ÁNO a 60 % (54) NIE.

**Po krátkom neutrálnom vysvetlení DBP nasledovala ďalšia časť:**

**Otázka 8:** *„Uvedená technológia: dynamický biometrický podpis by bola ako nástroj komunikácie alebo overovania prospešná pre Vás alebo Vašu spoločnosť (zjednodušenie a zvyšovanie efektívnosti komunikácie), alebo skôr by bola prekážkou?“*

Respondenti mohli vybrať jednu odpoveď s nasledujúcou architektúrou:

({hodnota}. „*slovná odpoveď*“ ) = {počet odpovedí}

- (1. *Nevýhoda*) = 0
- ( 2. *Skôr nevýhoda*) = 6
- (3. *Neutrálny postoj*) = 26

- (4. *Skôr výhoda*) = 40
- (5. *Výhoda*) = 15

Výsledný priemer hodnôt odpovedí je 3,73. Hodnota reprezentuje, že táto problematika je subjektívne pre respondentov medzi parametrom „Neutrálny postoj“ a bližšie k „Skôr výhoda“.

**Otázka 9:** *„Použitím technológie dynamického biometrického podpisu by sa zvyšovala bezpečnosť komunikácie u Vás alebo vo Vašej spoločnosti, alebo skôr by reprezentovala možnú hrozbu?“*

Respondenti mohli vybrať jednu odpoveď s nasledujúcou architektúrou:

({hodnota}. „*slovná odpoveď*“ ) = {počet odpovedí}

- (1. *Hrozba*) = 2
- (2. *Skôr hrozba*) = 3
- (3. *Neutrálny postoj*) = 31
- (4. *Skôr bezpečnosť*) = 42
- (5. *Väčšia bezpečnosť*) = 12

Výsledný priemer hodnôt odpovedí je 3,66. Hodnota reprezentuje, že táto problematika je subjektívne pre respondentov medzi parametrom „Neutrálny postoj“ a bližšie k „Skôr bezpečnosť“.

**Otázka 10:** *„V elektronickej komunikácii napríklad na podpísanie elektronických dokumentov, zmlúv atď. by ste preferovali používať svoj vlastnoručný podpis s technológiu dynamického biometrického podpisu (DBP) alebo iba pomocou kvalifikovaného (zaručeného) elektronického podpisu (KEP).“*

Respondenti odpovedali v 22 % (19) *„skôr by som zostal u KEP“*, a 78 % (67) „*skôr by som použil DBP“*.

Dotazník sa tu stretol s mienkou, v preklade: *„v mnohých prípadoch je stále potrebné mať pero a podpis, čo je absurdné. Každé z vyššie uvedených krokov by bolo zlepšením. Prosím vás, veď je 21. storočie“*.

**Otázka 11:** *„Vidíte rozdiely v použití kvalifikovaného (zaručeného) elektronického podpisu a dynamického biometrického podpisu? Vidíte výhody a nevýhody týchto systémov?“*

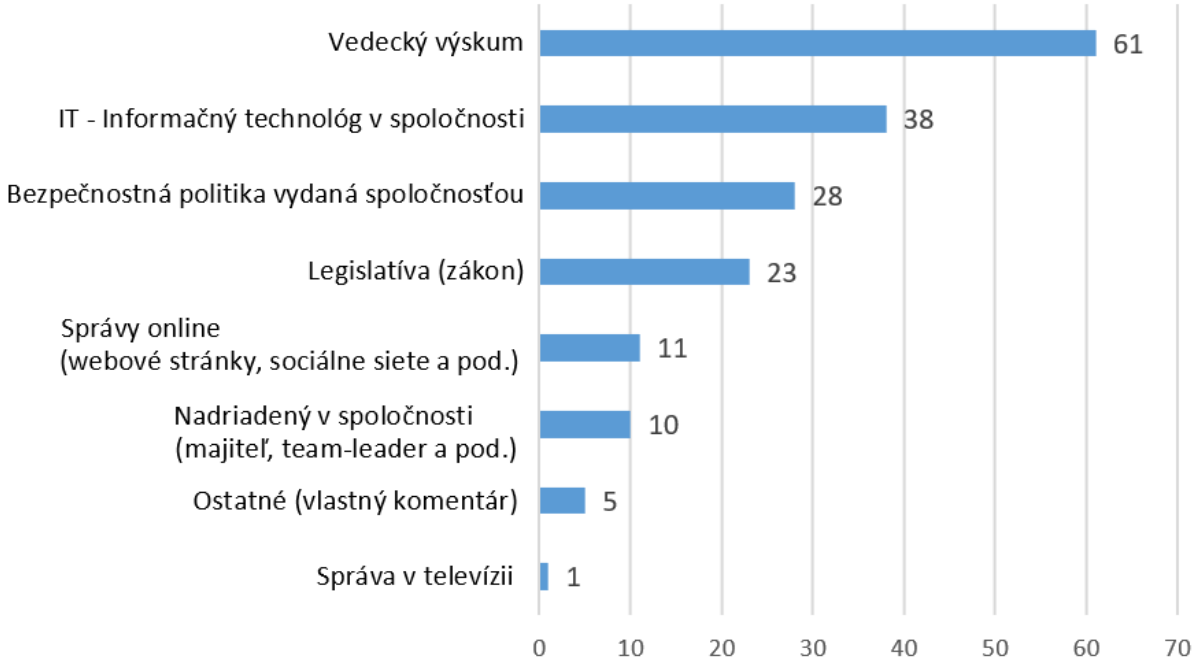
Respondenti odpovedali v 40,4 % (36) ÁNO, 47,2 % (42) NEVIEM a 12,4 % (11) NIE.

Dotazník sa tu stretol mienkami pri 11 komentárov na pozitívny prístup DBP (ťažiskom na bezpečnosť, efektívnosť, presnosť apod.). 1 prípad na negatívny komentár: *„Pokud*

*podepisuji něco za danou osobu, nelze použít DBP, ale u kvalifikovaného stačí karta s pinem. Ve větší firmě si to představit neumím, v malé kanceláři je důvěra nezbytná, spoustu běžných opakujících se věcí je potřeba podepisovat a stačí, aby se o to staral asistent/asistentka.“.*

**Otázka 12:** *„Kto alebo čo by Vás presvedčilo že táto technológia DBP je bezpečná a efektívna?“*

Respondenti mohli označiť viac odpovedí alebo pridať vlastný komentár, odpovedali:




**Otázka 13:** *„Aký spoločenský vplyv alebo zmenu v spoločnosti by mohla spôsobiť technológia dynamického biometrického podpisu? Alebo prosím doplňte iné subjektívne mienky o tejto technológie alebo dotazníka.“*

Celkovo odpovedali 32 komentárom. Väčšina odpovedí vidí skôr pozitívum v DBP. Z odpovedí vyplýva niekoľko mienok, ktoré dominovali:

- Spôsob väčšej bezpečnosti ako pri klasickom podpise.
- Mnoho ľudí by uprednostnilo bezpapierovú komunikáciu.
- Respondenti by ocenili úspory na papieroch aj vyplývajúcu ekologickosť.
- Rýchlosť (časové úspory pri schvaľovaní procesov).
- Kontroly a dostupnosť aj na diaľku.

Došlo aj k menšiemu množstvu skeptických odpovedí napr.: ako sa podpísať v *„prípade neschopnosti (zlomená ruka)“*; alebo tí, ktorí už majú zavedený kvalifikovaný certifikát, nevidia potrebu takéhoto systému DBP.

Otázka 13 slúžila aj ako priestor pre spätnú väzbu pre osoby zúčastnených na meraní stálosti podpisu pri zmenách polohy tela (viď kapitolu 5.8).

**Diskusia a zhrnutie tejto časti**

Pre potvrdenie alebo zamietnutie hypotéz bola použitá heterogénna vzorka a reprezentuje mienku respondentov dotazníka. Použitá vzorka svojou veľkosťou je pre určenie širokej verejnej mienky málo reprezentatívna (dotazník celkovo vyplnilo 90 osôb). Samotná vzorka napr. neberie do úvahy ľudí, ktorí nemajú skúsenosti s informačnými technológiami. Zistenia ale môžu byť použiteľné pre predpovede pri vyjadreniach o vzorkách, trendoch alebo rozdieloch medzi skupinami.

**H 5.4.I: Subjektívne je kybernetická bezpečnosť dôležitá pre ľudí alebo pre spoločnosti.**

Je **prijatá**. Z odpovedí 1. otázky dotazníka vyplýva, že táto problematika je subjektívne pre respondentov medzi parametrom „*Dôležitá*“ a „*Veľmi dôležitá*“.

**H 5.4.II: Subjektívne si ľudia myslia že majú znalosti o kryptografických technológiách.**

Je **zamietnutá**. Z odpovedí 2. otázky dotazníka vyplýva, že iba 27 % si myslí že má znalosti o kryptografických technológiách, pritom analyzovaná vzorka patrí do vzdelanejšej časti spoločnosti (cca 70 % respondentov má minimálne ukončený 1. vysokoškolský stupeň).

**H 5.4.III: Ľudia majú reálne znalosti o kryptografických technológiách.**

Je **zamietnutá**. Z hypotézy H 7.6.II vyplýva, že iba menšina respondentov predpokladá, že má určitú zlatosť o danej problematike. Respondenti, ktorí si ale myslia že majú znalosti o kryptografických technológiách pri krátkej kontrole týchto znalostí dosiahli iba celkový percentuálny priemer správnych odpovedí 62 %. Tým sa podporil fakt zamietnutia hypotézy.

**H 5.4.IV: Ľudia vedia aký je rozdiel medzi elektronickým rozpoznaním vlastnoručného podpisu ako obrázok a DBP.**

Je **zamietnutá**. Z odpovedí 7. otázky dotazníka vyplýva, že iba 40 % si myslí že pozná rozdiel. Pri celkovej analýze dotazníka má autor dojem, že laici nie že nevedia aký je rozdiel v snímaní podpisu off-line a on-line, ale si aj všeobecne mýlia pojmy elektronický podpis a elektronické snímanie podpisu.

**Predpoklad**

Z hypotéz 5.4.II, III a IV môžeme usúdiť, že respondenti majú nedostatok vedomostí ohľadne zabezpečovacích systémov. Možno konštatovať, že respondenti nerozlišujú spôsoby snímania zabezpečovacích systémov pri podpise.

- V. O. 5.4.1: Je potrebné oboznámiť ľudí v prípade implementácie DBP?

Z celkového vyhodnotenia dotazníka vyplýva, že v prípade implementácie DBP je racionálne rozhodnutie oboznámiť budúcich používateľov s technológiou DBP a vysvetliť im princíp funkčnosti pre zabezpečenie subjektívnej dôvery v tejto technológii. Dodatkom k tejto časti by mohli byť aj nazbierané skúsenosti pri meraní DBP v ostatných častiach primárneho výskumu, t. j. po vysvetlení používateľského prostredia boli užívatelia spokojnejší a predišlo sa zbytočnému zmätkovaniu pri používaní DBP. Preto je racionálne pri implementácii zabezpečiť školenia a sprístupniť krátky manuál o detailoch DBP a postup pri používaní.

- V. O. 5.4.2: Po neutrálnom oboznámení je pre ľudí DBP prijateľný?

Z odpovedí na otázok č. 9 až 13 vyplýva, že respondenti vo všeobecnosti majú pozitívny prístup k používaniu technológie DBP. Preto sa môže predpokladať, že verejnosť by uprednostnila (alebo prinajmenšom mala pozitívny postoj), aby používala DBP na autentizáciu, za predpokladu, že existuje bezpečné riešenie autentizácie pomocou DBP. Z otázky 12 vyplýva, že presvedčiť verejnosť o bezpečnosti DBP by mohlo byť prioritne: vedecký výskum, informačný technológ v spoločnosti a bezpečnostná politika vydaná spoločnosťou.

## 5.7 Technologický aspekt

Zariadenia na snímanie dynamického podpisu sa líšia podľa výrobcu spôsobom použitia a jeho významom, ale majú zhodnú vlastnosť použitia technológií citlivých na dotyk. Používajú sa špeciálne pady, tablety, PDA - Personal Digital Assistant (Martinez-Diaz et al., 2008) a notebooky s možnosťou dotykovej obrazovky.

Najprv sa skúmali poznatky z relevantnej vedeckej literatúry ako sú napríklad stabilita podpisu jedincov, vplyv okolností na proces podpisu, atď. Bolo to potrebné, aby výskum kontinuálne nadväzoval na skoršie publikované príspevky, ktoré sa konkrétne vzťahujú on-line DBP (Jain et al., 2002). Napr. nespochybniteľné prepojenie vytvoreného DBP s textom podpisovaného elektronického dokumentu bolo riešené v príspevkoch (Smejkal, Kodl, 2011; Smejkal, Kodl, Kodl Jr., 2013).

Boli vykonané základné experimenty preukazujúce unikátnosť DBP i odolnosť voči jeho falšovaniu (Smejkal, Kodl, 2014). Okrem potvrdenia jedinečnosti DBP je ďalším rozhodujúcim aspektom jeho stálosť. Podľa výskumu (Smejkal et al., 2015) možno dynamický biometrický podpis jednotlivca predpokladať za viac-menej konštantný. V tomto výskume sa zaoberali aj vplyvom alkoholu na stabilitu dynamického biometrického podpisu u viac homogénnej skupiny; unikátnosťou a odolnosťou podpisu proti falšovaniu u vysoko heterogénnej skupiny osôb vo veku od 12 do 92 rokov. Kolektív autorov (Smejkal et al., 2016) predniesli správu o vplyve stresu na stálosť dynamického biometrického podpisu, ktorá potvrdzuje, že stres nemá žiadny vplyv na stabilitu podpisu (hladinou významnosti 0,01).

Tieto výskumy sa zaoberali zmenami týkajúce sa signatára alebo vplyvmi jeho okolia na podpisovú situáciu, pričom použité zariadenie bolo vždy rovnaké, z čoho vyplýva, že snímajúce zariadenie v týchto prípadoch vystupovalo ako invariant. Preto sa indukoval návrh experimentu, ktorý nadväzuje na výskumy tejto technológie.

### 5.7.1 Metodológia technologického aspektu

Indukovaný experiment sa zameriava na možnosť prípadného vplyvu na kvalitu dát a stálosť DBP pri používaní rôznych snímacích zariadení rovnakou osobou. Na experiment sa použili všetky dostupné snímače výrobcu Signotec (Signotec GmbH, pre viac informácií viď webové stránky spoločnosti: www.signotec.com, 2018). Snímače sa od seba líšili vlastným prevedením, veľkosťou podpisového poľa, rozlíšením, rýchlosťou vzorkovania, dokonca aj použitou metódou snímania - bežné pero alebo špeciálne pero používajúce ERT

(Electromagnetic Resonance Technology). Účelom experimentov bolo poukázať na prípadnú zmenu stability DBP podpisovateľa v závislosti od použitého snímacieho zariadenia.

Nasledujúce hypotézy boli formulované:

- I. časť predpokladá, že pokusné osoby sa rôzne ťažko vyrovnávajú s meniacimi sa okolnosťami podpisu v závislosti na technickom prevedení snímača:
    - H 5.5.I.0 - stabilita podpisov pre danú osobu na jednotlivých zariadeniach sa podstatne nemení (priemer a rozptyl miery zhody podpisov pre každé zariadenie patrí do rovnakého základného súboru),
    - H 5.5.I.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri jednotlivých zariadeniach pre danú osobu.
- II. časť predpokladá, že stabilita podpisov dosahovaná na jednotlivých zariadeniach sa bude štatisticky významne odlišovať.
    - H 5.5.II.0 - priemerná miera a rozptyl zhody podpisov pre jednotlivé snímače sa podstatne nemení (priemer a rozptyl miery zhody podpisov pre každé zariadenie patrí do rovnakého základného súboru),
    - H 5.5.II.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri jednotlivých zariadeniach.

**Použitá vzorka**

Pre potvrdenie alebo zamietnutie hypotézy bola použitá heterogénna vzorka, pretože sa jednalo o osoby od 20 do 65 rokov oboch pohlaví. Celkovo bolo použitých 8 skenerov kde sa jedinci podpisovali na každom 10 krát (celkovo 80 podpisov na jednu osobu). Vzorkovacia frekvencia bola nastavená na 250 Hz (bodov za sekundu). Proces experimentu podstúpilo 40 ľudí. Vzorka svojou veľkosťou je štatisticky dostatočne reprezentatívna.

**Použité prístroje experimentu**

Testovanie sa uskutočnilo na nasledujúcich snímačoch dynamického biometrického podpisu spoločnosti Signotec GmbH s rôznymi technickými parametrami vyrobených v rozmedzí posledných piatich rokov:

*Tabuľka 5.4: Snímacie zariadenia DBP*

| **Spôsob zaznamenania podpisu** | **Model snímača dynamického biometrického podpisu** |
|---|---|
| Aktívne pero, display a pero sú vzájomne synchronizované | Signotec Alpha Pad<br>ST-A4E-2-UFTE100: Colour LCD Signature Pad Alpha ERT *(Electromagnetic Resonance Technology)* |
| Display je elektromagnetický, tlak je zaznamenávaný na základe prítlaku pasívneho pera na display | Signotec Delta Pad<br>Dotykový display ST-DERT-3-U100 |
| | Signotec Gamma Pad<br>Dotykový display ST-GERT-3-U100: 5" Colour LCD Signature Pad Gamma ERT |
| Display je dotykový, tlak je zaznamenávaný na základe prítlaku pasívneho pera | Signotec Omega Pad revize B<br>Dotykový display ST-CE1075-2-U100 (stará verzia) |
| | Signotec Omega Pad revize E<br>Dotykový display ST-CE1075-2-U100 (aktuálna verzia) |
| | Signotec Sigma Pad revize B<br>Dotykový display ST-ME105-2-U100-B (stará verzia) |
| | Signotec Sigma Pad revize E<br>Dotykový display ST-ME105–2– U100-B (aktuálna verzia) |
| Display neexistuje, iba dotyková plocha | Signotec Sigma Lite<br>Dotyková plocha bez displaya ST-LT105-2-U100 |

*Zdroj: vlastné spracovanie.*

Detailné špecifikácie prístrojov, manuály od výrobcu a výrobné čísla sú dostupné v elektronických prílohách tejto práce.

**Miesto a výskumný tým experimentu**

Experiment sa uskutočnil dňa 09. 05. 2017 v počítačovej miestnosti na MVŠO - Moravská vysoká škola Olomouc. Prítomné dohliadajúce osoby vykonaného experimentu boli:

- prof. Ing. Vladimír Smejkal, CSc. LL. M.
- Ing. Ladislav Sieger, CSc. (FEL ČVUT v Praze)
- Ing. Jindřich Kodl, CSc. (súdny znalec v oboru kybernetika)
- Ing. Jiří Ehleman (spoločnosť Contrisys, s.r.o.)
- Ing. Pavel Vaněček (spoločnosť Contrisys, s.r.o.)
- Ing. et Ing. František Hortai - (autor dizertačnej práce)

### 5.7.2 Vypracovanie

Výskumy sa zaoberali zmenami týkajúce sa signatára alebo vplyvmi jej okolia na podpisovú situáciu, pričom použité zariadenie bolo vždy rovnaké, t. j. zariadenie vystupovalo ako invariant. Preto sa indukovala otázka prípadného vplyvu na kvalitu dát a stálosť DBP pri používaní rôznych snímacích zariadení rovnakou osobou. V tejto časti sú popísané experimenty, ktoré sa týkali vplyvu použitia rôznych zariadení (padov) na dynamické biometrické podpisy danej osoby. Získané výsledky kontinuálne nadväzujú na predchádzajúce publikované príspevky.

V experimentoch sa použili všetky dostupné snímače výrobcu Signotec, ktoré sa od seba líšia vlastným prevedením, veľkosťou podpisového poľa, rozlíšením, rýchlosťou vzorkovania, alebo použitou metódou snímania - bežné pero alebo špeciálne pero používajúce ERT (Electromagnetic Resonance Technology). Pre zoznam použitých prístrojov viď tabuľku: *Tabuľka 5.4: Snímacie zariadenia DBP*. Účelom experimentov bolo ukázať prípadnú zmenu stability DBP podpisovateľa v závislosti na použitom snímacom zariadení.

Pre zvýšenie použiteľnosti systému DBP z realizovaných experimentov (Smejkal, Kodl, 2014; Smejkal et al.,2015; Smejkal, Kodl, Sieger, 2016) vyplýva, aby prvý podpis subjektu bol vynechaný pri vytváraní vzorového podpisu, aby sa tým zvýšila celková stabilita podpisov. V priebehu automatického vyhodnocovania biometrického podpisu sa tým dá zvýšiť stupeň prijatých autentizovaných podpisov. Bolo dokázané, že kvalita rozpoznania podpisu stúpa s dĺžkou napísanej informácie - dĺžkou podpisu (Smejkal, Kodl, Sieger, 2016).

**Meranie a správa údajov**

Na zariadeniach boli snímané DBP pomocou programu spoločnosti signotec *signoSign2* verzia 10.4.5. Každý účastník vytvoril na každom zariadení 10 podpisov, takže vznikla matica podpisov každého účastníka $\overline{P}_{i,j}$ takto:

$$\overline{P}_{i,j} = [x1, \dots, x10]_{i,j} \qquad (9)$$

kde je $i$ – poradové číslo zariadení (1 až 8), $j$ – poradové číslo účastníka (1 až 40), $P$ – konkrétny podpis.

V súlade s poznatkami zistenými v predchádzajúcich experimentoch (Smejkal & Kodl, 2014; Smejkal et al.,2015; Smejkal, Kodl, Sieger, 2016) prvé podpisy na všetkých zariadeniach

všetkých účastníkov síce boli nasnímané ale neboli do vyhodnotenia zaradené. Preto matica podpisov bola upravená a indexovo doladená na: $\overline{P}_{i,j}$ = [x1 … x9] $_{i,\,j}$ .

Ako základ vyhodnotenia experimentov sa skúmala miera zhody medzi podpismi každej osoby v rámci každého zariadenia. Z pôvodnej matice a z upravenej matice podpisov $\overline{P}_{i,j}$ je pomocou vlastného programu, ktorý používa originálny engine pre zhody dynamického biometrického podpisu používaný od spoločnosti signotec (napr. u programu *Signotec RSA Verifier* alebo *eSig-Analyze*), vytvorená tabuľka kombináciami možných zhodných podpisov, kde funkcia $f(a_x\ ,\ a_y)$ je výstup funkcie algoritmu zhody podpisov a znamená percentuálnu zhodu daných podpisov $a_x$ a $a_y$ s nasledujúcou architektúrou matice $Z_{i,j}$ (pre upravenú tabuľku bez 1 podpisu matica *9* nižšie; pre plnú tabuľku aj s kombináciami s 1. podpisom):

$$Z_{\mathrm{ij}} = \begin{bmatrix} - & f(a_1\ ,\ a_2) & f(a_1\ ,\ a_3) & f(a_1\ ,\ a_4) & f(a_1\ ,\ a_5) & f(a_1\ ,\ a_6) & f(a_1\ ,\ a_7) & f(a_1\ ,\ a_8) & f(a_1\ ,\ a_9) \\ - & - & f(a_2\ ,\ a_3) & f(a_2\ ,\ a_4) & f(a_2\ ,\ a_5) & f(a_2\ ,\ a_6) & f(a_2\ ,\ a_7) & f(a_2\ ,\ a_8) & f(a_2\ ,\ a_9) \\ - & - & - & f(a_3\ ,\ a_4) & f(a_3\ ,\ a_5) & f(a_3\ ,\ a_6) & f(a_3\ ,\ a_7) & f(a_3\ ,\ a_8) & f(a_3\ ,\ a_9) \\ - & - & - & - & f(a_4\ ,\ a_5) & f(a_4\ ,\ a_6) & f(a_4\ ,\ a_7) & f(a_4\ ,\ a_8) & f(a_4\ ,\ a_9) \\ - & - & - & - & - & f(a_5\ ,\ a_6) & f(a_5\ ,\ a_7) & f(a_5\ ,\ a_8) & f(a_5\ ,\ a_9) \\ - & - & - & - & - & - & f(a_6\ ,\ a_7) & f(a_6\ ,\ a_8) & f(a_6\ ,\ a_9) \\ - & - & - & - & - & - & - & f(a_7\ ,\ a_8) & f(a_7\ ,\ a_9) \\ - & - & - & - & - & - & - & - & f(a_8\ ,\ a_9) \\ - & - & - & - & - & - & - & - & - \end{bmatrix} \quad (10)$$

Kde značenie „ – “ sa týka porovnávania rovnakej (napr. $f(a_1\ ,\ a_1)$), či tej istej dvojice podpisov a preto sú z matice vynechané, nedefinované (prevencia proti duplicite údajov napr. $f(a_1\ ,\ a_2)$ a $f(a_2\ ,\ a_1)$).

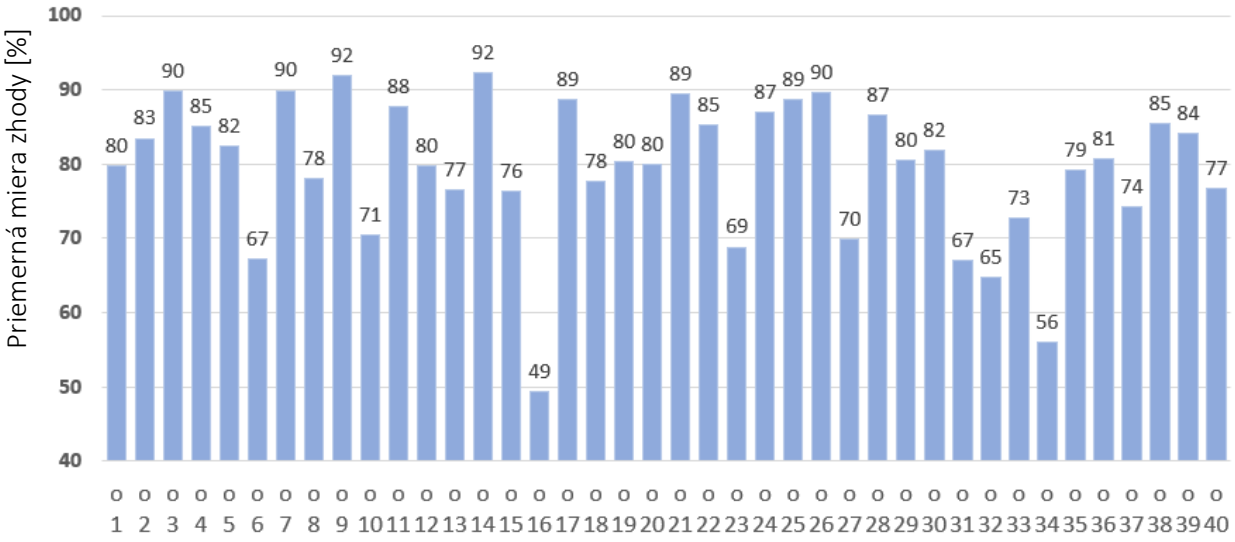
Výsledným výstupom sú matice, či tabuľky s hodnotami zhôd v trojuholníkovom tvare $Z\ i,j$ ; kde je: $i$ – poradové číslo zariadení (1 až 8) a $j$ – poradové číslo účastníka (1 až 40).

**Testovanie hypotéz I. časti**

V prvej časti vyhodnotenia experimentov bola zisťovaná miera zhody medzi podpismi každej osoby v rámci každého zariadenia z hodnôt tabuliek Z $_{i,\,j}$ . Pre každé zariadenie bola stanovená priemerná zhoda podpisov danej osoby na danom zariadení $\overline{x}$, výberový rozptyl zhody $s^2$ a výberová smerodajná odchýlka $s$. Týmto spôsobom bolo získané u príslušných podpisoch každej osoby na každom zariadení vektor zhôd $\overline{x}_1$ až $\overline{x}_8$, vektor výberových rozptylov $s_1^2$ až $s_8^2$ a vektor výberových smerodajných odchýlok $s_1$ až $s_8$.

Iba pri dvoch osobách (č. 16 a č. 34) sa priemerná miera zhody podpisov dostala pod priemernú mieru zhody biometrických podpisov (viď *Obrázok 5.12*), ktorá sa

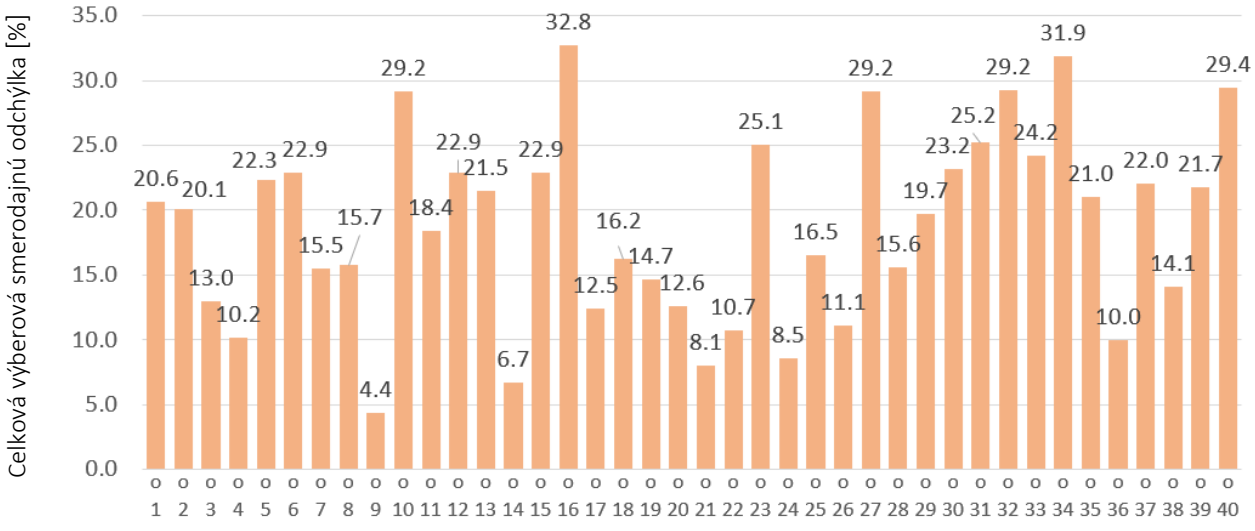
v predchádzajúcich experimentoch (Smejkal et al., 2015; Smejkal et al., 2016) pohybovala v intervale 70 % až 90 %, ale vždy bola > 60 %, a to aj za situácie ovplyvnenia testovanej osoby alkoholom alebo stresom.




*Obrázok 5.12: Priemerná miera zhody podpisov jednotlivých osôb*

*Zdroj: vlastné spracovanie.*

Viac vypovedá graf na *Obrázok 5.13*, ktorý ilustruje celkovú výberovú smerodajnú odchýlku *„s“* pre všetky osoby, t. j. akú celkovú „nestabilitu“ mieru zhody medzi podpismi prejavovali počas celého merania.




*Obrázok 5.13: Celková výberová smerodajná odchýlka jednotlivých osôb*

*Zdroj: vlastné spracovanie.*

Celkový výsledok charakterizujúci technológiu ako celok, teda bez rozlíšenia typu zariadenia a podpisujúcej sa osoby (t. j. pre všetky osoby na všetkých zariadeniach) je nasledovný:

*Tabuľka 5.5: Súhrnné výsledky miery zhody podpisov (bez 1. podpisu)*

| x [%] | $\sigma^2$ | σ |
|---|---|---|
| 79,33 | 173,29 | 13,16 |

*Zdroj: vlastné spracovanie.*

*Tabuľka 5.6: Súhrnné výsledky miery zhody podpisov (spolu s 1. podpisom)*

| x [%] | $\sigma^2$ | σ |
|---|---|---|
| 78,02 | 180,30 | 13,43 |

*Zdroj: vlastné spracovanie.*

Rozdiely hodnôt v tabuľkách: *Tabuľka 5.5* a *Tabuľka 5.6* opäť potvrdili, že vynechaním prvého podpisu vo výsledkoch znižujeme variabilitu podpisu pre každého účastníka. Prvý podpis v tomto prípade predstavuje „skúšobný“ proces podpisu.

Ďalej sa predpokladá, že nezávislé náhodné výbery pochádzajú z normálnych rozdelení so strednými hodnotami $\mu_1, \mu_2 \ldots. \mu_r$ s rovnakým rozptylom $\sigma^2$.

Bol použití Bartlettov test (Snedecor, Cochran, 1989) na testovanie zhodnosti rozptylov miery zhody podpisov na všetkých zariadeniach u každého probanda. Hodnoty B testu sa pohybovali cca. od 20 do 610, t. j. P-value = 0.00. U všetkých probandov bola preto zhodnosť rozptylov miery zhody podpisov na všetkých zariadeniach zamietnutá na hladine významnosti 0.01 a teda aj na hladine významnosti 0.05 (pretože P-value <0.01).

Test jednoduchého triedenia (analysis of variance, ANOVA) sa preto nedal použiť. U každej osoby boli Cochran-Cox testom (Cochran & Cox, 1957) testované všetky dvojice zariadení s hypotézou párovej zhody priemerov miery zhody podpisov na hladine významnosti 0.01 a 0.05. Pri testovaní párovej zhody priemerov sa pri niektorých prípadoch hodnoty dvojíc zhodovali (boli prijaté na danej hladine významnosti) avšak nie pri všetkých možných dvojiciach (ani pri jednom probandovy sa nezhodovali všetky dvojice na hladine významnosti 0.01 a ani na hladine významnosti 0.05). Preto sa výsledne zamieta zhodnosť priemerov miery zhody podpisov na hladine významnosti 0.01 a teda aj na hladine významnosti 0.05.

Z testovaní vyplýva, že nulová hypotéza: *H 5.5.I.0 stabilita podpisov pre danú osobu na jednotlivých zariadeniach sa podstatne nemení (priemer a rozptyl miery zhody podpisov pre každé zariadenie patrí do rovnakého základného súboru),* **sa zamieta**, a to na hladine významnosti 0.01 a aj na hladine významnosti 0.05.

Variabilita podpisov (rozptyl miery zhody) je pri jednotlivých testovacích osobách na rôznych zariadeniach pomerne vysoká, čo znamená, že niektoré osoby sa vyrovnávali horšie s rôznymi prevedeniami zariadení.

**Testovanie hypotéz II. časti**

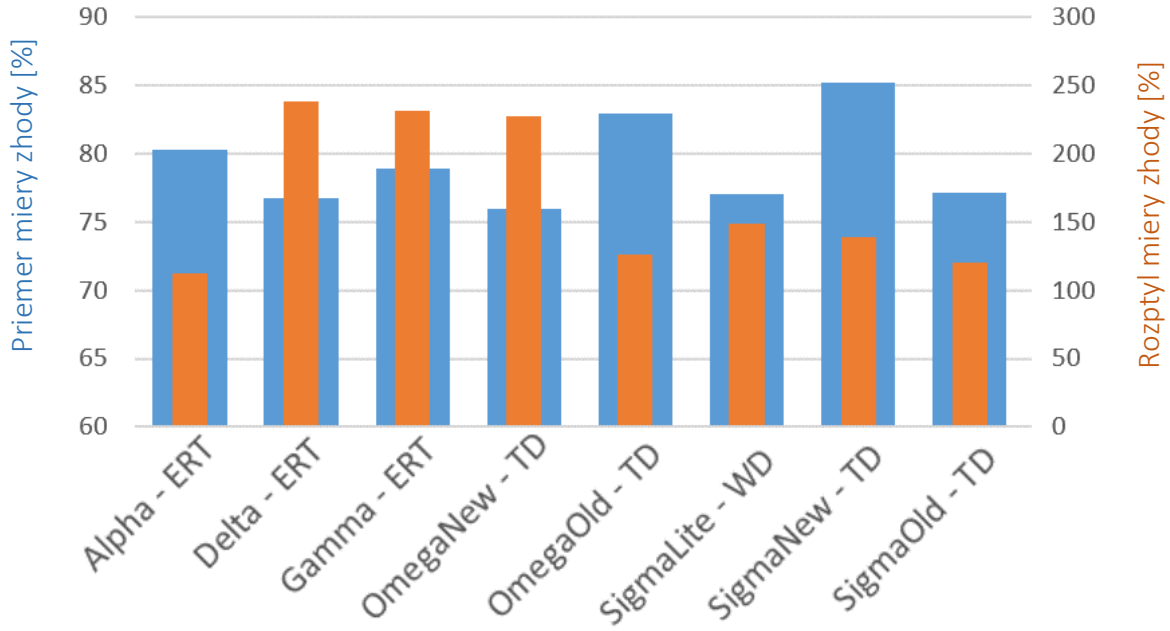
Zistené boli nasledujúce hodnoty priemerov a rozptylov miery zhody podpisov pre uvedené zariadenia:

*Tabuľka 5.7: Priemer a rozptyl miery zhody podpisov testovaných zariadení*

| ***Zariadenie Signotec*** | Priemerná zhoda podpisov zariadenia x [%] | Výberový rozptyl $s^2$ [%] |
|---|---|---|
| *Alfa* | 80.34 | 113.02 |
| *Delta x* | 76.75 | 238.27 |
| *Gamma* | 78.97 | 232.03 |
| *OmegaNew* | 76.02 | 228.05 |
| *OmegaOld* | 83.00 | 125.84 |
| *SigmaLite* | 77.10 | 148.57 |
| *SigmaNew* | 85.23 | 139.19 |
| *SigmaOld* | 77.20 | 120.34 |

*Zdroj: vlastné spracovanie.*

*Obrázok 5.14: Priemerná miera zhody a rozptylu podpisov pri jednotlivých zariadeniach*




ERT – Electromagnetic Resonance Technology; TD – Dotykový display; WD - Dotyková plocha bez displaya

*Zdroj: vlastné spracovanie.*

Zhoda rozptylov bola overená Bartlettovým testom (B= 11.206, k-1 = 7, α = 0.01 a 0.05, P-value= 0.0588). Z týchto výsledkov vyplývalo, že zhoda všetkých rozptylov sa dá prijať na hladine významnosti 0.01 i na hladine významnosti 0.05.

Test jednoduchého triedenia (ANOVA) (Cochran & Cox, 1957) poskytol výsledky (F=2.565, k=7, n-k=306, α = 0.01 a 0.05, $F_{0.01}$=2.6991 a $F_{0.05}$=2.0391, kde $F_{1-\alpha}$ (k -1, n-k) je (1- α) kvantil Fisherova-Snedecorova rozdelenia pre hladinu významnosti α), takže zhoda všetkých priemerov bola prijatá na hladine významnosti 0.01 a zamietnutá na hladine významnosti 0.05.

Výsledky Scheffého testu mnohonásobného porovnávania (Scheffé, 1999) umožnili určiť, medzi ktorými dvoma vyššie uvedenými súbormi dát existujú štatisticky významné rozdiely. Scheffeho test prijíma na hladine významnosti 0.01 i 0.05 rovnosť všetkých 28 dvojíc priemerov miery zhody podpisov.

Nulová hypotéza H 5.5.II.0 je prijatá, lebo neboli preukázané rozdiely medzi priemernými hodnotami miery zhody (x) a medzi hodnotami rozptylu miery zhody ($\sigma^2$) pri používaní rôznych zariadení, a to pri rozptyloch na hladine významnosti 0.05 a pri priemeroch na hladine významnosti 0.01. Možno teda konštatovať, že napriek technologických rozdielov v jednotlivých zariadeniach sa stabilita podpisov pri zmene zariadenia nemení, líši sa však variabilita (rozptyl, resp. smerodajná odchýlka) pri jednotlivých zariadeniach.

### 5.7.3 Diskusia a záver tejto časti

Všetky údaje sú dostupné v elektronických prílohách tejto práce. Postup a príklad výpočtov meraní sú na prílohách na konci tohto dokumentu (*Príloha II: výpočty analýzy technologického aspektu.*).

**Hypotézy I. časti** predpokladali, že pokusné osoby sa rôzne ťažko vyrovnávajú s meniacimi sa okolnosťami podpisu v závislosti na technickom prevedení snímača. Bola vyvrátená nulová hypotéza H 5.5.I.0 o tom, že stabilita podpisov pre danú osobu na jednotlivých zariadeniach sa podstatne nemení, a to na hladine významnosti 0.01, a tak aj na hladine významnosti 0.05. Tým sa potvrdila hypotéza H 5.5.I.1 o tom, že existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri jednotlivých zariadeniach pre danú osobu.

**Hypotézy II. časti** predpokladali, že stabilita podpisov dosahovaná na jednotlivých zariadeniach sa bude štatisticky významne odlišovať. V tomto prípade bola potvrdená nulová

hypotéza o H 5.5.II.0 o tom, že priemerná miera a rozptyl zhody podpisov pre jednotlivé snímače sa podstatne nemení, pretože neboli preukázané rozdiely medzi hodnotami priemerov a rozptylov miery zhody pri používaní rôznych zariadení, a to pri rozptyloch na hladine významnosti 0.05 a pri priemeroch na hladine významnosti 0.01. Hypotéza H 5.5.II.1 sa preto zamieta.

**Všeobecný záver výsledkov:** Tejto časti výskumu sa zúčastnilo 40 použiteľných probandov, a tak reprezentujú štatisticky reprezentatívnu vzorku. Výsledky ukázali, že priemerná miera zhody jednotlivých osôb síce vysoká (iba u 2 osôb klesla pod 60%), ale variabilita podpisov (rozptyl miery zhody) je pri jednotlivých osobách na rôznych zariadeniach pomerne vysoká, čo znamená, že niektoré osoby sa vyrovnávali horšie s rôznym prevedením zariadení. Bez ohľadu na individuálne vlastnosti signatárov boli priemerné hodnoty zhody podpisov všetkých osôb na všetkých zariadeniach vysoké (od 76 do 85) a neboli preukázané štatisticky významné rozdiely medzi hodnotami priemerov a rozptylov miery zhody pri používaní rôznych zariadení, a to pri rozptyloch na hladine významnosti 0.05 a pri priemeroch na hladine významnosti 0.01. Z výsledkov vyplýva, že technológie snímania DBP nemajú vplyv na mieru zhody a variabilitu podpisov.

Kľúčovým faktorom by mohla byť pre signatára „používateľská prívetivosť“, resp. ostatné okolnosti pri vytváraní podpisu. Aby sa dali objektívne posúdiť možné iné exogénne vplyvy pri stabilite podpisu je táto problematika skúmaná ďalej (viď nasledujúcu kapitolu 5.8).

## 5.8 Technologicko-používateľský aspekt

Z poznatkov z relevantnej vedeckej literatúry sekundárneho výskumu, ďalej z publikácií zmienených v časti primárneho výskumu v kapitole 5.7.1 Metodológia technologického aspektu ) napr. (Smejkal et al., 2015; Smejkal et al. 2016) a výskumy ako sú napríklad (Diaz et al., 2015; Pirlo et al., 2013) bol zistený ďalší invariant výskumu, a to pozícia tela podpisujúcej sa osoby. Tieto výskumy sa zaoberali zmenami týkajúce sa signatára alebo vplyvmi jeho okolia na podpisovú situáciu, pričom použitá pozícia tela bola rovnaká alebo nebola vôbec znázornená. Preto sa indukoval experiment, ktorý bol zameraný práve na túto problematiku, a to na polohu tela signatára.

### 5.8.1 Metodológia technologicko-používateľského aspektu (poloha tela)

Indukovaný experiment sa zameriava na možnosť prípadného vplyvu na kvalitu dát a stálosť DBP pri používaní rôznych polôh tela osoby pri podpisovaní a snímaní DBP na snímacie zariadenie rovnakého typu.

Nasledujúce hypotézy a výskumné otázky boli formulované:

- I. časť predpokladá, že celková stabilita podpisov dosahovaná pri jednotlivých pozíciách tela signatára sa budú štatisticky významne odlišovať.
    - H 5.6.I.0 - priemerná miera a rozptyl zhody podpisov pre jednotlivé pozície sa podstatne nemenia (priemer a rozptyl miery zhody podpisov pre každú pozíciu patrí do rovnakého základného súboru),
    - H 5.6.I.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri niektorých pozíciách.
- II. časť V prípade prijatia alternatívnej hypotézy sú skúmané výskumné otázky:
    - V.O. 5.6.I Ktoré pozície sú si ekvivalentné z pohľadu podpisovej stability? Pozície, kde priemer a rozptyl miery zhody podpisov patrili do rovnakého základného súboru.
    - V.O. 5.6.II Aký exogénny faktor spôsobil rozdiel pri stabilite podpisu u signatára?
    - V.O. 5.6.III Je stabilita skôr závislá na exogénnych faktoroch, alebo skôr na individuálnych charakteristikách signatára?

Spracovanie údajov a výpočtov boli zhrnuté v excelovskom zošite (viď elektronické prílohy) a znázornené na prílohách na konci dokumentu (*Príloha III: výpočty analýzy technologicko-používateľského aspektu (polohy tela)*). Vypracovanie viď v kapitole 5.8.2.

**Použité prístroje experimentu**

Testovanie sa uskutočnilo na snímačoch dynamického biometrického podpisu od spoločnosti *Signotec GmbH*:

- signotec LCD Signature Pad Omega.

Celkovo bolo použitých súbežne 10 prístrojov pripojených každý prístroj zvlášť na PC vybavenie. Vzorkovacia frekvencia bola nastavená na 250 Hz (bodov za sekundu). Výrobné čísla a špecifikácie snímačov sú dostupné v elektronických prílohách tejto práce. Pady boli poskytnuté od českej spoločnosti Contrisys s.r.o.


*Obrázok 5.15: Signotec LCD Signature Pad Omega*
*Zdroj: vlastné spracovanie.*

**Miesto a výskumný tým experimentu**

Experiment sa uskutočnil dňa 13. 12. 2017 na VUT FP (Vysoké učení technické v Brně, Fakulta podnikatelská), na adrese: Kolejní 2906/4, 612 00 Brno, v rámci voľnočasovej aktivity v časovom intervale 09:00-16:00 v učebni P267.

Prítomné dohliadajúce osoby vykonaného experimentu:

- Ing. Anikó Molnárová (doktorandka VUT FP)

- Ing. Jiří Ehleman (spoločnosť Contrisys, s.r.o.)
- Ing. Pavel Vaněček (spoločnosť Contrisys, s.r.o.)
- Ing. et Ing. František Hortai (autor dizertačnej práce)

**Použitá vzorka**

Pre potvrdenie alebo zamietnutie hypotéz bola použitá heterogénna vzorka. Zúčastnení boli študenti a akademici rozličných fakúlt Vysokého učení technického v Brně. Jednalo sa o osoby od 20 až do 70 rokov prevažne mužského pohlavia. Proces experimentu úspešne podstúpilo celkovo 63 osôb.

Každá osoba celkovo použila 5 skenerov DBP, každú zvlášť na 5 rozličných pozíciách držania tela. Pri každej pozícii sa signatári podpisovali na pad 10 krát (celkovo 50 podpisov na jednu osobu). Vzorka svojou veľkosťou je štatisticky dostatočne reprezentatívna.

Pozície pri ktorých bola stabilita podpisu skúmaná:

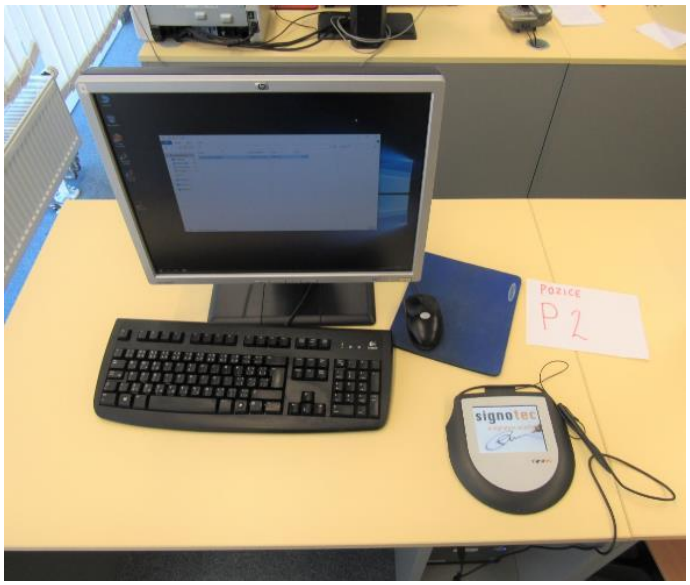
**Pozícia 1 (referenčná značená „P1“):**

Osoba sa podpíše klasicky (10-krát) posediačky na stoličke na pad, ktorý je na stole pri počítači, viď Obrázok 5.16:


*Obrázok 5.16: Skúmaná pozícia P1*
*Zdroj: vlastné spracovanie.*

**Pozícia 2 (značená „P2“):**

Osoba sa podpisuje na pad, ktorý je na stole bez stoličky, telo osoby je naklonené nad stôl, viď obrázok nižšie:




*Obrázok 5.17: Skúmaná pozícia P2*

*Zdroj: vlastné spracovanie.*

**Pozícia 3 (značená „P3“):**

Osoba sa podpisuje stojatým alebo nakloneným telom na pad, ktorý je pripevnený na stenu, v tomto prípade na umelej stene vo výške 125 cm, viď *Obrázok 5.19*.

*Obrázok 5.18: Skúmaná pozícia P3*

*Zdroj: vlastné spracovanie.*

**Pozícia 4 (značená „P4“):**

Osoba stojí a podpisuje sa na pad, ktorý je na pulte (vysoký stôl, napr. ako v bankách pri pokladni apod.), v tomto prípade je pad na barovom stole vo výške 110 cm, viď *Obrázok 5.19*.Obrázok 5.20

*Obrázok 5.19: Skúmaná pozícia P4*

*Zdroj: vlastné spracovanie*

**Pozícia 5 (značená „P5“):**

Pozícia imituje možnosť podpisu pri ležaní na posteli. Osoby sa podpisovali poležiačky na matraci (imitácia postele) na pad položenom na matraci, viď Obrázok 5.20:


*Obrázok 5.20: Varianty skúmanej pozície P5*

*Zdroj: vlastné spracovanie.*

**Priebeh experimentu**

1. Príprava meracích staníc v učebni. Skúmaných bolo 5 rôznych pozícií držaní tela a každá pozícia bola ekvivalentne vytvorená 2-krát. Pri každej stanici (celkom 10) sa na Windows PC nainštaloval SW balíček signoSign2 (10.7.2) a pripojenie na USB vstup počítača snímací pad (kontrola od Contrisys-u).
2. Nastavenie súborov a vzorkovacej frekvencie snímačov na 250 Hz.
3. O 09:00 sa začal postupný príchod osôb/signatárov.
4. Nasledovné postupy sa konali paralelne:
    a. Pri vstupe do miestnosti každá osoba dostala poradové číslo a bola oboznámená s postupom experimentu.
    b. Celkovo bolo vytvorených 10 staníc, kde sa všetky osoby paralelne podpisovali, no každá osoba sa podpísala iba na 5 staniciach a to sekvenčne pri rôznych pozíciách držania tela. Pri každej pozícii sa osoby podpisovali 10-krát.
    c. Nasnímané údaje boli zvlášť uložené do priečinka podľa pozície a do podpriečinka pre každú osobu zvlášť.
5. O 16:00 bolo ukončenie experimentu a počkanie, kým prítomné osoby dokončili proces podpisovania.
6. Archivácia údajov.
7. Odinštalovanie všetkého SW a HW.
8. Optická kontrola všetkých podpisov (človekom), a vyfiltrovanie nepodarkov (prázdne súbory, tvary pri ktorých bolo jednoznačné, že sa nejedná o podpis).
9. Extrakcia DBP a vyhodnotenie každého signatára.
10. Vypracovanie tejto časti merania a indukovaných hypotéz (viď **kapitolu 5.8).**

### 5.8.2 Vypracovanie

Na zariadeniach boli snímané DBP pomocou programu *signoSign2* verzia 10.7.2 32/64 Bit od spoločnosti signotec (2018). Každý účastník vytvoril na každom zariadení 10 DBP, na danom *.pdf súbore podľa pozícií P1 až P5 (viď kapitolu 5.8.1/Použitá vzorka). Poradie podpisovania nebola zohľadnená. Po vyexportovaní biometrických údajov - podpisov vznikla matica podpisov každého účastníka $\overline{P}_{i,j}$ nasledovne:

$$\overline{P}_{i,j} = [a1, \dots, a10]_{i,j} \qquad (11)$$

Kde je:

*i* a *j* je prirodzené číslo a predstavujú

*i* – poradové číslo pozície; $1 \leq \mathbf{i} \leq 5$ ; *j* – poradové číslo účastníka; $1 \leq \mathbf{j} \leq 63$ ;

$[a_1 \dots a_{10}]$ – 10 podpisov osoby **j** a na danej pozícii **i**.

**Vyhodnotenie údajov**

Ako základ vyhodnotenia experimentu sa skúmala miera zhody medzi podpismi každej osoby v rámci každej pozícii držania tela. V rámci jednej pozície - z matice podpisov $\overline{P}_{i,j}$ je pomocou vlastného programu, ktorý používa originálny engine pre zhody dynamického biometrického podpisu používaný od spoločnosti signotec (napr. u programu *eSig-Analyze* alebo *Signotec RSA Verifier*) vytvorená tabuľka kombináciami možných zhodných podpisov, kde funkcia $f(a_x , a_y)$ je výstup funkcie algoritmu zhody podpisov a znamená percentuálnu zhodu daných podpisov $a_x$ a $a_y$ s nasledujúcou architektúrou matice $S_{i,j}$ :

$$S_{i,j} = \begin{bmatrix} - & f(a_1,a_2) & f(a_1,a_3) & f(a_1,a_4) & f(a_1,a_5) & f(a_1,a_6) & f(a_1,a_7) & f(a_1,a_8) & f(a_1,a_9) & f(a_1,a_{10}) \\ - & - & f(a_2,a_3) & f(a_2,a_4) & f(a_2,a_5) & f(a_2,a_6) & f(a_2,a_7) & f(a_2,a_8) & f(a_2,a_9) & f(a_2,a_{10}) \\ - & - & - & f(a_3,a_4) & f(a_3,a_5) & f(a_3,a_6) & f(a_3,a_7) & f(a_3,a_8) & f(a_3,a_9) & f(a_3,a_{10}) \\ - & - & - & - & f(a_4,a_5) & f(a_4,a_6) & f(a_4,a_7) & f(a_4,a_8) & f(a_4,a_9) & f(a_4,a_{10}) \\ - & - & - & - & - & f(a_5,a_6) & f(a_5,a_7) & f(a_5,a_8) & f(a_5,a_9) & f(a_5,a_{10}) \\ - & - & - & - & - & - & f(a_6,a_7) & f(a_6,a_8) & f(a_6,a_9) & f(a_6,a_{10}) \\ - & - & - & - & - & - & - & f(a_7,a_8) & f(a_7,a_9) & f(a_7,a_{10}) \\ - & - & - & - & - & - & - & - & f(a_8,a_9) & f(a_8,a_{10}) \\ - & - & - & - & - & - & - & - & - & f(a_9,a_{10}) \\ - & - & - & - & - & - & - & - & - & - \end{bmatrix} \qquad (12)$$

Kde je:

*i* a *j* je prirodzené číslo a predstavujú

*i* – poradové číslo pozície; $1 \leq \mathbf{i} \leq 5$ ; *j* – poradové číslo účastníka; $1 \leq \mathbf{j} \leq 63$ ;

$f(a_x , a_y)$ - hodnota funkcie zhody podpisov;

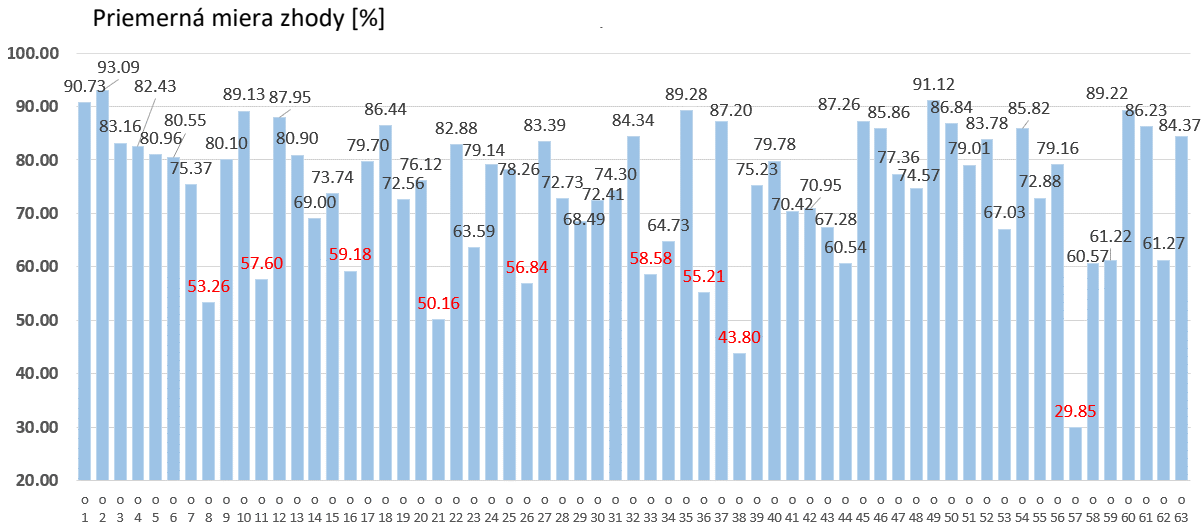
Značenie „ – “ sa týka porovnávania rovnakej (napr. $f(a_1 , a_1)$), či tej istej dvojice podpisov a preto sú z matice vynechané, nedefinované (prevencia proti duplicite údajov napr. $f(a_1 , a_2)$ a $f(a_2 , a_1)$).

Výstupom sú tabuľky s hodnotami zhôd podpisov v trojuholníkovom tvare $S_{P1,\,1}$ až $S_{P5,\,63}$. Pre každú tabuľku je stanovená priemerná zhoda podpisov danej osoby na dané pozície $\overline{x}$ a výberový rozptyl zhody $s^2$ . Tým spôsobom bol získaný rad priemerných zhôd $\overline{x}_{1,j}$ až $\overline{x}_{5,\,j}$ ,

rad hodnôt výberových rozptylov $s_{i,j}^2$ a jej odmocninou rad výberový odchýlok $s_{1,j}$ až $s_{5,j}$ na každú pozíciu pre každú osobu.

### Prípad osôb

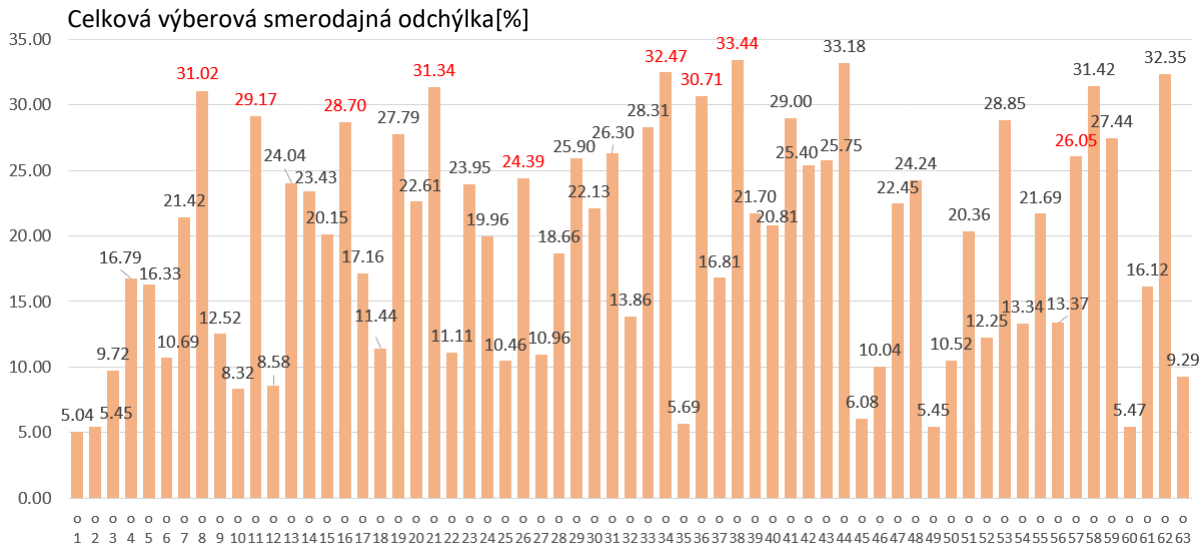
Pri 9 osobách sa priemerná miera zhody podpisov dostala pod priemernú mieru zhody biometrických podpisov (viď *Obrázok 5.21*), ktorá sa v predchádzajúcich experimentoch (Smejkal et al., 2015; Smejkal et al., 2016) pohybovala v intervale 70 % až 90 %, ale vždy bola > 60 % a to aj za situácie ovplyvnenia testovanej osoby alkoholom alebo stresom.




*Obrázok 5.21: Priemerná miera zhody podpisov jednotlivých osôb*

*Zdroj: vlastné spracovanie.*

Viac vypovedá graf na *Obrázok 5.22*, ktorý ilustruje celkovú výberovú smerodajnú odchýlku „$s$“ pre všetky osoby, t. j. akú celkovú „nestabilitu“ mieru zhody medzi podpismi prejavovali počas celého merania.




*Obrázok 5.22: Celková výberová smerodajná odchýlka jednotlivých osôb*

*Zdroj: vlastné spracovanie.*

Celkový výsledok charakterizujúci meranie pozícií ako celok, teda bez rozlíšenia typu použitej pozície podpisujúcej sa osoby je nasledovný:

*Tabuľka 5.8: Súhrnné výsledky miery zhody všetkých podpisov*

| x [%] | $\sigma^2$ | σ |
|---|---|---|
| 74.36 | 258.31 | 16.07 |

*Zdroj: vlastné spracovanie.*

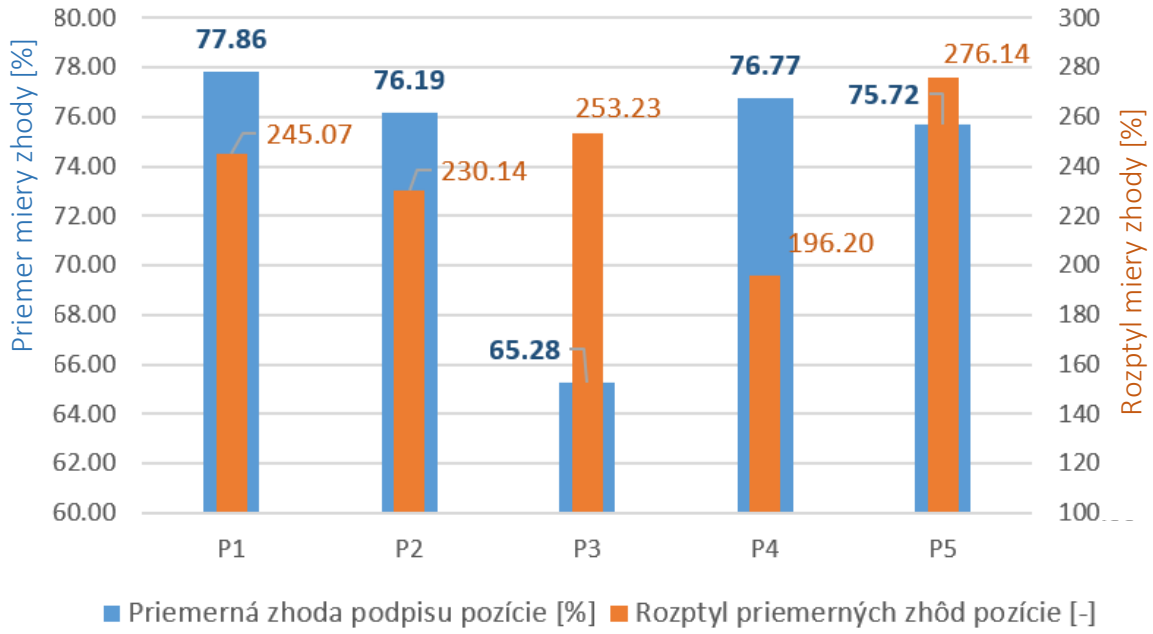
Zistené boli nasledujúce hodnoty priemerov a rozptylov miery zhody podpisov pre uvedené pozície:

*Tabuľka 5.9: Priemer a rozptyl miery zhody podpisov skúmaných pozícií*

| | Priemerná zhoda podpisov pozície x [%] | Výberový rozptyl $s^2$ [%] |
|---|---|---|
| ***P1*** *(Obrázok 5.16)* | 77.86 | 245.07 |
| ***P2*** *(Obrázok 5.17)* | 76.19 | 230.14 |
| ***P3*** *(Obrázok 5.18)* | 65.28 | 253.23 |
| ***P4*** *(Obrázok 5.19)* | 76.77 | 196.20 |
| ***P5*** *(Obrázok 5.20)* | 75.72 | 276.14 |

*Zdroj: vlastné spracovanie.*

*Obrázok 5.23: Priemerná miera zhody a rozptylu podpisov pri jednotlivých pozíciách*




*Zdroj: vlastné spracovanie.*

Z grafu vyššie je vidno, že najväčšia priemerná stabilita bola dosiahnutá v prípade pozície P1 a najmenšia v prípade pozície P3.

**I. časť: testovanie hypotéz**

Táto časť predpokladá, že celková stabilita podpisov dosahovaná pri jednotlivých pozíciách tela signatára sa bude štatisticky významne odlišovať.

**Zhoda všetkých rozptylov**

Zhoda rozptylov bola overená Bartlettovým testom (B= 1.9633, počet voľností = 4, $\alpha$ = 0.01 a 0.05, P-value= 0.7425). Z týchto výsledkov vyplýva, že zhoda všetkých rozptylov sa dá prijať na hladine významnosti 0.01 i na hladine významnosti 0.05.

**Zhoda všetkých priemerov**

Test jednoduchého triedenia (ANOVA) (Cochran & Cox, 1957) poskytol výsledky (F = 6.9335, k = 4, n-k = 310, $\alpha$ = 0.01 a 0.05, $F_{0.01}$= 3.3802 a $F_{0.05}$= 2.4008, kde $F_{1-\alpha}$ (k-1, n-k) je (1-$\alpha$) kvantil Fisherova-Snedecorova rozdelenia pre hladinu významnosti $\alpha$), z nich vyplýva že zhoda všetkých priemerov sa dá zamietnuť na hladine významnosti 0.01 aj na hladine významnosti 0.05.

Výsledky Scheffého testu mnohonásobného porovnávania (Scheffé, 1999) umožnili určiť, medzi ktorými dvoma vyššie uvedenými súbormi dát existujú štatisticky významné rozdiely. Scheffého test prijíma na hladine významnosti 0.01 aj na 0.05 rovnosť 6 z 10 prípadov dvojíc a v prípade 4 dvojíc pri porovnaní s pozíciou P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05. Pre uistenie testu sa použil aj Tukeyho test mnohonásobného porovnávania (Hsu, 1996, str 119), ktorý obvykle odhalí viac rozdielov medzi strednými hodnotami ako Scheffého test. No v tomto prípade sa zhoduje s výsledným rozsudkom zo Scheffého testu mnohonásobného porovnávania, t. j. rovnosť dvojíc s kombináciami pozícií P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05 a v prípade dvojíc s pozíciou P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05.

Priemery sú štatisticky významne rozdielne na hladinách významnosti 0.01 aj 0.05.

**Záver k hypotézam**

Z testovaní vyplýva, že zhoda všetkých rozptylov síce bola prijatá na hladine významnosti 0.01 i na hladine významnosti 0.05, ale v prípade testovania zhody všetkých priemerov testy jednoznačne zamietli zhody všetkých priemerov na hladine významnosti 0.01 aj na hladine významnosti 0.05. Preto sa nulová hypotéza *H 5.6.I.0* zamieta, v prospech alternatívnej hypotézy:

- *H 5.6.I.1 - existuje štatisticky významná odlišnosť priemerov a rozptylov miery zhody podpisov pri niektorých pozíciách.*

Zistené rozdiely pri jednotlivých pozíciách sú skúmané v nasledujúcej časti (viď ďalej II. časť).

**II. časť: Testovanie a odpovede na výskumné otázky**

**V.O. 5.6.I Ktoré pozície sú si ekvivalentné z pohľadu podpisovej stability?**

Vychádza sa z predpokladu prijatia hypotézy *H 5.6.I.1*. Pri testovaní zhody všetkých rozptylov boli prijaté na hladine významnosti 0.01 i na hladine významnosti 0.05 (overená Bartlettovým testom). Prípad párových zhôd pozícií P1 až P5 bola testovaná pomocou Fisherovho testu (Markechová et al., 2011, str. 145), v tomto prípade dvojstranného F-testu pre zhodu rozptylov. Výsledky dvojstranného F-testu pre zhodu rozptylov prijímajú na hladine významnosti 0.01 aj na 0.05 rovnosť zhody rozptylov pre všetkých 10 prípadov porovnaných dvojíc pozícií.

Z pohľadu zhody priemerov testované pomocou: Scheffého testu mnohonásobného porovnávania (Scheffé, 1999), Tukeyho test mnohonásobného porovnávania (Hsu, 1996, str 119), Dvojvýberový t-test (Študentov t-test) pri predpoklade rovnosti rozptylov sa výsledným rozhodnutím zhodovali: rovnosť priemerov dvojíc s kombináciami pozícií P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05 a v prípade dvojíc s pozíciou P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05.

Pre rovnosť pozícií P1, P2, P4, P5 bol vykonaný dodatočne test jednoduchého triedenia (ANOVA) (Cochran & Cox, 1957), ktorý poskytol už očakávané výsledky: zhoda všetkých priemerov sa dá prijať na hladine významnosti 0.01 aj na hladine významnosti 0.05.

**Záver k V.O. 5.6.I**

Rovnosť priemerov dvojíc s kombináciami pozícií P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05 a v prípade dvojíc s pozíciou P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05.

Zhody všetkých rozptylov, a to aj v prípade porovnaných všetkých 10 prípadov dvojíc pozícií sa prijíma rovnosť zhody rozptylov na hladine významnosti 0.01 aj na 0.05.

Za predpokladu, že stabilitu podpisov na jednotlivých pozíciách odráža variancia, resp. čím väčšia stabilita, tým menšia variancia, sa pozície z pohľadu rozptylov zhodujú. Z pohľadu celkových hodnôt sú pozície P1, P2, P4 a P5 prakticky ekvivalentné. Z celkových výsledkov vyplýva, že signatári síce preukázali nižšiu priemernú zhodu podpisov v prípade pozície P3, ale pri týchto nižších zhodách mali varianciu/nestabilitu podpisov zhodnú ako v prípade ostatných pozíciách.

**V.O. 5.6.II Aký exogénny faktor spôsobil rozdiel pri stabilite podpisu u signatára?**

Pre základnú analýzu boli zohľadnené subjektívne mienky probandov/signatárov. Signatári po vyhodnotení boli oboznámený s vlastnými hodnotami zhody podpisov a vyzvaný na vyplnenie anonymného dotazníka pre spätnú väzbu. Viď niektoré citované mienky respondentov:

- *„Pozícia 3 spôsobovala pre mňa nepríjemnosti, keď sa pozerám, je to aj jednoznačné z môjho osobného výsledku.“*
- *„Všeobecne sa musím podpisovať v pozíciách 1, 2, 3.“*
- *„Pozícia 4 je pohodlnejšia ako pozícia 2.“*

- *„Najmenej pohodlná je asi 3 pozícia, je typická pri podpisovaní prijatia balíka, ale vtety nie je povrch pevne zafixovaný.“*
- *„Poležiačky bolo príjemné sa podpisovať, ale nevidím v tom praktické použitie.“*

Mienky signatárov svedčia o tom, že pozícia P3 spôsobovala pre nich ťažkosti. Z pohľadu analýzy celkových dosiahnutých hodnôt sa priemerná miera a rozptyl zhody podpisov pre pozície P1, P2, P4 a P5 sa štatisticky významne nemení, prakticky sa môžu brať z pohľadu celkových hodnôt a podpisovej stability za ekvivalentné. Pri pozícii P3 signatári vykazovali nižšiu priemernú zhodu podpisov a subjektívne pre nich spôsobovala ťažkosti pri vytváraní podpisu. Pre zistené fakty sa podrobnejšie analyzovala pozícia P3. Zistené rozdiely pri procesu vytvárania podpisu (pre ilustratívnu reprezentáciu viď *Obrázok 5.25*):

- Podpisové zariadenie bolo ukotvené na stene, nedalo sa s ním hýbať, resp. meniť/prispôsobiť pozíciu zariadenia (pri ostatných pozíciách sa so zariadeniami dalo manipulovať).
- Zmena polohy zariadenia z horizontálneho na vertikálnu ukotvenú polohu. Z tohto faktu vyplýva aj dôsledok zmeny polohy ramena pri písaní. Rameno signatára pri podpise sa z horizontálneho pohybu menil na vertikálny pohyb.
- Rameno sa nedalo zafixovať alebo lakeť ukotviť na nejakú stabilnú plochu.

*Obrázok 5.24: reprezentácia rozdielov pri procesu podpisu*

*Zdroj: vlastné spracovanie.*

Vyššie vymenované rozdiely môžu byť faktorom zmeny nižšej priemernej zhody pri tejto pozícii. Z nej vyplýva, že optimálna poloha na podpisovanie DBP, nemusí byť špecifická, ale pozícia pre používateľa má byť prirodzená pre podpis a bez možných bariér, ktoré by ho

v tomto prirodzenom procese obmedzovali. V prípade výskumov na presnú analýzu zhody podpisov je doporučené používať jednu zvolenú pre používateľov prirodzenú polohu a vytrvať pri tejto polohe počas celého výskumu.

### V.O. 5.6.III Je stabilita skôr závislá na exogénnych faktoroch, alebo skôr na individuálnych charakteristikách signatára?

Stabilitu podpisov DBP by mala odrážať variancia zhody podpisov. I keď sa pokusné osoby individuálne rôzne ťažko vyrovnávajú s meniacimi sa okolnosťami pri podpise (viď napr. kapitolu *5.7 Technologický aspekt* alebo skúmaný prípad aplikovanej polohy tela signatára), sú tieto skúmané exogénne okolnosti z pohľadu celkovej zhody variancie stále, lebo podľa štatistických testov nebol zistený významný štatistický rozdiel v prípade rozptylov zhôd pri podpise.

Preto faktorom vplyvu by mohli byť skôr individuálne vlastnosti signatára. Myslí sa tým na intra-personálnu variabilitu signatára (Diaz-Cabrera, Ferrer, Morales, 2015), ktorá je založená na detekcii lexikálnych a morfologických aspektov písaného textu, v tomto prípade na analýze podpisov daného signatára. Výskumy v prípade off-line analýzy (Diaz et al., 2015) a v prípade on-line analýzy (Parziale et al., 2013) dokázali, že čím je väčšia intra-personálna variabilita, tým menej je stabilný signatár. Variabilita podpisu, či nízka miera zhody medzi jednotlivými podpismi preto úzko súvisí so stabilitou podpisu. Pritom existujú dva typy variability podpisov: krátkodobá (závisí na psychologickom stave osoby a na podmienkach písania) a dlhodobá variabilita (závisí na zmene systému fyzického písania, resp. modifikácia motorického programu v mozgu) (Pirlo, Impedovo, 2013) - napr. vplyvom starnutia alebo choroby. Podľa experimentov (Smejkal et al., 2013; Smejkal, Kodl 2014; Smejkal, et al., 2015; Smejkal et al., 2016), kde sa namiesto optického vyhodnocovania obrázkov podpisu boli analyzované biometrické charakteristiky (on-line DBP) dokázali, že vplyv vonkajších faktorov na krátkodobú variabilitu je zanedbateľný (napr. stres, alkohol).

Pre možný relatívny výskyt vysokej variability podpisu osôb bola stanovená hranica priemernej miery zhody > 60 %, lebo priemerná miera zhody biometrických podpisov v predchádzajúcich experimentoch (Smejkal et al., 2015; Smejkal et al., 2016) sa pohybovala v intervale 70 % až 90 %, ale vždy bola > 60 %. V časti experimentu v kapitole *5.7 Technologický aspekt* vysoká variabilita podpisu bola zistená pri 2 osobách (č. 16 a č. 34) z 40 (relatívne 5 %), v prípade tejto časti experimentu pri meraní vplyvu polohy pri podpise bolo zistené, že vysoká variabilita podpisu bola pri 9 osobách z 63 (relatívne cca 14 %) (viď *Obrázok*

*5.21*). Oba experimenty reprezentujú štatisticky reprezentatívnu vzorku, preto môžeme predpokladať, že vysoká variabilita podpisu sa prejavuje výnimočne pri signatárov.

## 5.9 Aspekt možných rizík zneužitia DBP

Používanie dynamického biometrického podpisu je spojené s dvoma hlavnými rizikami. Prvá sa vzťahuje k prelomeniu bezpečnosti implementácie DBP, t. j. možnosť extrahovania statických a dynamických komponentov podpisu z podpísaného dokumentu a použitie takto získaného DBP pre podpísanie iného dokumentu. Druhé riziko súvisí s možnosťou falšovania DBP, t. j. napodobenie oboch zložiek DBP inou osobou.

Prvé riziko je eliminovateľné správnou systémovou implementáciou a nesúvisí s princípmi DBS. Druhé riziko je však často spomínané a spojené s implementáciou DBS v rôznych aplikáciách a predstavuje možnosť napodobnenia DBP. Z dôveryhodného výskumu uskutočneného v roku 2014 (Smejkal, Kodl, 2014) boli skúmané charakteristiky DBP pri pokuse o falšovania podpisu inej osoby, ktorej podpisový vzor, výsledný obraz podpisu bol k dispozícii. Ani jeden z pokusných „falšovateľov“ zo 190 pokusov neuspel. Preto možnosť napodobenia DBP bez znalosti dynamiky bola zamietnutá.

Z tohto dôvodu sa indukoval výskum kontinuálne nadväzujúci na predchádzajúce výskumy. Cieľom experimentu bolo overiť, nakoľko je možné napodobniť DBP pri znalosti dynamiky podpisu. Z výsledkov potom vyplývala aj odpoveď na otázku: aká má byť stanovená požadovaná miera zhody podpisu aby bol DBP považovaný za pravý?

### 5.9.1 Metodológia technologicko-používateľského aspektu (časť II: riziká falšovania)

Cieľom experimentu bolo overiť, nakoľko je možné napodobniť DBP pri znalosti dynamiky podpisu. Preto tento experiment sa pokúšal vytvoriť potenciálnym falšovateľom čo najlepšie podmienky pre napodobňovanie vzorového DBP. Účastníci mali po celú dobu vykonávania experimentu k dispozícii ako statické zobrazenia podpisov, tak jeho dynamiku. To bolo dosiahnuté opakovaným premietaním zobrazenia postupne vytváraného podpisu. Každý účastník mohol opakovať pokusy napodobenia bez pocitu tlaku časového obmedzenia až do tej doby, než sám usúdil, že považuje napodobnenie podpisu za najviac sa blížiace originálu.

Účastníci mali k dispozícii všetky možnosti, ktoré im poskytoval audítorský softvér z hľadiska zobrazenia dynamických vlastností podpisu:

- možnosť simulácie (zobrazenia) priebehu vytvoreného celého podpisu,
- možnosť prehliadnutia podpisu po krokoch,
- zastavovanie procesu podľa vlastného výberu.

Súčasne boli k dispozícii odborníci, ktorí zodpovedali na prípadné otázky vzťahujúce sa k podpisu, jeho snímaniu, ovládaniu audítorského softvéru apod. Testovacie osoby ale nemali k dispozícii vyhodnotenie zhody podpisov auditného softvéru, tá bola uskutočnená až po skončení experimentu. Tým sa simulácia priblížila podmienkam ozajstných falšovateľov, keď falšovateľ nemá k dispozícii softvér pre overenie miery zhody pravého podpisu a falzifikátu, a musí sa spoľahnúť na vlastné odhady podobnosti podpisov.

Pomocou sprístupnenia oficiálneho SW modulu od spoločnosti signotec (distribúcia od Contrisis s.r.o.), sa použil originálny engine pre vyhodnotenie zhody dynamického biometrického podpisu pre komparáciu zhody podpisov sfalšovaných reláciou na originálne podpisy. Pre ďalšie možné spracovanie a výpočty boli tieto výsledné údaje zhrnuté v excelovskom zošite (viď elektronické prílohy) a znázornené na prílohách na konci dokumentu (tabuľka výsledkov miery zhôd podpisov pri falšovaní).

Navrhli sa nasledujúce výskumné hypotézy a výskumné otázky:

- Hypotézy časti I. predpokladajú, že miera schopnosti napodobňovania podpisov je u každej osoby rovnaká pre všetky podpisy.
    - H 5.7.I.0 – Každý podpis je pre jednotlivcov rovnako ťažké napodobniť.
    - H 5.7.I.1 – Každý podpis je pre jednotlivcov rôzne ťažké napodobniť.
- Hypotézy časti II. predpokladajú, že rozdielne podpisy je rôzne ťažké napodobniť.
    - H 5.7.II.0 – Podpis A a B sú rovnako ťažko napodobniteľné.
    - H 5.7.II.1 – Podpis A a B sú rôzne ťažko napodobniteľné.
- Hypotézy časti III. predpokladajú, že miera zhody medzi pravým podpisom a jeho falzifikátom je priamo úmerná počtom pokusov o napodobnenie.
    - H 5.7.III.0 – Existuje štatisticky významná korelácia a regresia medzi počtom pokusov o napodobenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho napodobnením.

    - H 5.7.III.1 – Korelácia a regresie medzi počtom pokusov o napodobnenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho falzifikátom nie sú štatisticky významné.
- Výskumná otázka na stanovenie miery zhody podpisu.
    - V.O. 5.7.II.1 – Aká má byť stanovená miera zhody podpisu aby bol DBP považovaný za pravý?

Pre výsledky tejto časti merania a hypotéz viď kapitolu 5.9.2.

**Použité prístroje experimentu**

Testovanie sa uskutočnilo na snímačoch dynamického biometrického podpisu od spoločnosti Signotec GmbH:

- signotec LCD Signature Pad Omega (ST-CE1075-2-U100)

Celkovo bolo použitých súbežne 10 prístrojov pripojených každý prístroj zvlášť na PC vybavenie. Vzorkovacia frekvencia bola nastavená na 250 Hz (bodov za sekundu). Výrobné čísla a špecifikácie snímačov sú dostupné v elektronických prílohách tejto práce.

**Miesto a výskumný tým experimentu**

Experiment sa uskutočnil dňa 23. 11. 2017 na VŠE - Vysoká škola ekonomická v Praze (Ekonomická 957, 148 00 Praha 4, budova B, učebna JM359), v rámci cvičenia študentov v časových intervaloch 14:30-16:00, 16:15-17:45, 18:00-19:30 na VŠE,

Prítomné dohliadajúce osoby vykonaného experimentu:

- Ing. Jindřich Kodl CSc. (súdny znalec v oboru kybernetika)
- Ing. Jiří Ehleman (spoločnosť Contrisys, s.r.o.)
- Ing. Pavel Vaněček (spoločnosť Contrisys, s.r.o.)
- Ing. Jana Fortinová (Katedra informačních technologií - FIS VŠE)
- Ing. et Ing. František Hortai (autor dizertačnej práce)

**Použitá vzorka**

Na tento účel boli vybrané pokusné osoby, u ktorých sa predpokladala adekvátna odborná a mentálna kvalifikácia aj podpisové zručnosť na snímacích zariadeniach, ako aj motivácia pre získanie čo najlepšieho výsledku. Boli to študenti oboch pohlavia 1 ročníka Vysoké školy ekonomické v Praze. Študenti boli motivovaní dosiahnuť čo najlepší výsledok, lebo pri možnom úspešnom napodobnení dostali dodatočné body, ktoré sa im započítavali v rámci

zápočtu daného predmetu. Merania sa zúčastnili aj dohliadajúce osoby vykonaného experimentu. Celkovo sa merania zúčastnilo cca 50 osôb.

Proces experimentu podstúpilo viac ľudí ako bolo vo výslednej analýze zohľadnené. Filtrovanie, či kontrola všetkých podpisov bola vykonaná človekom, a to optickou kontrolou. Filtrácia bola dôležitá aby nedošlo k skresleniu údajov. Odôvodnenie filtrovania:

- niektorí zabudli uložiť výsledný sfalšovaný podpis a odovzdali prázdny súbor,
- falšovali iba jeden podpis a druhý vynechali,
- boli adepti, ktorí jednoznačne sa nepodpisovali a odovzdali kresbičky, tvary atď.

Z prítomných ľudí, bolo nakoniec výsledných 48 osôb, ktorí pochopili postup procesu falšovania, úspešne vykonali danú úlohu a aktívne sa zúčastnili procesu falšovania, či napodobenia popisov. Tí sa snažili napodobňovať **dva rôzne podpisy písané pravou rukou**.

Na tento účel boli vytvorené dva vzorové podpisy - podpis A a podpis B. Tieto podpisy boli svojím pôvodom iné: podpis **A** bol umelo vytvorený ženský podpis *„Fortinová“* organizátorkou experimentu, podpis **B** *„Ehleman“* bol originály mužský podpis, dlhodobo používaný jedným z organizátorov.

Výsledná vzorka svojou veľkosťou je štatisticky dostatočne reprezentatívna na analýzu.

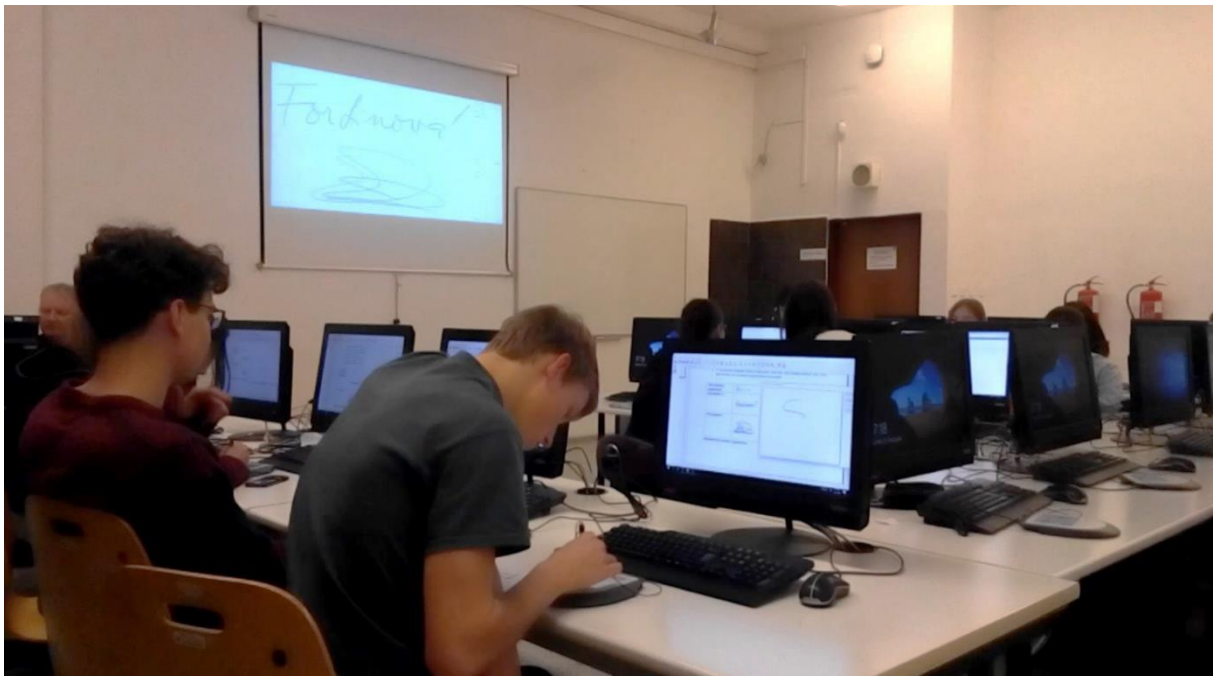
**Priebeh experimentu**

1. Nainštalovanie snímacích padov na počítače v učebni (kontrola od Contrisys-u), nastavenie vzorkovania na 250 Hz.
2. Pripojenie notebooku s auditným programom, ktorý bude zobrazovať stále dookola dynamický priebeh vybraných podpisov (ktoré sa budú snažiť falšovať).
3. Príchod študentov 1. študijnej skupiny, vysvetlenie princípov DBP jej použiteľnosť, a vysvetlenie experimentu.
4. Rozdelenie prítomných osôb na skupiny po 10. Následne bolo zahájenie experimentu v rámci ktorého sa pokúsilo napodobniť zobrazovanú dynamiku podpisov. Osoby napodobňovali 2 rôzne dynamické podpisy od dvoch rôznych osôb (podpis muža a ženy). Na učenie či napodobnenie daných podpisov mali cca 30 minút s možnosťou ľubovoľného množstva pokusov. Výsledné podpisy daného účastníka (sfalšované podpisy) boli na ich subjektívnom rozhodnutí (že urobili ten správny falzifikát podpisov) a sami ho výsledne potvrdili. Tento postup odrážal skutočnosť, že falšovateľ nemá k dispozícii inú možnosť, než odpozorovať dynamiku podpisu

a následne porovnávať výsledok svojho napodobňovania vizuálne, bez možnosti takto vytvoreného falzifikátu spracovať analytickým programom na účel strojového vyhodnotenia podobnosti oboch podpisov. Tým sa aj zjednodušilo vyhodnocovanie, pretože sa porovnával iba 1 výsledný podpis s predlohou (celkovo na osobu 2 s príslušnými etalónmi).

5. Ukončenie experimentu danej skupiny, archivácia údajov danej skupiny.
6. Opakovanie bodov 3.-5. pre 2. a 3. skupinu.
7. Celkový archív a odinštalovanie všetkého SW a pozbieranie HW.
8. Optická kontrola všetkých podpisov (človekom), a vyfiltrovanie nepodarkov (prázdne súbory, tvary pri ktorých bolo jednoznačné že sa nejedná o podpis).
9. Extrakcia DBP a vyhodnotenie zhody vzorového podpisu a napodobnenia pre každého signatára.

Pre lepšiu predstavu priebehu merania viď obrázok nižšie:



*Obrázok 5.25: Ilustrujúci obrázok merania pri napodobnení DBP*

*Zdroj: vlastné spracovanie.*

### 5.9.2 Výsledky

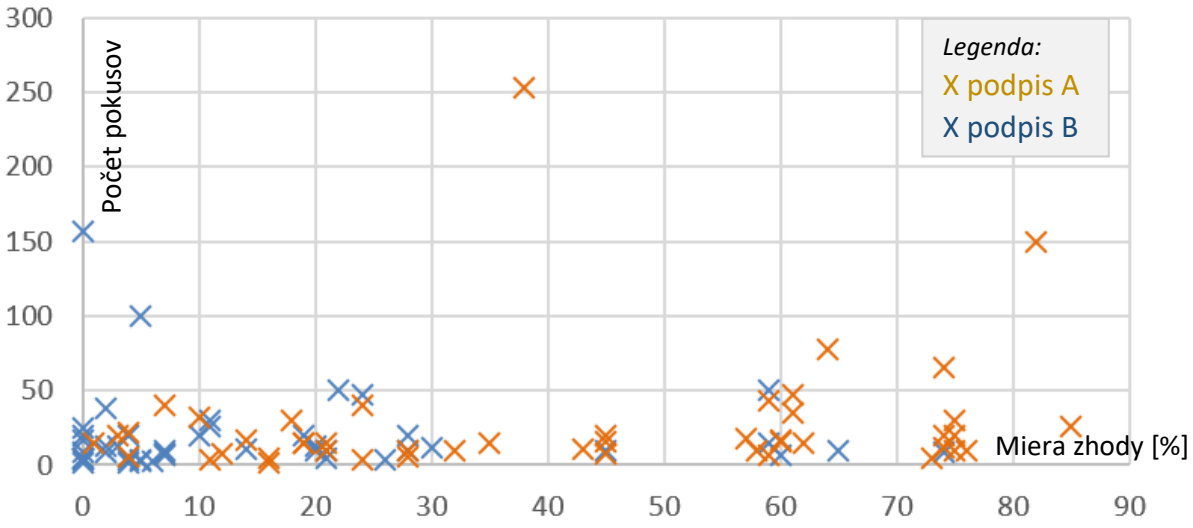
Podpisu A (umelo vytvorený ženský podpis „*Fortinová*“) sa úspešne sa zúčastnilo 47 osôb. Podpisu B (originály mužský podpis „*Ehleman*“) sa úspešne sa zúčastnilo 45 osôb. Zistená bola nasledujúce miera zhody pri počte uskutočnených pokusov (viď *Tabuľka 5.10*).

*Tabuľka 5.10: Miera zhody pri počte uskutočnených pokusov*

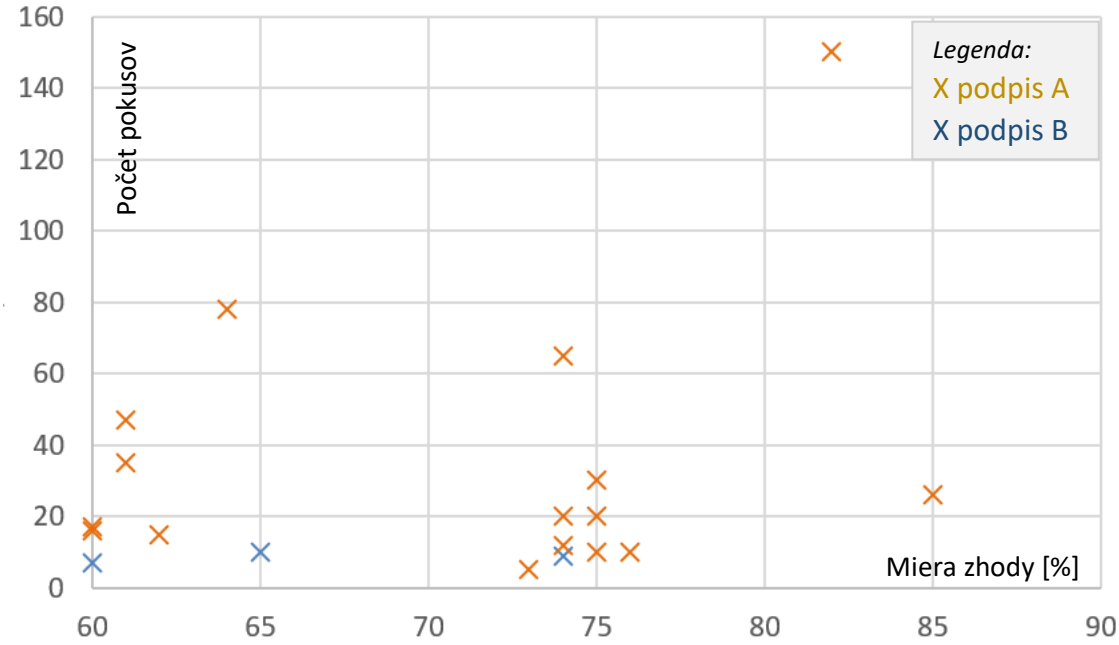
| Podpis A *(Fortinová)* | | Podpis B *(Ehleman)* | |
|---|---|---|---|
| Pokusy ≥ 60 % zhody | 16 | Pokusy ≥ 60 % zhody | 3 |
| Pokusy ≥70 % zhody | 10 | Pokusy ≥ 70 % zhody | 1 |
| Pokusy ≥ 80 % zhody | 2 | Pokusy ≥ 80 % zhody | 0 |
| Pokusy ≥ 90 % zhody | 0 | Pokusy ≥ 90 % zhody | 0 |

*Zdroj: vlastné spracovanie*

Závislosť miery zhody podpisov sú znázornené na obrázkoch: *Obrázok 5.26 a Obrázok 5.27*




*Obrázok 5.26: Závislosť miery zhody podpisov a počtu pokusov u všetkých účastníkov*
*Zdroj: vlastné spracovanie.*




*Obrázok 5.27: Závislosť miery zhody podpisov a počtu pokusov u účastníkov ≥ 60 %*
*Zdroj: vlastné spracovanie.*

Celkové výsledky merania zúčastnených 48 osôb, ktoré napodobňovali dva rôzne podpisy sú zhrnuté v *Tabuľka 5.11*:

*Tabuľka 5.11: Celkové hodnoty merania falzifikácie podpisov*

| | Zhody pri podpisov A [%] | Počet pokusov podpisu A | Zhody pri podpisov B [%] | Počet pokusov podpisu B |
|---|---|---|---|---|
| ***Priemer*** | **41.43** | **27.28** | **16.59** | **19.80** |
| *Počet hodnôt* | 47 | 47 | 45 | 45 |
| *Výb. smerodajná odchýlka.* | 26.08 | 41.67 | 19.91 | 27.43 |

*Zdroj: vlastné spracovanie.*

Z celkových hodnôt merania falzifikácie podpisov (Tabuľka 5.11) vyplýva, že priemerné hodnoty jednotlivých podpisov sú si rozdielne. Podpis A má priemer zhody falzifikátov viac ako dvojnásobok priemeru B. Tieto hodnoty sú pre všetkých 48 osôb.

**Ukazovateľ FRR a FAR:**

Zohľadnili sa ukazovatelia FAR a FRR podľa vzorcov v kapitole 3.6.6, FAR na str. 62 a FRR na str. 63. FRR - Mieru chybného odmietnutia nebolo možné v tomto experimente stanoviť, pretože podpis A bol „umelý“ (umelo vytvorený pre tento experiment) a autor podpisu B porovnávanie svojho pravého podpisu so svojím vzorom v rámci tohto experimentu nevykonal. Z iného experimentu (Smejkal et al., 2015) je však známa výška FRR pre túto osobu, ktorá v tom prípade predstavovala 1.82 % pre hladinu zhody ≥ 80 % a 0.00 % pre hladinu zhody ≥ 70 %.

Dosiahnuté výsledky v tejto časti experimentu viedli k hodnotám FAR (Tabuľka 5.12):

*Tabuľka 5.12: Hodnoty FAR pri skúmaných podpisoch*

| | Podpis A | Podpis B |
|---|---|---|
| FAR pri zhode ≥ 60 % | 1.25 % | 0.34 % |
| FAR pri zhode ≥ 70 % | 0.78 % | 0.11 % |
| FAR pri zhode ≥ 80 % | 0.16 % | 0.00 % |
| FAR pri zhode ≥ 90 % | 0.00 % | 0.00 % |

*Zdroj: vlastné spracovanie.*

**Testovanie údajov**

Pre analýzu údajov boli vykonané štatistické testy na uvedených charakteristikách podpisov (*Miera zhody A, Miera zhody B, Počet A* a *Počet B*).

**Normalita rozdelenia**: pre test normality bol použitý Kolmogorov-Smirnov test a Shapiro-Wilk test. Pre všetky štyri súbory dát oba testy zamietajú normalitu na hladine významnosti 0.01 (významnosti *sig.* < 0.01), a to s nasledujúcimi výsledkami (viď *Tabuľka 5.13*):

*Tabuľka 5.13: Test normálneho rozdelenie údajov pri falzifikovaní podpisov*

| | Kolmogorov-Smirnov | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Stat. hod. | df | Sig. | Stat. hod. | df | Sig. |
| **Miera zhody A** | 0.1503 | 47 | 0.0095 | 0.921 | 47 | 0.0036 |
| **Počet A** | 0.2738 | 47 | 0.0000 | 0.500 | 47 | 0.0000 |
| **Miera zhody B** | 0.2133 | 45 | 0.0000 | 0.777 | 45 | 0.0000 |
| **Počet B** | 0.2909 | 45 | 0.0000 | 0.566 | 45 | 0.0000 |

*Zdroj: vlastné spracovanie.*

**Korelácia**: vzhľadom na zamietnutie normality rozdelenia údajov neodporúča sa použiť Pearsonov korelačný koeficient, ktorý normalitu rozdelenia údajov predpokladá (Stigler, 1989). Preto bol vypočítaný Kendallov koeficient poradovej korelácie (rank korrelation) τ (viď: Kendall, Gibbons 1990; vypočítaný podľa: Press et al., 2007, str. 751-754), ktorý je kvalitatívne atraktívnejší na neparametrické testovanie, ako Spearmanov koeficient *rho* (Gibbons, 1993). Vypočítané údaje sú v tabuľke (*Tabuľka 5.14*):

*Tabuľka 5.14: Kendallov korelační koeficient*

| | Kendallovo τ | Obojstranný P-value |
|---|---|---|
| Miera zhody A x Počet A | 0.1848 | 0.06699 |
| Miera zhody B x Počet B | 0.0893 | 0.38705 |
| Miera zhody A x Miera zhody B | 0.1261 | 0.22752 |
| Počet A x Počet B | 0.3355 | 0.00133 |

*Zdroj: vlastné spracovanie.*

Ak obojstranná *P-value* je väčšia ako 0.01 nie je možné zamietnuť hypotézu o nekorelovanosti veličín na hladine významnosti 0.01. Z výsledkov Kendallova testu

poradovej korelácie vyplýva, že existuje signifikantná kladná korelácia medzi *Počet A* a *Počet B*, čo vypovedá o tom, že účastník sa približne rovnako rýchlo vysporiadal s napodobením oboch podpisov. V ostatných prípadoch nebola zistená korelácia, ktorá by bola významná na hladine významnosti 0.01.

**Testovanie hypotéz I. časti**

Táto časť predpokladala, že talent falzifikovať podpisy je u každej osoby iný ale stály. Inými slovami môžeme predpokladať, že každá osoba bude „talentom“ iný, ale osoba schopnejšia napodobniť podpis A bude rovnako dobre schopná napodobniť aj podpis B. Z toho predpokladu vyplýva, že miera zhody falzifikovaných podpisov s príslušným originálnym podpisom pri A a B sú si v konečnom dôsledku pri každej osobe na sebe závislé. Toto testovanie je vyhodnotené analýzou korelácie pri tých prípadoch, kedy osoby falzifikovali ako podpis A, tak aj podpis B.

Z výsledných údajov 44 osôb falzifikoval ako A tak aj B podpis, preto boli tieto osoby vyfiltrované a analyzované ďalej. Tieto osoby sa pokúsili napodobniť podpis A aj B. Pri týchto osobách priemer absolútnych rozdielov zhôd podpisov A a B je 29,8 % (zaokrúhlené nahor desatinným miestom). V prípade štandardného priemeru (priemer zhody A, a priemer zhody B) je rozdiel 24,16 %. V prípade podpisu A dosiahli priemernú mieru zhody 22,77 %, v prípade podpisu B dosiahli priemernú mieru zhody 16,59 %.

Z výsledkov Kendallova koeficientu vyplýva (*Tabuľka 5.14*), že signifikantná korelácia medzi mierou zhody A a B neexistuje (hodnota $p = 0.22 > 0.05 > 0.01$), možno nulovú hypotézu H 5.7.I.0 o zhode „talentu“ napodobňovať všetky podpisy sa dá zamietnuť na hladine významnosti $\alpha = 0.05$ aj 0.01 v prospech alternatívnej hypotézy:

*H 5.7.I.1 – Každý podpis je pre jednotlivcov rôzne ťažké napodobniť.*

Hypotéza bola prijatá.

**Dodatok :**

Vzorové podpisy boli písané pravou rukou. Ľaváci (celkom 4 osoby, ktoré napodobňovali podpisy ľavou rukou) jednoznačne mali horšie výsledky, t. j. menšie zhody podpisov (s celkovým priemerom 15 percent a pritom nikto z nich neprekročil hranicu zhody 60 percent). Štatisticky je táto vzorka malá na reprezentatívnu vzorku. Môžeme ale predpokladať, že ľavou rukou je ťažšie falšovať podpis písaný pravou rukou a opačne.

**Testovanie hypotéz II. časti**

Táto časť rieši ekvivalentnosť podpisového napodobnenia z pohľadu celkových hodnôt, t. j. či oba podpisy sú rovnako ťažko napodobiteľné.

Vychádza sa z predpokladu prijatia hypotézy H 5.7.I.1. Bola zistená hodnota Fisherovho testu (Markechová et al., 2011, str. 145), v tomto prípade dvojstranného F-testu pre zhodu rozptylov Z = 1.7156. Kvantil Fisher - Snedecor rozdelenia pri 46 a 44 stupňoch voľnosti pre $\alpha = 0.01$ je 2.1923 a pre $\alpha = 0.05$ je 1.8111. Pretože $Z < 1.8111$ nemôžeme zamietnuť zhodu rozptylov na hladine významnosti 0.05 a ani na hladine významnosti 0.01.

Pre testovanie stredných hodnôt sa preto použil dvojvýberový t-test pri rovnosti rozptylov. Hodnota t-testu vyšla na t = 5.1749. Kvantil Študentova t-rozdelenia pri 90 stupňoch voľnosti pre $\alpha = 0.01$ je 2.6316, pre $\alpha = 0.05$ je 1.9867. Pretože $t > 2.6316$, sa zamieta rovnosť stredných hodnôt, a to na hladine významnosti 0.05 aj na 0.01.

Z výsledkov je jednoznačné, že je štatisticky významný rozdiel priemerov pri zhode falšovania dvoch rozdielnych podpisov. Umelo vytvorený podpis A bolo jednoduchšie falšovať ako skutočný podpis B vykonávaný nacvičeným spôsobom na základe dlhodobého návyku písania danej osoby.

Na základe zistených rozdielov sa nulová hypotéza H 5.5.II.0 zamieta (a to na hladine významnosti 0.05 aj na 0.01) v prospech alternatívnej hypotézy:

*H 5.7.II.1 – Podpis A a B sú rôzne ťažko napodobniteľné.*

Hypotéza bola prijatá.

**Testovanie hypotéz III. časti**

Táto hypotéza sa zaoberá tým, či je miera zhody medzi pravým podpisom a jeho falzifikátom priamo úmerná počtom vykonaných pokusov o jeho napodobnenie. Bola skúmaná korelácia a regresie medzi počtom pokusov a dosiahnutou mierou zhody medzi pravým a falzifikovaným podpisom. Vychádzalo sa z predpokladu, že podpis je biomechanický pohyb s pomocou nástroja pre podpisovanie, preto sa ľudia môžu trénovaním pohybov naučiť jednotlivé pohyby a opakovaním ich zdokonaľovať.

Bol skúmaný možný regresný vzťah za predpokladu, že počet pokusov (nezávislá premenná) je funkciou miery zhody pravého a falzifikovaného podpisu (závislá premenná). Možný regresný vzťah bol skúmaný $R^2$ štatistickým meradlom, ktorý znázorňuje ako sú údaje blízko k navrhovanej regresnej línii. V praxi je $R^2$ hodnota, ktorá poskytne nejaké informácie

o spôsobilosti modelu. V regresii je koeficient určenia $R^2$ štatistickým ukazovateľom toho, ako dobre predpovede regresie približujú k skutočným dátovým bodom. $R^2 = 1$ označuje, že regresné predpovede dokonale zodpovedajú údajom. 0 % naznačuje, že model neaproximuje žiadnu variabilitu údajov o predikciách okolo jeho priemeru. V prípade testovaných údajov pre zhody podpisov A aj B bola hodnota ukazovateľa $R^2$ vo všetkých prípadoch skúmaných závislostí (lineárna, kvadratická, logaritmická apod.) hodnotou malá ($R^2 << 1$) či blízka k 0. Možno teda usúdiť, že silná aproximačná závislosť medzi údajmi počet pokusov a miery zhody nebola zistená.

Vzhľadom na nemožnosť použiť Pearsonov korelačný koeficient bol použitý Kendallov koeficientu korelácie. Z výsledkov Kendallova koeficientu vyplýva (*Tabuľka 5.14*), že nebola zistená štatistická významná závislosť ani na hladine významnosti 0.01 medzi údajmi *Počet pokusov „n“* a *Miera zhody „n“*; kde *„n“* sú údaje podpisov A alebo B). Možno teda konštatovať, že signifikantná korelácia medzi mierou zhody a počtom pokusov neexistuje ani pri jednom z podpisov A a B.

Nulová hypotéza *H 5.7.III.0* sa preto zamieta (korelácia minimálne na hladine významnosti 0.01) a prijíma sa alternatívna hypotéza

*H 5.7.III.1 – Korelácia a regresie medzi počtom pokusov o napodobnenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho falzifikátom nie sú štatisticky významné.*

Hypotéza bola prijatá.

**Dodatok k tejto časti**

Korelácia a regresie medzi počtom pokusov o napodobenie podpisu a výslednou mierou zhody medzi pravým podpisom a jeho napodobením nie je štatisticky významná. Z výsledkov sa môže preto predpokladať, že talent falzifikovať podpisy je individuálna záležitosť jednotlivých osôb a úspešnosť je „funkciou“ talentu falzifikovať a nie je priamo úmerná počtu pokusov o napodobnenie.

Postupné individuálne zlepšovanie zhody falzifikácie na počte pokusov nebola skúmaná, lebo každý signatár odovzdával 1 výsledný falzifikovaný podpis na každý vzorový podpis. Nebola presne stanovená metóda na čítanie počtu pokusov, tá hodnota bola ponechaná na signatára. Rozdiely mohli byť spôsobené rozličnou subjektívnou úvahou jednotlivých signatárov.

**V.O. 7.5.II.1 – Aká má byť stanovená miera zhody podpisu?**

Výskumná otázka, ku ktorej smerovali výsledky testovaných hypotéz slúži na overenie, či vôbec existuje reálna možnosť falšovania DBP. Preto sú skúmané podmienky falšovania a stanovuje sa odporúčaná reakcia pri stanovení signifikantnej miery zhody pri DBP v rôznych aplikáciách.

Potvrdila sa hypotéza o tom, že jednotlivé podpisy sa dajú rôzne ťažko napodobniť a to aj v prípade, ak má falšovateľ k dispozícií dynamický model podpisu. V tomto prípade sa jednalo o umelo vytvorený podpis A, ktorý bolo ľahšie napodobniť, ako skutočný podpis B vykonávaný nacvičeným spôsobom na základe dlhodobého návyku písania danej osoby. Miera úspešnosti falšovania podpisov bola veľmi malá a znižovala sa zvýšením požadovanej výšky zhody podpisov pre akceptáciu audítorským softvérom. Za podmienok, ktoré nemožno štandardne zabezpečiť (získanie vzorového DBP a opakované premietanie dynamiky podpisu pri pokusoch falšovania), potrebnú mieru zhody ( $\geq$ 80%) pri prvom umelo vytvorenom podpise dosiahli len 2 osoby a pri druhom originálnom podpise nedosiahol nikto z účastníkov.

Možno teda konštatovať, že DBP je vysoko odolný proti napodobeniu inou osobou (za štandardných podmienok zaistenia bezpečnosti dát vypovedajúcich o dynamike DBP). Okrem nesporných falšovateľských schopností to totiž súčasne vyžaduje vytvorenie podmienok na analýzu dynamiky vykonaného podpisu (prístup k dátam, ktoré sú chránené šifrovaním, viď Obrázok 5.4) čo pri bezpečnej implementácii DBP (viď Smejkal et al., 2013) je prakticky vylúčené, pretože falšovateľ za štandardných podmienok nemá možnosti zobraziť dynamiku podpisu.

**Výsledky získané v minulosti z primárne dostupných dôveryhodných zdrojov:**

- V roku 2015 bolo zistené, že priemerná miera zhody podpisov u testovaných osôb je **77 %**, s vynechaním prvého podpisu pri vytváraní vzorového podpisu až **81 %**. (Smejkal et al., 2015)
- V roku 2016 bolo zistené, že priemerná miera zhody podpisov osôb, ktoré sa nachádzali v stresujúcej situácii, bez uvažovania prvého podpisu predstavovala **79%** až **84 %**. (Smejkal et al., 2016)
- Z primárneho výskumu bolo zistené (viď Tabuľka 5.5 a Tabuľka 5.6), že priemerná miera zhody podpisov vytváraných na rôznych snímacích zariadeniach bez uvažovania prvého podpisu predstavovala **79 %**.

**Signifikantná miera zhody pre praktické použitie DBP**

Podľa oznámenia distribútora hardware aj software používaného pri primárnom výskume (Contrisys s.r.o., 2018) je obvykle ako natívna hranica pre pravosť podpisu bez nutnosti ďalšieho preverovania považovaná miera zhody 70 % a viac. Táto hodnota korešponduje s vyššie uvedenými výsledkami. Z experimentu možno odvodiť, že vo veľmi výnimočných prípadoch, ak by falšovateľ mal možnosť zistiť, aký je celkový priebeh dynamiky podpisu, nebude uvedených 70% postačujúcich.

Na základe analýzy rizík, bezpečnostných politík a ďalších orientačných dokumentov organizácie, môže signifikantná požadovaná miera zhody pri DBP byť škálovateľne/kaskádovo nastavený napr. nasledovne:

- **60% a viac** - podpis vytvorený za osobnej prítomnosti zodpovedného zamestnanca organizácie, ktorý dohliada na priebeh podpisu (eliminuje svojou prítomnosťou pokusy o napodobenie) a môže si vyžiadať identifikáciu osoby aj iným spôsobom,
- **70% a viac** - podpis môže byť uskutočnený na diaľku a je postačujúce v prípade, keď sa ním neprekročí stanovený limit pre operácie takouto autentizáciou, daný analýzou rizík, resp. bezpečnostnou politikou,
- **80% a viac** - podpis môže byť vytvorený na diaľku a je považovaný za pravý. Pre prípad veľmi citlivých transakcií (daných hodnotou vyjadrenou v peniazoch, alebo inou charakteristikou) by úplnú istotu mohlo poskytnúť zvýšenie hranice na 85 % (v súlade s výsledkami tohto experimentu). Tu je ale treba počítať s možnou vysokou mierou odmietnutia pravých podpisov (FRR), preto je toto ďalšie zvýšenie hranice akceptácie na diskusiu a/alebo ďalším experimentom.

### 5.9.3 Diskusia a záver tejto časti

Predmetom tohto výskumu bola on-line metóda, ktorá na rozdiel od off-line metódy využíva snímanie procesu podpisovania a následnú analýzu vzorky biometrických dát vytvorených v procese podpisovania.

Výsledky experimentu v kontexte s predchádzajúcimi publikovanými výsledkami ukázali, že možnosť napodobnenia cudzieho podpisu bez znalosti dynamiky nie je možné. Ak by mal falšovateľ najluxusnejšie možné podmienky, spočívajúce v možnosti neobmedzeného skúmania a napodobňovanie cudzieho DBP, potom nemožno úspešné napodobenie úplne

vylúčiť, hoci by k nemu došlo iba nízkou pravdepodobnosťou (viď hodnoty FAR v tabuľke: *Tabuľka 5.12*).

Potvrdila sa hypotéza o tom, že jednotlivé podpisy sa dajú rôzne ťažko napodobniť. Bolo ťažšie napodobniť originálny podpis vykonávaný nacvičeným spôsobom na základe dlhodobého návyku písanie danej osoby (viď podpis B). Preto možnosť napodobniť určitý podpis je závislý na samotnej komplexnosti daného podpisu. Ďalej bolo preukázané, že úspešnosť napodobenia cudzieho DBP všeobecne nezávisí od počtu pokusov, ale skôr na individuálnych schopnostiach falšovateľov

Voľbou nastavenia hranice miery zhody pre akceptáciu podpisu možno dobre riadiť riziká spojené s používaním DBP v rôznych situáciách. Za predpoklad bezpečnej implementácie DBP a vhodne nastavenej signifikantnej miery zhody možno konštatovať, že DBP je pri dodržaní štandardných podmienok vysoko odolný proti napodobeniu inou osobou.

Vzhľadom na riziká, ktoré sú späté s používaním inými spôsobmi autentizácie (znalosťou alebo vlastníctvom predmetu) nemožno DBP považovať za metódu, ktorá by prinášala vyššie bezpečnostné riziko ako ostatné formy autentizácie.

## 5.10 Súhrn a syntéza primárneho výskumu

Hlavným cieľom bolo prijať alebo vyvrátiť hlavnú hypotézu o tom, že DBP je vhodný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu. Pod váhou zistených dôkazov vyplývajúcich z výskumov a experimentov sa hypotéza H 0.0: *„DBP je použiteľný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu“* **prijíma**. Tým pádom sa alternatívna hypotéza H 0.1*“DBP nie je použiteľný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu“* **zamieta**.

**Odôvodnenie**

Použitie DBP je prirodzený, ľahko dostupný nástroj pre overovanie používateľov a kombináciami s ďalšími faktormi môže dosiahnuť silné zabezpečenie autentizácie dokumentov, resp. iných foriem právnych úkonov. Táto metóda v on-line režime zaručuje vysokú spoľahlivosť a presnosť overenia. Zavedením dynamického biometrického podpisu sa dá dosiahnuť eliminácia možností podpisových podvodov, kvôli unikátnosti biometrického podpisu jedinca.

DBP je výborná alternatíva na elektronický podpis pre vnútropodnikovú komunikáciu a vie plne podporiť obeh elektronických dokumentov v podniku. Bolo dokázané, že použitím DBP sa vie zefektívniť vnútropodniková komunikácia a plne podporiť elektronický obeh dokumentov. Preto implementácia DBP vie byť pre podnik ekonomicky rentabilná investícia.

Z experimentov možno konštatovať, že napriek technologickým rozdielom v jednotlivých snímacích zariadených DBP sa stabilita podpisov pri zmene zariadenia nemení, líši sa však variabilita (rozptyl, resp. smerodajná odchýlka) jednotlivých zariadení. V primárnom výskume sa skúmala aj stálosť podpisu pri rôznych pozíciách držania tela. Z výsledkov sa dá posúdiť, že v prípade technológie DBP hodnoty chybovosti FRR a FAR sú závislé na variabilite podpisu signatára. Variabilita podpisu, či nízka miera zhody medzi jednotlivými podpismi sa prejavuje výnimočne u signatárov a úzko súvisí so stabilitou podpisu (správnym vyhodnotením používateľa).

Vzhľadom na riziká, ktoré sú späté s používaním iných spôsobov autentizácie (znalosťou alebo vlastníctvom predmetu) primárny výskum potvrdil, že DBP nemožno považovať za metódu, ktorá by prinášala vyššie bezpečnostné riziko ako ostatné formy autentizácie.

Napriek tomu je potrebné v pri zavedení DBP zvážiť niekoľko hlavných aspektov:

- Prístup k používaniu DBP u osôb s vysokou variabilitou vlastného podpisu. Sú osoby, pri ktorých je podpis nenacvičená procedúra, alebo majú vysokú intra-personálnu variabilitu, a preto majú menej stabilný podpis. V prípade laikov by mohla byť stabilita

podpisu kompenzovaná natrénovaním. Pri mentálnych a iných chorobách prejavujúce vysokú intra-personálnu variabilitu podpisu (napr. Parkinsovova choroba, pri ktorej dochádza k poruchám písma (tzv. mikrografii), ktorá je typická pre toto ochorenie a je charakterizovaná postupným zmenšovaním písmen, nápadným zhoršením čitateľnosti rukopisu a tiež zhusťovaním textu (parkinson-help, 2018)) by mal byť vyhodnocovací algoritmus testovania zhody doladený, alebo by bolo potrebné použiť nejakú vhodnú doplnkovú/alternatívnu autentizáciu pre používateľa (napr. pre prípady krátkodobého ochorenia alebo pri Parkinsonovej chorobe, pri demencii apod.).

- Zvýšenie celkovej prijateľnosti podpisu používateľov sa dá docieliť vynechaním 1 podpisu signatára. Preto je racionálne pri vytváraní vzorového podpisu (etalónu) prvý podpis vynechať (prvý interpretovať ako „skúšobný“ podpis).
- Nastavenie konkrétnej minimálnej miery zhody popisov, pri ktorej sú považované podpisy za zhodné (vytvorené rovnakou osobou), ktorá zostáva otázkou implementácie, respektíve na rozhodnutí používateľa/organizácie, a to vrátane zohľadnenia výsledkov analýzy rizík.

**Výhody použitia DBP**

- Používateľ sa vie podpísať ako perom na papier (a pod podpisovým povrchom je snímač), alebo častejšie na pad (elektronické zariadenie) špeciálnym perom.
    - Prijateľné a dobre známe pre používateľa - proces podpisu je bežná forma verifikácie a tak intuitívna a známa činnosť pre používateľa.
    - Priame implementovanie do IS. Relatívne jednoduchá integrovateľnosť zariadenia do už existujúcich systémov.
- Podpis sa nedá stratiť, ani zabudnúť (výnimkou sú extrémne prípady, napr. silná amnézia, demencia). Nemal by nastať problém ako pri autentizácii pomocou znalosti, že dotyčný na tajné heslo/PIN zabudne. Výhoda oproti autentizácie pomocou vlastníctva (napr. token) je, že DBP sa nedá stratiť, požičať alebo ako predmet odcudziť.
    - Na rozdiel od statického (off-line) podpisu, ktorý môže byť pozorovaním napodobňovaný, dynamiku podpisu nie je možné odpozorovať z výsledného obrazu podpisu.
- Stálosť podpisu. Používatelia sa podpisujú stále rovnako.
- Podpísanie elektronických dokumentov z podhľadu bezpečnosti:

- zaistenie integrity dokumentu všeobecne, aby z otvoreného dokumentu bolo jasné, či sa jedná o originál alebo falzifikát (protiopatrenie proti falšovaniu obsahu dokumentu);
- pripojenie podpisu k dokumentu pre zaistenie integrity a ochrana proti podpisovým podvodom (protiopatrenie proti falšovaniu podpisu inou osobou);
- zaistenie nepopierateľnosti vlastného podpisu.

- Podpísanie elektronických dokumentov z podhľadu efektívnosti komunikácie – bolo dokázané že plne elektronická komunikácia zefektívňuje podnikové procesy.
  - Podpora nástrojov automatickej kontroly správneho vyplnenia elektronických dokumentov, rýchlejšie šírenie informácie a rýchlejšia komunikácia.
  - DBP vie plne podporovať „Document management system“.
- Úspory a ekologickosť - možnosť plne nahradiť papierové dokumenty elektronickými, resp. bezpapierový proces komunikácie (úspora spotreby papiera a zbytočnej tlače).
- Archivácia a rýchla dostupnosť elektronických dokumentov prostredníctvom ICT.
  - Možnosť komunikácie aj na diaľku.

**Nevýhody použitia dynamického biometrického podpisu:**

- Nutnosť použitia hardvéru.
- Pri relevantných zraneniach podpisujúcej sa ruky je táto metóda prakticky vylúčená.
  - Preto je racionálne zaviesť sekundárny autentizačný systém, ktorý ale musí byť bezpečný (odporúča sa viacfaktorová autentizácia).
- V dlhodobom časovom horizonte sa proces vytvárania podpisu subjektu môže meniť. Môže to byť spôsobené prostredníctvom procesu starnutia používateľa, onemocnení (reuma, Parkinsonova choroba) atď. V takomto prípade je potrebné, aby riešenie autentizácie počítalo s touto situáciou podobne, ako v prípade krátkodobého zranenia podpisovej ruky. Empiricky je táto zmena zanedbateľná v komparácii s ostatnými autentizačnými faktormi:
  - Autentizačný faktor znalosti: časová platnosť hesiel a použiteľnosť elektronických certifikátov je obmedzená.
  - Autentizačný faktor predmetmi: rýchly vývoj technológií spôsobuje spätnú nekompatibilitu hardvérových tokenov (magnetové pásky, staré typy USB rozhraní, atď.).

- Zriedkavo sa môže prejaviť u jednotlivcov nestabilita podpisu.
    - Osoby sa môžu inak podpisovať ale nacvičenie podpisu by malo kompenzovať stabilitu (dôkazom slúžia pri experimentoch osoby s nacvičeným podpisom, ktorý je stabilný).
    - Pri neurologických poruchách (napr. Parkinsonova choroba), vzniká problém predikcie algoritmu pri vyhodnotení rukopisu a ručne kreslených tvarov.

# 6 Prínos práce

Hlavné prínosy dizertačnej práce sú vzájomne prepojené. Možné delenie prínosov by mohlo byť do oblastí vedeckej teórie, do akademickej pedagogiky/andragogiky a do prínosov použiteľných v praxi, a to konkrétne pri autentizácii a identifikácii používateľov a pri efektívnej vnútropodnikovej, či vnútroorganizačnej komunikácii. Za hlavné prínosy dizertačnej práce v oblastiach teórie a praxe sa môže považovať predovšetkým:

- Prínos do akademickej pedagogiky/andragogiky. Na základe literárnej rešerše bola vykonaná systematizácia autentizačných faktorov a metód autentizácií. Rešeršný charakter sekundárneho výskumu obsahuje viac ako dvesto zdrojov publikácií a vedeckých prác zo zahraničnej a tuzemskej vedeckej literatúry, zo svetovej a tuzemskej legislatívy a súvisiacich noriem. Výskum vychádza zo všeobecnej teórie informačných systémov a reprezentuje autentizačné možnosti používateľov, autorizáciu a riadenie prístupu. Slúži na objasnenie aktuálnych poznatkov a možností IS a bezpečnej autentizácie používateľov. Je reprezentovaný široký prehlaď autentizačných technológií, ktoré majú vymenované výhody ba aj úskalia, a preto ich možno jednoducho porovnať, či vyhodnotiť komparatívnou metódou. Tento komparatívny prehľad autentizačných metód, ako aj výsledky dizertačnej práce sú využiteľné v predmetoch v oblasti informačných systémov, informačných technológií a ich bezpečnosti.
- Z pohľadu praxe sú poznatky zo sekundárneho výskumu použiteľné na objasnenie vzorov a trendov v ICT a vnútropodnikovej komunikácie. Boli reprezentované aj očakávania autentizačných technológií v podnikovej praxi.
- Prínos pre ekonomické hodnotenie rentabilnosti kybernetickej bezpečnosti v praxi. Bol stanovený vzorec pre výpočet ekonomickej efektívnosti kybernetickej bezpečnosti. Reprezentované bolo na niekoľkých ukážkových príkladoch, že zvládnutie kybernetickej bezpečnosti má vplyv na dlhodobú stabilitu firmy (zníženie nákladov pri kybernetických útokoch, zvýšenie prínosov znížením rizika pokút napr. podľa GDPR, zaistenie business continuity apod.). Tiež bolo dokázané, že elektronický obeh dokumentov vie zefektívniť vnútropodnikovú komunikáciu a urýchliť spracovanie údajov.

- Vedecký prínos. Na základe relevantnej odbornej literatúry boli indukované výskumy, ktoré kontinuálne nadväzujú na problematiku DBP. Indukovaných výskumných otázok bolo celkovo 18 a indukovaných hypotéz bolo celkovo 18. Na odpovede výskumných otázok a testovanie hypotéz bola navrhnutá vlastná metodológia a bol vykonaný primárny zber údajov. Celkovo bolo do výskumov angažovaných: 90 dotazníkových respondentov a viac ako 150 signatárov. Analyzovaných bolo viac ako 1000 podpisov pri rôznych okolnostiach. Pri experimentoch boli použité rôzne snímacie technológie, SW a programovacie techniky. Pre testovania hypotéz boli použité primárne údaje a adekvátna štatistická matematika. Všetky výskumné otázky boli zodpovedané a všetky hypotézy vyhodnotené.
- Prínos dôležitých informácií ohľadne DBP a jej použiteľnosti v praxi. Výsledky experimentov sú významnou informáciou pre diskusie o bezpečnosti a používania DBP ako v oblasti e-governmentu, tak pre súkromnoprávne účely. Na základe analýzy rizík, bezpečnostných politík a ďalších orientačných dokumentov organizácie, môže byť signifikantná požadovaná miera zhody pri DBP škálovateľne/kaskádovo nastavená. Tento návrh bol aj príkladom reprezentovaný. Bolo zistené, že DBP vie zabezpečiť dôveryhodnú výmenu dát medzi oprávnenými používateľmi pri zaistení neodmietnuteľnosti vykonaných činností.

# Záver

Prvá hlavná kapitola práce je určená pre unifikáciu dôležitých pojmov a skratiek, ktoré sú relevantné na skúmanú tému. Druhá hlavná kapitola v krátkosti stanovuje zdôvodnenia a zameranie dizertačnej práce. Tretia hlavná kapitola je rozsiahla a zahŕňa teoretické východiská a stav vedeckého poznania danej problematiky. Z tejto kapitoly sa potom odráža nasledujúca hlavná kapitola, v poradí štvrtá, ktorá stanovuje ciele celej práce. Táto štvrtá kapitola združuje aspekty a hypotézy, ktoré obsahovo znázorňujú komplexicitu danej témy. Samotný výskum sa potom delí na sekundárny a primárny výskum.

Sekundárna analýza kladie za základný cieľ analyzovať oblasti skúmania v rámci danej problematiky. Toto je vykonané nielen prostredníctvom zoznamu odborných literárnych zdrojov, legislatívy, normami a poskytnutou diskusiou nad ich obsahom, ale aj demonštráciou autentizačných faktorov a metód v kapitole *3 Teoretické východiská a stav vedeckého poznania*. Sekundárny výskum tiež ukázal, že novodobé trendy odbúravajú hranice medzi vnútorným a vonkajším prostredím firmy. Odbúravaním hraníc medzi vnútorným a vonkajším prostredím firmy sa zvyšuje tlak na informačnú bezpečnosť, ktorú novodobé trendy sťažujú a bez zavedenia ochranných prvkov aj ohrozujú. Preto sa v primárnom výskume navrhla metóda na hodnotenie rentabilnosti kybernetickej bezpečnosti, kde spadá aj výsledná problematika DBP.

Piata hlavná kapitola slúži na vyhodnotenie analýzy a výskumu. V kapitole *5.1* sú zodpovedané výskumné otázky 1 až 5. Tieto výskumné otázky sa zameriavali na možnosti používania autentizačných technológií v podnikoch. Výsledky analýzy porovnávania jednotlivých faktorov a metód autentizácie slúžili na výber hlavnej autentizačnej metódy podľa stanovených podmienok. Ich cieľom bol návrh metódy pre bezpečnú autentizáciu používateľov a efektívnu vnútropodnikovú komunikáciu. Práca súbežne znázorňuje legislatívu a normy vzťahujúce sa na implementáciu autentizačných systémov.

Ako vhodný nástroj pre efektívnu vnútropodnikovú komunikáciu sa javí technológia, ktorá zahŕňa použitie dynamického biometrického podpisu. Práca sa preto s touto tematikou zaoberá podrobnejšie a testuje túto metódu autentizácie. Bolo vykonaných niekoľko nezávislých experimentov na zber primárnych údajov pre každý aspekt DBP zvlášť.

Šiesta kapitola sumarizuje celkový prínos práce. Výsledky experimentov sú významnou informáciou pre diskusie o bezpečnosti a používania DBP ako v oblasti e-governmentu, tak pre súkromnoprávne účely. Pod váhou zistených dôkazov vyplývajúcich z výskumov a experimentov bola prijatá hypotéza o tom, že DBP je použiteľný nástroj pre bezpečnú a efektívnu vnútropodnikovú komunikáciu.

# Zoznam použitej literatúry a zdroje dát


[1] AKYILDIZ, I. F., SU, W., SANKARASUBRAMANIAM, Y., CAYIRCI, E. (2002). Wireless sensor networks: a survey. *Computer networks*, *38*(4), 393-422.

[2] ALSALEH, M., MANNAN, M., VAN OORSCHOT, P. C. (2012). Revisiting Defenses against Large-Scale Online Password Guessing Attacks. *IEEE Transactions on Dependable and Secure Computing*, v.9 n.1, p.128-141, January 2012.

[3] APPLE. (2017). *Face ID Security*. [online]. [cit. 20. 08. 2018] URL: https://www.apple.com/business/docs/FaceID_Security_Guide.pdf

[4] ARTHUR, C. (2014). "Naked celebrity hack: security experts focus on iCloud backup theory. [online]. *The Guardian,* september 1, 2014. [cit. 26. 01. 2017]. URL: https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence

[5] BADRINATH, G., GUPTA, P. (2011). Stockwell transform based palm-print recognition. *Applied Soft Computing*, 11 (7), 4267–4281

[6] Bala, R. (2017). Finger Nail Plate Classification for Transient Biometric Identification. *IJSRCSEIT*, Volume 2, Issue 4, ISSN : 2456-3307

[7] BANERJEE, S. P., WOODARD, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7(1), pp.116-139

[8] BIČONSKÝ, R. (1992). *Tajemství písma*. Praha: Panorama. 112 s. ISBN: 80-7038-268-6

[9] BIOHACK.ME. (2018). [online]. [cit. 2014-11-21] URL: https://biohack.me/

[10] BLACK, H. C., NOLAN, J. R. NOLAN-HALEY, J. M. (1993). *Blackův právnický slovník*. 6. vyd., v ČR 1. Praha: Victoria Publishing,. 768 p. ISBN 80-85605-23-6

[11] BONNEAU, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. *IEEE Security & Privacy* (Oakland) 2012. San Francisco, CA, USA, p. 538-552. DOI: 10.1109/SP.2012.49

[12] BOUAMRA, W., DJEDDI, C., NINI, B., DIAZ, M., SIDDIQI, I. (2018). Towards the design of an offline signature verifier based on a small number of genuine samples for training. *Expert Systems with Applications*, *107*, p. 182-195.

[13] BURR, E. W. et al. (2013). *Electronic Authentication Guide. Special Publication* 800-63-2. [online]. NIST Special Publication 800-63-2. 123 p. [cit. 2016-11-16]. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[14] BUTTLE, F. (2004). *Customer relationship management*. Routledge. Elsevier Butterworth-Heinemann. ISBN 0 7506 5502 X

[15] CHRISTIE MEDICAL HOLDINGS. (2016). *See how veinviewer works.* [online]. [cit. 20. 02. 2017]. URL: https://www.christiemed.com/

[16] CINKAIS, R., VÁBEK, J. (2015). *Důležité otázky při výběru biometrické modality.* [online]. Přednáška na konferenci SECURITY 2015, 18. 02. 2015. [cit. 21. 11. 2017]. URL: http://docplayer.cz/34431484-Dulezite-otazky-pri-vyberubiometricke-modality-roman-cinkais-jiri-vabek-wincor-nixdorf-s-r-o.html

[17] COCHRAN, W. G., COX, G. M.. *Experimental designs.* 2nd edition. New York: John Wiley and Sons, 1957. ISBN: 978-0-471-54567-5

[18] CONTRISYS. (2018). [online]. Contrisys s. r. o. [cit. 16. 06. 2018] URL: http://www.contrisys.com/

[19] DANGEROUS THINGS. (2018). [online]. [cit. 21. 11. 2014] URL: https://dangerousthings.com/

[20] DAVIS, J. (2014). *Two Factor Auth (2FA).* [online]. [cit. 21. 11. 2014] URL: https://twofactorauth.org

[21] DIAZ, M., FERRER, M. A., PIRLO, G., GIANNICO, G., HENRIQUEZ P. IMPEDOVO, D. (2015) Off-line Signature Stability by Optical Flow: Feasibility Study of Predicting the Verifier Performance. In *Proceedings of 49th Annual 2015 IEEE International Carnahan Conference on Security Technology (ICCST)*, 21-24 September 2015, Taipei, Taiwan, R.O.C., pp. 341-345, ISBN 978-9-860-46303-3

[22] DIAZ-CABRERA, M., FERRER, M. A., MORALES, A. (2015). Modeling the lexical morphology of western handwritten signatures. *PloS one,* vol. 10, no. 4, p. e0123254

[23] DOLEŽAL, P., CINKOVÁ, P., BENEDIKTOVÁ, K., URBAN, Š., LNĚNIČKOVÁ, J., PINC, L. (2016). Molekulová skladba pachové signatury člověka. In: *Kriminalistika* Roč. 49, č. 3 (2016), p. 200-210

[24] DOSEDĚL, T. (2004). *Počítačová bezpečnosť a ochrana dat*. Praha, nakladatelství Computer Press. ISBN 80-251-0106-1

[25] DRAHANSKÝ, M. (2007). *Přehled biometrických systémů a testování jejich spolehlivosti*. [online]. Kongres Bezpečnosti sítí, Praha, 11.04.2007. [cit. 22. 08. 2018] URL: https://docplayer.cz/14955421-Biometrickych-systemu-a-testovani-jejich-spolehlivosti-prehled-drahan-fit-vutbr-cz-martin-drahansky-drahan.html

[26] DRAHANSKÝ, M., PERNICKÝ, R., KANICH, O., BAROTOVÁ, Š. (2017). Verarbeitung von beschädigten Fingerabdrücken in der polizeilichen Praxis. *DuD - Datenschutz und Datensicherheit*, 2017, roč. 41, č. 7, s. 407-414. ISSN: 1614-0702

[27] DRAHANSKÝ, M., ORSÁG, F., DVOŘÁK, R., HÁJEK, J., VÁŇA, J., HERMAN, D., KNĚŽÍK, J., MARVAN, A., LODROVÁ, D., DOLEŽEL, M. (2011). *Biometrie*. Brno: Computer Press, s.r.o. , p. 294. ISBN: 978-80-254-8979-6

[28] DVOŘÁK, M., DRAHANSKÝ, M. (2017). Security of Hand Geometry. In *Proceedings of Conference SPI 2017*. Brno: Brno University of Defence, 2017. p. 17-29. ISBN: 978-80-7231-414-0

[29] ENSMINGER, J. J. (2010) Canine Tracking and Scent Identification: Factoring Science into the Threshold for Admissibility [online]. *The Social Science Research Network (SSRN)*. [cit. 20. 08. 2018]. URL: https://ssrn.com/abstract=1666490 , http://dx.doi.org/10.2139/ssrn.1666490

[30] ENSMINGER, J. J. (2011). *Police and Military Dogs: Criminal Detection, Forensic Evidence, and Judicial Admissibility*. CRC Press. ISBN 13: 978-1-4398-7240-6

[31] ENTRUST (2018). *Strong Authentication via Patented Grid Card Technology*. [online]. [cit. 20.08.2018]. URL: https://www.entrust.com/gridcard/

[32] ERDOGMUS, H., FAVARO, J., STRIGEL, W. (2004). Return on investment. *IEEE Software, 21*(3), 18-22.

[33] FAHMI, P. A., KODIROV, E., CHOI, D. J., LEE, G. S., AZLI, A. M. F., SAYEED, S. (2012). Implicit authentication based on ear shape biometrics using smartphone camera during a call. In *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on* (pp. 2272-2276). IEEE

[34] FAN, D., YU, P., DU, P., LI, W., CAO, X. (2012). A novel probabilistic model based fingerprint recognition algorithm. *Procedia Engineering, 29* , p 201–206

[35] FFIEC - Federal Financial Institutions Examination Council. (2005). *Authentication in an Internet Banking Environment.* [online]. [cit. 12. 11. 2015]. URL: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[36] FIERREZ, J., POZO, A., MARTINEZ-DIAZ, M., GALBALLY, J., & MORALES, A. (2018). Benchmarking Touchscreen Biometrics for Mobile Authentication. *IEEE Transactions on Information Forensics and Security*

[37] FORSYTH, D., PONCE, J. (2003). *Computer vision: a modern approach*. London: Prentice Hall, xxv, 693 p. ISBN 01-308-5198-1

[38] FOX-BREWSTER, T. (2015). *Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images* [online]. Forbes. [cit. 20. 08. 2018]. URL: https://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/#5618ace9214a

[39] FRANCIS, F., APARNA, M.S. & VINCENT, A. (2015). Biometric Online Signature Verification. *IOSR Journal of Electronics and Communication Engineering*, pp. 82-89.

[40] FUJITSU. (2013). *Biometrická technologie Fujitsu PalmSecure vrací identitu do vašich rukou.* [online]. Praha, 19 March, 2013. [cit. 18. 04. 2015]. URL: http://www.fujitsu.com/sk/about/resources/news/press-releases/2013/Biometrick--technologie-Fujitsu-PalmSecure-vrac--identitu.html

[41] GALBALLY, J., DIAZ-CABRERA, M., FERRER, M. A., GOMEZ-BARRERO, M., MORALES, A., & FIERREZ, J. (2015). On-line signature recognition through the combination of real dynamic data and synthetically generated static data. *Pattern Recognition.* Volume 48, Issue 9, 1 September 2015, Pages 2921-2934. ISSN: 00313203

[42] GIBBONS, J. D. (1993). Nonparametric Measures of Association. Sage University Paper series, *Quantitative Applications in the Social Sciences*, vol 91. Newbury Park, CA: Sage. doi: 10.4135/9781412985291

[43] GOOGLE. (2017). *About 2-Step Verification* [online]. [cit. 12. 01. 2017]. URL: https://support.google.com/accounts/answer/180744?hl=en

[44] HAFEMANN, L. G., SABOURIN, R., OLIVEIRA, L. S. (2016). Writer-independent feature learning for offline signature verification using deep convolutional neural networks. In *Neural networks (IJCNN), 2016 international joint conference on* (p. 2576–2583). IEEE

[45] HAFEMANN, L. G., SABOURIN, R., OLIVEIRA, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognition, 70,* p. 163–176

[46] HÁJEK, J., DOLEŽEL, M., DRAHANSKÝ, M. (2014) Biometric device for retina and iris recognition in intelligent houses. In: *Beiträge zum Usability Day XII Assistenztechnik für betreutes Wohnen*. Dornbirn: University of Applied Sciences Vorarlberg, 2014, pp. 143-147. ISBN 978-3-89967-943-4.

[47] HAN, W., CHAN., Ch.-F., CHOY, Ch.-S., PUN, K.-P. (2006). An efficient MFCC extraction method in speech recognition. *IEEE International Symposium on Circuits and Systems*, Island of Kos, 2006, pp. 4 pp.-.doi: 10.1109/ISCAS.2006.1692543

[48] HARPER, D. (2018). *communication (n.)* [online]. [cit. 08. 08. 2018]. URL: https://www.etymonline.com/word/communication

[49] HE, D., WANG, D. (2015). Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, *9*(3), 816-823.

[50] HIGGINBOTHAM JR., LEON, A. (1978). In The Matter of Color Race and the American Legal Process: The Colonial Period. New York: Oxford University. pp. 176–184.

[51] HM Government. (2016). National Cyber Security Strategy 2016 to 2021. [Online]. Published 1 November 2016. [cit. 12. 06. 2018]. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[52] HORTAI, F. (2015). Low- cost data mining application via unused smartphone devices using computer vision and relevant data security issues. In *18 Annual International Conference Enterprise and Competitive Environment Conference Proceedings.* First edition. Brno: Mendel University in Brno,. p. 304-313. ISBN: 978-80-7509-342- 4.

[53] HORTAI, F. (2017). Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature. *Ekonomika Management Inovace*, 2017, roč. Vol. 9, č. 2, 2017, s. 72-89. ISSN: 1804-1299.

[54] HSU, J. (1996). *Multiple comparisons: theory and methods*. Chapman and Hall/CRC. ISBN 0-412-98281-1

[55] HUANG, X., XIANG, Y., CHONKA, A., ZHOU, J., DENG, R.H.. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 22(8), pp.1390-1397.

[56] HUMPHREYS, E. (2011). *Information security management system standards. Datenschutz und Datensicherheit* - DuD 35 (1): 7–11. Print ISSN 1614-0702, Online ISSN 1862-2607.

[57] INBAVALLI, P., NANDHINI, G. (2014). Body odor as a biometric authentication. *Int. J. Comput. Sci. Inform. Technol*, *5*(5), 6270-6274.

[58] JAIN, A. K., ROSS, A. (2015). Bridging the gap: from biometrics to forensics. *Phil. Trans. R. Soc. B*, *370*(1674), 20140254.

[59] JAIN. A. K., GRIESS, F. D., CONNELL, S. D. (2002). On-line signature verification. In: *Pattern Recognition* 35, p. 2963 – 2972

[60] KANICH, O., DRAHANSKÝ, M. (2017). Simulation of Synthetic Fingerprint Generation Using Petri Nets. *IET Biometrics,* 2017, roč. 6, č. 6, s. 402-408. ISSN: 2047-4938

[61] KARNAN, M., AKILA, M., KRISHNARAJ, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing, 11* (2), 1565–1573

[62] KENDALL, M. G., J. D. GIBBONS. (1990). *Rank Correlation Methods*. 5th ed. London: Griffin. ISBN: 0195208374

[63] KISLINGEROVÁ, E. (2001). *Oceňování podniku*. 2. přeprac. a dopl. vyd. Praha: C. H. Beck

[64] KOCH, M., CHVÁTALOVÁ, Z. (2017). Information Systems Efficiency Model. *Journal of Systems Integration*, *8*(3), 3-9.

[65] KODL J. Jr. (2010). *Mechanisms of Human Arm Motion Planning in the Presence of Multiple Solutions*. Imperial College, London.

[66] KORBAŘ T., STRÁNSKÝ A. et al. (1962). *Technický naučný slovník G – L*. Praha, Bratislava : SNTL, SVTL, 421 p.

[67] KOŠTIALIK, D., MARUNIAK, L., DRAHANSKÝ, M. (2017). Symptoms Detection in Eye Retina Image. In *2017 IEEE Symposium Series on Computational Intelligence.* Hawaii: IEEE Computer Society, 2017. s. 3088-3093. ISBN: 978-1-5386-4058-6.

[68] KRHOVJÁK, J. MATYÁŠ, V. (2007). *Autentizace a identifikace uživatelů.* [online]. Zpravodaj ÚVT MU. ISSN 1212-0901, roč. XVIII, č. 1, s. 1-5. [cit. 16. 11. 2014]. URL: http://webserver.ics.muni.cz/bulletin/articles/560.html

[69] KRIŠTOUFEK, K. et al. (1982). *Oborová encyklopedie - Výpočetní a řídící technika*. Praha.

[70] KUMAR, A., GARG, S., HANMANDLU, M. (2014). Biometric authentication using finger nail plates. *Expert systems with applications*, *41*(2), 373-386.

[71] KUMAR, A., PRATHYUSHA, K. V. (2009). Personal authentication using hand vein triangulation and knuckle shape. IEEE Transactions on Image processing, 18(9), 2127-2136.

[72] KUMAR, A., WU, C. (2012). Automated human identification using ear imaging. *Pattern Recognition*, *45*(3), 956-968.

[73] KUMAR, A., ZHOU, Y. (2012). Human identification using finger images. *IEEE Transactions on image processing*, *21*(4), 2228-2244.

[74] LAJEVARDI, S. M., ARAKALA, A., DAVIS, S. A., HORADAM, K. J. (2013). Retina verification system based on biometric graph matching. *IEEE transactions on image processing*, *22*(9), 3625-3635.

[75] LANDI, M. (2014). Stars' nude photo attack may have been down to password codes. In: *Irish Independent* [online]. September 2, 2014 . [cit. 26. 01. 2017]. URL: http://www.independent.ie/business/technology/news/stars-nude-photo-attack-may-have-been-down-to-password-codes-30552629.html

[76] LECUN, Y., BENGIO, Y., HINTON, G. (2015). Deep learning. *nature*, *521*(7553), 436.

[77] LEE, C. P., TAN, A. W., TAN, S. C. (2013). Gait recognition via optimally interpolated deformable contours. *Pattern Recognition Letters, 34* (6), 663–669

[78] LEE, J., JAIN, A., TONG, W. (2012). Image retrieval in forensics: tattoo image database application. *IEEE MultiMedia*, *19*(1), 40-49.

[79] LENZINI, G. BARGH, M. S., HULSEBOSCH, B. (2008). Trust-enhanced Security in Location-based Adaptive Authentication. Electronic Notes in: *Theoretical Computer Science*. Volume 197, Issue 2, 22 February 2008, Pages 105–119. Proceedings of the 3rd International Workshop on Security and Trust Management (STM 2007).

[80] LOPEZ-GARCIA, M., RAMOS-LARA, R., MIGUEL-HURTADO, O., CANTÓ-NAVARRO, E. (2014). Embedded system for biometric online signature verification. *IEEE Transactions on Industrial Informatics*. Publisher: IEEE Computer Society. ISSN: 15513203

[81] LORENC, V., MATYÁŠ, V. (2007). *Autentizační HW a možná vylepšení*. Zpravodaj ÚVT MU. ISSN 1212-0901, roč. XVIII, č. 1, s. 17-20. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/563.html

[82] LYREBIRD. (2018). [online]. [cit. 29. 06. 2018]. URL: https://lyrebird.ai/

[83] MADAR, Z. et al. (1995). *Slovník českého práva*. Praha, , sv. 1.

[84] MALATINO, H. (2017). Biohacking Gender: cyborgs, coloniality, and the pharmacopornographic era. *Angelaki*, *22*(2), 179-190.

[85] MALIK, M. I. (2015). *Automatic signature verification: Bridging the gap between existing pattern recognition methods and forensic science*. Ph.D. thesis, University of Kaiserslautern, Germany.

[86] MAŘÍK, V. (2016) *Průmysl 4.0 – výzva pro Českou republiku*. Praha: Management Press 2016 EAN: 9788072614400.

[87] MARKECHOVÁ, D. TIRPÁKOVÁ, A. STEHLÍKOVÁ, B. (2011). *Základy štatistiky pre pedagógov*. [online]. Druhé upravené a doplnené vydanie. Vydavateľ: Fakulta prírodných vied UKF v Nitre. ISBN 978-80-8094-899-3. [cit. 16. 06. 2018]. URL: http://www.km.fpv.ukf.sk/upload_publikacie/20120130_90405__1.pdf

[88] MARTINEZ-DIAZ, M. FIERREZ, J. GALBALLY, J. ORTEGA-GARCIA, J. (2008). Towards Mobile Authentication Using Dynamic Signature Verification: Useful Features and Performance Evaluation. In Proceedings Paper IEEE Conference*: 19th International Conference on Pattern Recognition* (ICPR 2008) Location: Tampa, FL Date: DEC 08-11, 2008. Pages: 2787-2791. ISBN:978-1-4244-2174-9, ISSN: 1051-4651

[89] MATES, P. MATOUŠOVÁ, M. (1997). *Evidence, informace, systémy-právní úprava*. 1. vydání. Praha: CODEX Bohemia. ISBN 80-85963-27-2

[90] MATES, P. SMEJKAL, V. (2012). *E-government v České republice: Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání, Praha: Leges, 2012. ISBN 978-80-87576-36-6.

[91] MAYES, K., & MARKANTONAKIS, K. (2008). *Smart Cards Tokens Security and Applications*. Springer-Verlag. Publisher: Springer, Cham. Print ISBN: 978-3-319-50498-8. Online ISBN 978-3-319-50500-8

[92] MEURANT, G. (2012). Introduction to electronic document management systems. Academic Press.

[93] MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY. (2013). *Informačná bezpečnosť.* [online]. Bratislava, [cit. 24. 04. 2014]. URL: http://informatizacia.sk/ext_dok-stud_2014_02_laici/16984c

[94] NEUHAUS, R., ARTKÄMPER, H. (2014) *Kriminaltechnik und Beweisführung im Strafverfahren. München*. C. H. Beck, München. ISBN 978-3-406-65653-8

[95] OBSIL, T., OBSILOVA, V. (2011). Structural basis for dna recognition by foxo proteins. *Biochimica et Biophysica Acta (BBA)-Molecular Cell Research, 1813* (11), 1946–1953

[96] OU, W., YOU, X., TAO, D., ZHANG, P., TANG, Y., ZHU, Z. (2014). Robust face recognition via occlusion dictionary learning. *Pattern Recognition, 47* (4), 1559–1572

[97] PAL, S., PAL, U., BLUMENSTEIN, M. (2014). Signature-based Biometric Authentication. In *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, (Eds. Editors: Azah Kamilah Muda, Yun-Huoy Choo, Ajith Abraham, Sargur N. Srihari), pp.285-314.

[98] PARKINSON-HELP. (2018). Online. URL: https://parkinson-help.cz/parkinsonova-nemoc-pn/priznaky-motoricke/poruchy-souvisejici-s-pohybem/

[99] PARZIALE, A., FUSCHETTO, S. G., MARCELLI, A. (2013). Exploiting stability regions for online signature verification. In *International Conference on Image Analysis and Processing* (pp. 112-121). Springer, Berlin, Heidelberg.

[100] PEOPLE V. KELLY (1976) 17 Cal.3d. 24. [online]. Crim. No. 19028. Supreme Court of California. May 28, 1976. [cit. 21. 08. 2018]. URL: https://scocal.stanford.edu/opinion/people-v-kelly-23058

[101] PHILLIPS, J. J. (1997). *Measuring return on investment* (Vol. 2). American Society for Training and Development. ISBN: 1-56286-065-8

[102] PILLAI, J. K., PATEL, V. M., CHELLAPPA, R., RATHA, N. K. (2011). Secure and robust iris recognition using random projections and sparse representations. *IEEE transactions on pattern analysis and machine intelligence*, *33*(9), 1877-1893.

[103] PIPER, F. ŚWIEBOCKA, T. (1996). *Auschwitz: Nazi Death Camp*. Translated by Douglas Selvage. Oświęcim: The Auschwitz-Birkenau State Museum. pp. 60–61. ISBN-13: 978-8385047742, ISBN-10: 8385047743

[104] PIRLO, G., IMPEDOVO. D. (2013). Verification of Static Signatures by Optical Flow Analysis. IEEE Trans. Human-Machine Systems, Vol. 43, Iss. 5, Sept. 2013, pp. 499-505.

[105] PORADA, V., SMEJKAL, V. (2017) Forensic identification and its possibilities in the process of detection, investigation and proving of cyber offences. In *International Day of Science 2017 - Economics, Managemnet, Innovation*. Moravian University College Olomouc, 2017. ISBN: 978-80-7455-060- 7.

[106] POSLANECKÁ SNĚMONVA PARLAMENTU ČR. (2018) Sněmovní tisk č. 138, 2. čtení

[107] POZO, A., FIERREZ, J., MARTINEZ-DIAZ, M., GALBALLY, J., & MORALES, A. (2017). Exploring a statistical method for touchscreen swipe biometrics. In *Security Technology (ICCST), 2017 International Carnahan Conference*, p. 1-4. IEEE.

[108] PRESS, W.H., TEUKOLSKY, S.A., VETTERLING, W.T., FLANNERY, B.P. (2017). *Numerical Recipes: The Art of Scientific Computing*. Third Edition, New York: Cambridge University Press. ISBN: 978-0-511-33555-6

[109] RAK, R., MATYÁŠ, V., ŘÍHA, Z. (2008). *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: GRADA. ISBN 978-80-247-2365-5.

[110] RAK, R., PORADA, V. (2007). Rozpoznávání identity člověka na základe jeho chůze. In: *Karlovarská právní revue*. - Roč. 3, č. 3, - s. 49-61. Lit.

[111] RANTZSCH, H., YANG, H., MEINEL, C. (2016). Signature embedding: Writer indepen- dent offline signature verification with deep metric learning. In *International symposium on visual computing*, p. 616–625. Springer

[112] ROBIN, E. (2017). NATO to spend 3 billion euros on satellite, cyber defenses. [Online]. *Reuters Online.* [cit. 2018-06-12]. URL: https://www.reuters.com/article/us-nato-cyber/nato-to-spend-3-billion-euros-on-satellite-cyber-defenses-idUSKBN16Y0P5

[113] ROSEN, L. D., SEARS, D. C., WEIL, M. M. (1993). Treating technophobia: A longitudinal evaluation of the computerphobia reduction program. *Computers in human behavior*, *9*(1), 27-50.

[114] ROSEN, L. D., WEIL, M. M. (1995). Computer availability, computer experience and technophobia among public school teachers. *Computers in human behavior*, *11*(1), 9-31.

[115] ROWE, R. K. (2010). U.S. Patent No. 7,735,729. Washington, DC: U.S. Patent and Trademark Office.

[116] RUSSELL, S. J., NORVIG, P. (2016). *Artificial intelligence: a modern approach*. Third edition. Malaysia; Pearson Education Limited. ISBN: 1292153962

[117] SATO, H., BERRY, C. W., CASEY, B. E., LAVELLA, G., YAO, Y., VANDENBROOKS, J. M., MAHARBIZ, M. M. (2008). A cyborg beetle: insect flight control through an implantable, tetherless microsystem. In *Micro Electro Mechanical Systems, 2008. MEMS 2008. IEEE 21st International Conference on* (pp. 164-167).

[118] SCHEFFÉ, H. (1999). *The Analysis of Variance.* New York: John Wiley & Sons. ISBN 0-471-34505-9.

[119] SCHOON, A., HAAK, R. (2002). *K9 Suspect Discrimination*. Canada: Detselig Enterprises Ltd. ISBN: 1-55059-233-5

[120] ŠČUREK, R. (2008). *Biometrické metody identifikace osob v bezpečnostní praxi*. Ostrava. [online]. [cit. 21. 11. 2014]. Dostupné z: http://www.biometrickypodpis.cz/PDF/biometricke_metody.pdf

[121] SHALAL, A., SELYUKH, A. (2015). Obama seeks $14 billion to boost US cybersecurity defenses. [Online]. [cit. 12. 06. 2018]. *Reuters Online*, URL: https://www.reuters.com/article/us-usa-budget-cybersecurity/obama-seeks-14-billion-to-boost-u-s-cybersecurity-defenses-idUSKBN0L61WQ20150202

[122] SHANNON, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal, 27 (July and October)*, p. 379-423 & 623-656

[123] SHIKARWAR, S., RATHOD, D., DIWANJI, H. (2014). Review paper on retina authentication and its security issues. *International Journal for Technological Research in Engineering*.

[124] SIGNOTEC. (2018). [Online]. [cit. 18. 06. 2018]. URL: https://www.signotec.com/

[125] SINGH, A. K., JOSHI, P., NANDI, G. Ch. (2014). Face recognition with liveness detection using eye and mouth movement. In: Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on. IEEE, 2014. p. 592-597.

[126] SINGH, S. (2003). *Kniha kódů a šifer*. 1. vydání. Praha: Argo. ISBN 8086569187.

[127] SMEJKAL, V. (2017). Dynamický biometrický podpis a nařízení GDPR. *Revue pro právo a technologie*. [online]. 2017, č. 16, s. s. 89-112. [cit. 2018-06-07]. ISSN: 1805-2797. URL: https://journals.muni.cz/revue/article/view/8282

[128] SMEJKAL, V. (2018). *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, s.r.o., 936 p. ISBN: 9788073807207.

[129] SMEJKAL, V., KODL, J. (2011). Strong authentication using dynamic biometric signature. In: *Proceedings of 45th Annual 2010 IEEE International Carnahan Conference on Security Technology (ICCST)*, Barcelona, Spain, October 18-21, p. 340–344, ISBN 978-145-7709-02.

[130] SMEJKAL, V., KODL, J. (2014). Assessment of the authenticity of Dynamic Biometric Signature. In *Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, p. 45–49, ISBN: 978-1-4799-3530-7.

[131] SMEJKAL, V., KODL, J. (2016). Authentication and Encryption in Ensuring the Security of Information Systems. In: Lisník, A., Pavlíček, A. (ed.) *Current Trends and Challenges in Economics and Management. Conference proceedings of the international conference "The message of John Paul II"*, 21.-22. 4. 2016, Poprad: VERBUM – 2017, p. 251-262. ISBN 978-80-561-0440-8.

[132] SMEJKAL, V., KODL, J., KODL, J. Jr. (2013). Implementing trustworthy dynamic biometric signature according to the electronic signature regulations. In: *Proceedings of 47th International Carnahan Conference on Security Technology, ICCST 2013*; Medellin; Colombia, pp. 165–170, ISBN 978-958-8790-65-7

[133] SMEJKAL, V., RAIS, K. (2013). *Řízení rizik ve firmách a jiných organizacích*. 4., aktualizované a rozšířené vydání. Grada Publishing, a.s., Praha. 488 s. ISBN 978-80-274-4644-9

[134] SMEJKAL, V., HORTAI, F., MOLNÁROVÁ, A. (2017). Risk and legal aspects of company's cyber security. In *Workshop specifického výzkumu 2017*. Brno: 2017. p. 50-61. ISBN: 978-80-214-5598-6.

[135] SMEJKAL, V., HORTAI, F., MOLNÁROVÁ, A. (2017). Znižovanie rizika ako nástroj zvýšenia hodnoty firmy. In *Řízení rizik procesů spojených s technickými díly.* Praha: ČVUT v Praze, Fakulta dopravní, 2017. s. 224-233. ISBN: 978-80-01-06351-4.

[136] SMEJKAL, V., KODL, J. (2008). Development trends of electronic authentication. Proceedings of the 42nd Annual Conference *IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1 – 6.

[137] SMEJKAL, V., KODL, J. (2009). Trendy rozvoje elektronické autentizace. *Data Security Management*, XIII., č 1, s 36-39, ISSN 2111-8737

[138] SMEJKAL, V., KODL, J., SIEGER, L., HORTAI, F., TESAŘ, P. (2017). Stability of a dynamic biometric signature created on various devices. In *Security Technology (ICCST), 2017 International Carnahan Conference on* (pp. 1-5). IEEE.

[139] SMEJKAL, V., KODL, J., SIEGER, L. (2016). The Influence of Stress on Biometric Signature Stability. In *Proceedings of 50th Annual 2016 IEEE International Carnahan Conference on Security Technology*. Orlando, Florida, USA, New York: Institute of Electrical and Electronics Engineers,. s. 37-41. ISBN: 978-1-5090-1070- 7

[140] SMEJKAL, V., KODL, J., SIEGER, L., NOVÁK, D., SCHNEIDER, J. (2015). The Dynamic Biometric Signature. Is the Biometric Data in the Created Signature Constant? In *Proceedings of 49th Annual 2015 IEEE International Carnahan Conference on Security Technology (ICCST)*. Taipei, Taiwan: R.O.C.,. pp. 385-390. ISBN 978-9-860-46303-3.

[141] SMITH, R. (2002). *Authentication*. Boston: Addison-Wesley. 549 s. ISBN 02-016-1599-1.

[142] SNEDECOR, G. W., COCHRAN, W. G. (1989). *Statistical Methods.* Eighth Edition. Iowa State University Press, 1989. ISBN 978-0-8138-1561-9.

[143] SOLEIMANI, A., ARAABI, B. N., FOULADI, K. (2016). Deep multitask metric learning for offline signature verification. *Pattern Recognition Letters, 80*, p. 84–90

[144] STANFORD UNIVERSITY. (2016). *Two-Step Authentication*. [online]. Stanford, California. [cit. 18. 11. 2016]. URL: https://itservices.stanford.edu/service/webauth/twostep

[145] STIGLER, S. M. (1989). Francis Galton's account of the invention of correlation. Statistical Science. *Statistical Science*, 4 (2), 73–79. doi: 10.1214/ss/1177012580. JSTOR 2245329

[146] STRAUS, J., JONÁK, J. (2006). Je možné identifikovat osobu podle pohybového projevu lokomoce?. In: *Identifikace a reflexe rizik společenské praxe jako teoretický základ pro rozvoj policejních služeb*: Sborník. II. díl. - Praha: Policejní akademie České republiky, 2006. - S. 301-314.

[147] STRAUS, J., JONÁK, J., AKADÉMIA POLICAJNÉHO ZBORU SR. (2008). *Využití záznamů z bezpečnostních kamer ve forenzní praxi.* Vydaní: 1. Vydavatel: Tribun EU. Brno.

[148] STRAUS, J., KLOUBEK, M. 2010. *Kriminalistická odorologie*. Plzeň: Aleš Čeněk. ISBN: 9788073802387

[149] STROGATZ, S. H. (2001). *Nonlinear dynamics and chaos: with applications to physics, biology and chemistry*. 512 pages Perseus publishing. ISBN-10: 0738204536, ISBN-13: 978-0738204536

[150] THEOHARIS, T., PASSALIS, G., TODERICI, G., KAKADIARIS, I. A. (2008). Unified 3D face and ear recognition using wavelets on geometry images. *Pattern Recognition*, *41*(3), 796-804.

[151] TRESNER, M., SALYKIN, A. (2016). Fraud Detection in AI era [online]. *Digital Economy World.* Ročník 2, červen 2016. ISSN 2464-5303. [cit 27. 01. 2017]. URL: http://deworld.cz/wp-content/uploads/2016/07/Vydani-casopisu-Digital-Economy-World-03-2016-1.pdf

[152] TREVISAN, M.A., EGUIA, M.C., MINDLIN, G.B. (2005). Topological voiceprints for speaker identification. *Physica D: Nonlinear Phenomena*, 200(1), pp.75-80

[153] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. (2018). *Upozornění na změnu v posuzování systémů využívajících biometrické údaje (dříve "Stanovisko č. 1/2017 - Biometrická identifikace nebo autentizace zaměstnanců")*. [online]. [cit. 23. 08. 2018]. URL: https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048/p1=1099

[154] ÚSTAVNÍ SOUD ČESKÉ REPUBLIKY. (2016). *Pachové stopy jako nepřímý důkaz v trestním řízení.* [online]. Česká republika, NÁLEZ Ústavního soudu. IV.ÚS 1098/15 ze dne 22. 3. 2016, N 47/80 SbNU 573. [cit. 21. 08. 2018]. URL: http://nalus.usoud.cz/Search/GetText.aspx?sz=4-1098-15

[155] VENKATARAMANI, S., RANJAN, A., BANERJEE, S., DAS, D., AVANCHA, S., JAGANNATHAN, A., DURG, A., NAGARAJ, D., KAUL, B., DUBEY, P. AND RAGHUNATHAN, A. (2017). Scaledeep: A scalable compute architecture for learning and evaluating deep networks. In *ACM SIGARCH Computer Architecture News* (Vol. 45, No. 2, p. 13-26). ACM.

[156] VENKATESH, V., MORRIS, M., DAVIS, G., DAVIS, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425-478. doi:10.2307/30036540

[157] WALL STREET JOURNAL. (2017). iPhone X Review: Testing (and Tricking) FaceID. [online]. *Youtube*, Published on Nov 2, 2017. [cit. 22. 08. 2018]. URL: https://www.youtube.com/watch?v=FhbMLmsCax0

[158] WANG, S.-L., LIEW, A. W.-C. (2012). Physiological and behavioral lip biometrics: A comprehensive study of their discriminative power. *Pattern Recognition, 45* (9), 3328–3335

[159] WAYMAN, J., JAIN, A., MALTONI, D., MAIO, D. (2005). *Biometric systems technology, design and performance evaluation*. Springer-Verlag London limited. ISBN: 1852335963

[160] WLODARCZYK, R. (2012). Biometric Features Used for Forensic Identification of Humans. *Internal Security*, *4*(1), 125

[161] WÓJCIKIEWICZ, J. (2000*). Scientific Evidence in Judicial Proceedings*. Kraków: Institute of Forensic Research Publisher. ISBN: 8387425613

[162] Woodcock, J. et al. (1993). *Slovník výpočetní techniky: Výklad standardních pojmů pro vědu, školství a obchod*. Praha: Plus. 421 s. ISBN 80-85297-48-5

[163] WRIGHT, J. YANG, A. Y. GANESH, A. SASTRY, S. S., MA, Y. (2009). Robust Face Recognition via Sparse Representation, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 2, pp. 210-227, Feb. 2009. ISSN: 0162-8828, doi: 10.1109/TPAMI.2008.79

[164] WU, K.-S., LEE, J.-C., LO, T.-M., CHANG, K.-C., CHANG, C.-P. (2013). A secure palm vein recognition system. *Journal of Systems and Software, 86* (11), 2870–2876

[165] XU, J., ZHU, W.T., FENG, D.G., (2009). An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces*, *31*(4), pp.723-728

[166] ZHAO, X., FENG, T., SHI, W., KAKADIARIS, I. A. (2014). Mobile user authentication using statistical touch dynamics images. *IEEE Transactions on Information Forensics and Security*, (Volume:9 , Issue: 11), 1780-1789. ISSN:1556-6013

[167] ZHENG, N., PALOSKI A., WANG H. (2011). *An efficient user verification system via mouse movements*. In Proceedings of the 18th ACM conference on computer and communications security, 139–150. ACM

[168] ZHU, L., YANG, Q. (2012). Speaker recognition system based on weighted feature parameter. *Physics Procedia, 25*, p.1515–1522

**Zákony, nariadenia a normy:**

[169] ČSN ISO/IEC 2382-1 Informační technologie – Slovník. Část 1: Základní termíny.

[170] ČSN ISO/IEC 2382-16, Informační technologie – Slovník. Část 16

[171] ČSN ISO/IEC TR 13335 1 – 4 Informační technologie – Směrnice pro řízení bezpečnosti IT

[172] GDPR. Nariadenie Európskeho parlamentu a Rady č. 2016/679 zo dňa 27. 04. 2016 ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46/ES, ktoré je označované ako General Data Protection Regulation (GDPR).

[173] ISO 19005-1. (2005). Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1). ISO 19005-1:2005/Cor 1:2007. ISO 19005-1:2005/Cor 2:2011

[174] ISO 19005-2. (2011). Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)

[175] ISO 19092 Financial services -- Biometrics -- Security framework

[176] ISO 32000-1. (2008). Document management -- Portable document format -- Part 1: PDF 1.7

[177] ISO/IEC 18000 Information technology -- Radio frequency identification for item management. From part 1 to 64.

[178] ISO/IEC 19785-2 Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority

[179] ISO/IEC 19785-4 Information technology -- Common Biometric Exchange Formats Framework -- Part 4: Security block format specifications

[180] ISO/IEC 19792 Information technology -- Security techniques -- Security evaluation of biometrics

[181] ISO/IEC 19794-1 Information technology – Biometric data interchange formats – Part 1: Framework

[182] ISO/IEC 19794-10 Information technology -- Biometric data interchange formats -- Part 10: Hand geometry silhouette data

[183] ISO/IEC 19794-11 Information technology -- Biometric data interchange formats -- Part 11: Signature/sign processed dynamic data

[184] ISO/IEC 19794-11: 2014 Biometric data interchange formats - Part 11: Signature/sign processed dynamic data). Českou verziou medzinárodnej normy je ČSN ISO/IEC 19794-11 (369860) Informační technologie - Formáty výměny biometrických dat - Část 11: Zpracovaná dynamická data podpisu/značky. Katalogové číslo: 95083.

[185] ISO/IEC 19794-14 Information technology -- Biometric data interchange formats -- Part 14: DNA data

[186] ISO/IEC 19794-2 Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data

[187] ISO/IEC 19794-3 Information technology -- Biometric data interchange formats -- Part 3: Finger pattern spectral data

[188] ISO/IEC 19794-4 Information technology -- Biometric data interchange formats -- Part 4: Finger image data

[189] ISO/IEC 19794-5 Information technology -- Biometric data interchange formats -- Part 5: Face image data

[190] ISO/IEC 19794-6 Information technology -- Biometric data interchange formats -- Part 6: Iris image data

[191] ISO/IEC 19794-7 Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data

[192] ISO/IEC 19794-7: 2015 Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data. Českou verziou medzinárodnej normy je ČSN ISO/IEC 19794-7 (369860), Informační technologie - Formáty výměny biometrických dat - Část 7: Data časových řad podpisu/značky. Katalogové číslo: 98678.

[193] ISO/IEC 19794-8 Information technology -- Biometric data interchange formats -- Part 8: Finger pattern skeletal data

[194] ISO/IEC 19794-9 Information technology -- Biometric data interchange formats -- Part 9: Vascular image data

[195] ISO/IEC 19795-1 Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework

[196] ISO/IEC 19795-2 Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation

[197] ISO/IEC 19795-4 Information technology -- Biometric performance testing and reporting -- Part 4: Interoperability performance testing

[198] ISO/IEC 19795-7 Information technology -- Biometric performance testing and reporting -- Part 7: Testing of on-card biometric comparison algorithms

[199] ISO/IEC 20248. (2018). Information technology -- Automatic identification and data capture techniques -- Data structures -- Digital signature meta structure.

[200] ISO/IEC 2382-37 Information technology –Vocabulary - Part 37: Biometrics

[201] ISO/IEC 24745 Information technology -- Security techniques -- Biometric information protection

[202] ISO/IEC 24761 Information technology -- Security techniques -- Authentication context for biometrics

[203] ISO/IEC 27000 :2016 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Českou verziou medzinárodnej normy je ČSN ISO/IEC 27000 (369790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

[204] ISO/IEC 29167. (2014). Information technology -- Automatic identification and data capture techniques.

[205] ISO/IEC 29167-10. (2017). Information technology -- Automatic identification and data capture techniques.

[206] ISO/IEC 7816-11 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods

[207] ISO/IEC JTC 1/SC 31. (1996). Automatic identification and data capture techniques.

[208] ISO/IEC TR 19795-3 Information technology -- Biometric performance testing and reporting -- Part 3: Modality-specific testing

[209] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 zo dňa 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

[210] P CEN/TS 16428 Biometrics Interoperability profiles - Best Practices for slap tenprint captures

[211] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV

[212] Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy

[213] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[214] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

[215] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

[216] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů*.

[217] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

[218] Zákon č. 305/2013 Z. z. Zákon o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

[219] Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

[220] Zákon č. 91/2016 Z. z. Zákon o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov

[221] Zákon. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů

[222] Zákon. č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

# Zoznam obrázkov

# Zoznam tabuliek

# Zoznam príloh

**Príloha I:** prehlásenia

Prehlásenie spoluautorov k prínosom požitých článkov.

**Príloha II:** výpočty analýzy technologického aspektu.

**Príloha III:** výpočty analýzy technologicko-používateľského aspektu (polohy tela)

**Príloha IV:** tabuľka výsledkov miery zhôd podpisov pri falšovaní

**Príloha V:** odborný životopis

Odborný životopis Ing. et Ing. Františka Hortaiho.

**Príloha VI:** zoznam všetkých publikácií

**Príloha VII:** elektronické médium pre elektronické prílohy

Elektronické médium a odkaz pre údaje a vysvetlenie hierarchie údajov.

**Príloha I: prehlásenia**

**A.** Vypracovanie časti *technologického aspektu* v kapitole *5.7* bola súčasťou článku, ktorá bola publikovaná počas doktorského štúdia v roku 2017 kolektívom autorov Smejkal, V., Kodl, J., Sieger, L., Hortai, F., Tesař, P. v článku dostupný v databázy IEEE, s celím názvom:

Smejkal, V., Kodl, J., Sieger, L., Hortai, F., Tesař, P. (2017). Stability of a dynamic biometric signature created on various devices. In *Security Technology (ICCST), 2017 International Carnahan Conference on* (pp. 1-5). IEEE.

Celkovo sa na tvorbe článku zúčastnilo 5 autorov, ktorí si podiel na článku rozložili rovnakým podielom. Na autora dizertačnej práce ako spoluautora článku spadá 20% podiel. Hlavný prínos k článku autora dizertačnej práce spočíva: asistenčná pomoc pri meraní DBP, extrahovanie DBP údajov, vypracovanie aplikácie pre podporu vyhodnotenia pri porovnaní podpisových údajov, výpočet základných štatistických údajov a grafické znázornenia údajov pre výsledné vypracovanie článku.

Súhlas a podpis primárneho autora článku prof. Ing. Vladimír Smejkal, CSc. LL. M. aj v mene aj ostatných spoluautorov:

V Brne dňa: 12. 09. 2018 ……

**B.** Časti: kapitola *5.3*, kapitola *5.7.1* a kapitola *5.7* obsahujú texty z publikácie autora dizertačnej práce, ktorý je dostupný v open-access recenzovanom vedeckom časopise *EMI journal*:

HORTAI, F. (2017). Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature. *Ekonomika Management Inovace,* 2017, roč. Vol. 9, č. 2, 2017, s. 72-89. ISSN: 1804-1299.

Súhlas a podpis autora dizertačnej práce Ing. et Ing. Františka Hortaiho

V Brne dňa: 12. 09. 2018 ……

**C.** Vypracovanie v časti v kapitole *5.9 Aspekt možných rizík zneužitia DBP* bude súčasťou článku, ktorá sa očakáva na opublikovanie v zborníku z *52nd IEEE International Carnahan Conference on Security Technology* (október 2018) a je zaradení v databázy IEEE. Tento výskum bol vykonaná počas doktorského štúdia v roku 2017 s kolektívom autorov Smejkal, V., Kodl, J., Hortai, F., Tesař, P. v článku s predpokladaným názvom:

*About the Abuse Options of the Dynamic Biometric Signature*

Celkovo sa na tvorbe článku zúčastnili 4 autori, ktorí si podiel na článku rozložili rovnakým podielom. Na autora dizertačnej práce ako spoluautora článku spadá 25% podiel. Hlavný prínos k článku autora dizertačnej práce spočíva: asistenčná pomoc pri meraní DBP, extrahovanie DBP údajov, vypracovanie aplikácie pre podporu vyhodnotenia pri porovnaní podpisových údajov, výpočet štatistických údajov a grafické znázornenia údajov pre výsledné vypracovanie článku.

Súhlas a podpis primárneho autora článku prof. Ing. Vladimír Smejkal, CSc. LL. M. aj v mene aj ostatných spoluautorov:

V Brne dňa: 12. 09. 2018 ……

**Príloha II: výpočty analýzy technologického aspektu.**

## I. ÚPLNÁ TABULKA

Toto vyhodnotenie je na základe tabuľky zo súboru *" Protokol_experimentu_Olomouc-(s-1-podpisom).xlsx "*, viď elektronické prílohy.

### A. Snímače

#### 1. ANALÝZA ROZPTYLU JEDNODUCHÉ TRIEDENIE

POČET ENTIT = 8 POČET PRVKOV = 314

| | Počet | Priemer | Nestranná var. | Názov zariadenia |
|---|---|---|---|---|
| 1.Item: | 40 | 79.127 | 130.271 | ALPHA |
| 2.Item: | 39 | 75.246 | 243.985 | DELTA |
| 3.Item: | 39 | 77.767 | 214.270 | GAMMA |
| 4.Item: | 39 | 75.205 | 230.683 | OMEGANový |
| 5.Item: | 38 | 81.746 | 151.738 | OMEGAStarý |
| 6.Item: | 40 | 74.629 | 170.362 | SIGMALite |
| 7.Item: | 40 | 84.083 | 149.884 | SIGMANový |
| 8.Item: | 39 | 76.348 | 105.893 | SIGMAStarý |

#### BARTLETT-TEST ZHODY VARIANCIÍ

(*corrected test statistic*) B = 11.113 P_value = 0.13

- Zhoda všetkých rozptylov prijatá na hladine významnosti 0.01 aj na hladine významnosti 0.05

#### JEDNODUCHÉ TRIEDENIE - TEST ZHODY PRIEMEROV

F = 2.643 P_value = 0.0115

df_1 = 7 df_2 = 306

F-kvantil (0.01) = 2.698 F-kvantil (0.05) = 2.039

- Zhoda všetkých priemerov prijatá na hladine významnosti 0.01 a zamietnutá na hladine významnosti 0.05.

#### SCHEFFEHO TEST

prijatá na hladine významnosti 0.01 aj 0.05, rovnosť všetkých 28 dvojíc priemerov.

## 2. TEST PÁROVEJ ZHODY PRIEMEROV

Zhoda rozptylov bola prijatá vo všetkých 28 dvojiciach na hladine významnosti 0.01. Zhoda rozptylov bola prijatá v 25 dvojiciach na hladine významnosti 0.05. Pri zhode rozptylov bol použitý dvojstranný t-test v opačnom prípade Cochran-Cox test pre párovú zhodu priemerov.

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 130.27 | A | A | A | A | A | A | A |
| Delta | A | 243.99 | A | A | A | A | A | N |
| Gamma | A | A | 214.27 | A | A | A | A | N |
| Omega N | A | A | A | 230.68 | A | A | A | N |
| Omega S | A | A | A | A | 151.74 | A | A | A |
| Sigma L | A | A | A | A | A | 170.36 | A | A |
| Sigma N | A | A | A | A | A | A | 149.88 | A |
| Sigma S | A | N | N | N | A | A | A | 105.89 |

*NESTRANNÁ VARIANCIA - Hladina významnosti 0.05*

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 79.127 | A | A | A | A | A | A | A |
| Delta | A | 75.246 | A | A | A | A | N | A |
| Gamma | A | A | 77.767 | A | A | A | A | A |
| Omega N | A | A | A | 75.205 | A | A | N | A |
| Omega S | A | A | A | A | 81.746 | A | A | A |
| Sigma L | A | A | A | A | A | 74.629 | N | A |
| Sigma N | A | N | A | N | A | N | 84.083 | N |
| Sigma S | A | A | A | A | A | A | N | 76.348 |

*PRIEMER - Hladina významnosti 0.01*

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 79.127 | A | A | A | A | A | A | A |
| Delta | A | 75.246 | A | A | N | A | N | A |
| Gamma | A | A | 77.767 | A | A | A | N | A |
| Omega N | A | A | A | 75.205 | N | A | N | A |
| Omega S | A | N | A | N | 81.746 | N | A | N |
| Sigma L | A | A | A | A | N | 74.629 | N | A |
| Sigma N | A | N | N | N | A | N | 84.083 | N |
| Sigma S | A | A | A | A | N | A | N | 76.348 |

*PRIEMER - Hladina významnosti 0.05*

Kde: A znamená, že hypotéza o rovnosti hodnôt bola prijatá na danej hladine významnosti

N znamená, že hypotéza o rovnosti hodnôt bola zamietnutá na danej hladine významnosti

Hodnota na diagonále je príslušná hodnota

**B. Probandi**

Bol použitý Barlettov test na testovanie zhodnosti rozptylov všetkých zariadení u každého probanda. Z tabuľky je vidieť, že pri všetkých probandoch bola táto hypotéza zamietnutá na hladine významnosti 0.01 a teda aj na hladine významnosti 0.05 (lebo P-value <0.01).

Test jednoduchého triedenia preto nemožno použiť. Pri každom probandovi boli Cochran-Cox testom testované všetky dvojice zariadení s hypotézou párovej zhodnosti priemerov na hladine významnosti 0.01 a 0.05. Počet dvojíc, kde bola hypotéza rovnosti priemerov prijatá/zamietnutá je vo štvrtom stĺpci tabuľky

| Proband | P-value | Počet párových zhôd/nezhôd priemerov na hladine významnosti 0.01 a 0.05 |
|---|---|---|
| 1 | 0.0000 | 12/16 10/18 |
| 2 | 0.0000 | 11/17 7/21 |
| 3 | 0.0000 | 9/19 6/22 |
| 4 | 0.0000 | 7/21 7/21 |
| 5 | 0.0000 | 11/10 10/11 |
| 6 | 0.0000 | 14/14 11/17 |
| 7 | 0.0000 | 11/17 6/22 |
| 8 | 0.0000 | 12/16 9/19 |
| 9 | 0.0000 | 17/11 13/15 |
| 10 | 0.0000 | 15/13 9/19 |
| 11 | 0.0000 | 3/12 0/15 |
| 12 | 0.0000 | 9/19 8/20 |
| 13 | 0.0000 | 13/15 9/19 |
| 14 | 0.0000 | 20/8 19/9 |
| 15 | 0.0000 | 10/18 5/23 |
| 16 | 0.0001 | 21/7 18/10 |
| 17 | 0.0000 | 11/17 9/19 |
| 18 | 0.0000 | 9/19 7/21 |
| 19 | 0.0000 | 17/11 15/13 |
| 20 | 0.0000 | 13/15 8/20 |
| 21 | 0.0000 | 13/15 11/17 |
| 22 | 0.0000 | 15/13 11/17 |
| 23 | 0.0000 | 14/14 11/17 |
| 24 | 0.0000 | 13/15 9/19 |
| 25 | 0.0000 | 16/12 11/17 |
| 26 | 0.0000 | 14/14 11/17 |
| 27 | 0.0003 | 12/9 10/11 |
| 28 | 0.0000 | 18/10 16/12 |
| 29 | 0.0000 | 9/19 9/19 |
| 30 | 0.0000 | 11/17 10/18 |
| 31 | 0.0000 | 21/7 19/9 |
| 32 | 0.0000 | 15/13 14/14 |
| 33 | 0.0000 | 23/5 18/10 |

| | | | |
|---|---|---|---|
| 34 | 0.0011 | 21/7 | 16/12 |
| 35 | 0.0000 | 11/10 | 11/10 |
| 36 | 0.0000 | 26/2 | 24/4 |
| 37 | 0.0000 | 12/16 | 9/19 |
| 38 | 0.0000 | 14/14 | 9/19 |
| 39 | 0.0000 | 9/12 | 7/14 |
| 40 | 0.0000 | 7/21 | 7/21 |

## II . NEÚPLNÁ TABULKA (bez 1. podpisu)

Toto vyhodnotenie je na základe tabuľky zo súboru *" Protokol_experimentu_Olomouc-(bez-1-podpisu).xlsx",* viď elektronické prílohy.

### A. Snímače

### 1. ANALÝZA ROZPTYLU JEDNODUCHÉ TRIEDENIE

POČET ENTIT = 8 POČET PRVKOV = 314

| | Počet | Priemer | Nestranná var. | Názov zariadenia |
|---|---|---|---|---|
| 1.Item: | 40 | 80.3417 | 113.0188 | ALPHA |
| 2.Item: | 39 | 76.7487 | 238.2677 | DELTA |
| 3.Item: | 39 | 78.9714 | 232.0272 | GAMMA |
| 4.Item: | 39 | 76.0221 | 228.0518 | OMEGANový |
| 5.Item: | 38 | 83.0022 | 125.8436 | OMEGAStarý |
| 6.Item: | 40 | 77.0973 | 148.5743 | SIGMALite |
| 7.Item: | 40 | 85.2333 | 139.1943 | SIGMANový |
| 8.Item: | 39 | 77.1952 | 120.3379 | SIGMAStarý |

### BARTLETT-TEST ZHODY VARIANCIÍ

(*corrected test statistic*) B = 13.597 P_value = 0.0588

- Zhoda všetkých rozptylov prijatá na hladine významnosti 0.01 aj na hladine významnosti 0.05

### JEDNODUCHÉ TRIEDENIE - TEST ZHODY PRIEMEROV

F = 2.565 P_value = 0.014

df_1 = 7 df_2 = 306

F-KRITICKA (1%) = 2.67 F-KRITICKA (5%) = 2.04

- Zhoda všetkých priemerov prijatá na hladine významnosti 0.01 a zamietnutá na hladine významnosti 0.05.

**SCHEFFEHO TEST**

prijatá na hladine významnosti 0.01 aj 0.05, rovnosť všetkých 28 dvojíc priemerov.

**2. TEST PÁROVEJ ZHODY PRIEMEROV**

Zhoda rozptylov bola prijatá vo všetkých 28 dvojiciach na hladine významnosti 0.01. Zhoda rozptylov bola prijatá v 23 dvojiciach na hladine významnosti 0.05. Pri zhode rozptylov bol použitý dvojstranný t-test v opačnom prípade Cochran-Cox test pre párovú zhodu priemerov.

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 113.02 | N | N | N | A | A | A | A |
| Delta | N | 238.27 | A | A | A | A | A | N |
| Gamma | N | A | 232.03 | A | A | A | A | N |
| Omega N | N | A | A | 228.06 | A | A | A | A |
| Omega S | A | A | A | A | 125.84 | A | A | A |
| Sigma L | A | A | A | A | A | 148.57 | A | A |
| Sigma N | A | A | A | A | A | A | 139.19 | A |
| Sigma S | A | N | N | A | A | A | A | 120.34 |

*NESTRANNÁ VARIANCIA - Hladina významnosti 0.05*

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 80.3417 | A | A | A | A | A | A | A |
| Delta | A | 76.7487 | A | A | A | A | N | A |
| Gamma | A | A | 78.9714 | A | A | A | A | A |
| Omega N | A | A | A | 76.0221 | A | A | N | A |
| Omega S | A | A | A | A | 83.0022 | A | A | A |
| Sigma L | A | A | A | A | A | 77.0973 | N | A |
| Sigma N | A | N | A | N | A | N | 85.2333 | N |
| Sigma S | A | A | A | A | A | A | N | 77.1952 |

*PRIEMER - Hladina významnosti 0.01*

| | Alpha | Delta | Gamma | Omega N | Omega S | Sigma L | Sigma N | Sigma S |
|---|---|---|---|---|---|---|---|---|
| Alpha | 80.3417 | A | A | A | A | A | A | A |
| Delta | A | 76.7487 | A | A | N | A | N | A |
| Gamma | A | A | 78.9714 | A | A | A | N | A |
| Omega N | A | A | A | 76.0221 | N | A | N | A |
| Omega S | A | N | A | N | 83.0022 | N | A | N |
| Sigma L | A | A | A | A | N | 77.0973 | N | A |
| Sigma N | A | N | N | N | A | N | 85.2333 | N |
| Sigma S | A | A | A | A | N | A | N | 77.1952 |

*PRIEMER - Hladina významnosti 0.05*

Kde: A znamená, že hypotéza o rovnosti hodnôt bola prijatá na danej hladine významnosti; N znamená, že hypotéza o rovnosti hodnôt bola zamietnutá na danej hladine významnosti; Hodnota na diagonále je príslušná hodnota

**B. Probandi**

Bol použitý Barlettov test na testovanie zhodnosti rozptylov všetkých zariadení u každého probanda. Z tabuľky je vidieť, že pri všetkých probandoch bola táto hypotéza zamietnutá na hladine významnosti 0.01 a teda aj na hladine významnosti 0.05 (lebo P-value <0.01).

Test jednoduchého triedenia preto nemožno použiť. Pri každom probandovi boli Cochran-Cox testom testované všetky dvojice zariadení s hypotézou párovej zhodnosti priemerov na hladine významnosti 0.01 a 0.05. Počet dvojíc, kde bola hypotéza rovnosti priemerov prijatá/zamietnutá je vo štvrtom stĺpci tabuľky

| Proband | P-value | Počet párových zhôd/nezhôd priemerov na hladine významnosti 0.01 a 0.05 | |
|---|---|---|---|
| 01 | 0.0000 | 13/15 | 11/17 |
| 02 | 0.0000 | 11/17 | 7/21 |
| 03 | 0.0000 | 9/19 | 6/22 |
| 04 | 0.0000 | 7/21 | 7/21 |
| 05 | 0.0000 | 11/10 | 10/11 |
| 06 | 0.0000 | 12/16 | 9/19 |
| 07 | 0.0000 | 14/14 | 9/19 |
| 08 | 0.0000 | 20/8 | 17/11 |
| 09 | 0.0000 | 14/14 | 10/18 |
| 10 | 0.0000 | 19/9 | 14/14 |
| 11 | 0.0000 | 3/12 | 0/15 |
| 12 | 0.0000 | 7/21 | 6/22 |
| 13 | 0.0000 | 13/15 | 9/19 |
| 14 | 0.0000 | 13/15 | 11/17 |
| 15 | 0.0000 | 12/16 | 7/21 |
| 16 | 0.0049 | 21/7 | 18/10 |
| 17 | 0.0000 | 12/16 | 10/18 |
| 18 | 0.0000 | 11/17 | 9/19 |
| 19 | 0.0000 | 14/14 | 10/18 |
| 20 | 0.0000 | 9/19 | 7/21 |
| 21 | 0.0000 | 14/14 | 12/16 |
| 22 | 0.0000 | 14/14 | 10/18 |
| 23 | 0.0000 | 19/9 | 15/13 |
| 24 | 0.0000 | 16/12 | 13/15 |
| 25 | 0.0000 | 18/10 | 13/15 |
| 26 | 0.0000 | 17/11 | 11/17 |
| 27 | 0.0003 | 10/11 | 7/14 |
| 28 | 0.0000 | 13/15 | 11/17 |
| 29 | 0.0000 | 8/20 | 7/21 |
| 30 | 0.0000 | 12/16 | 10/18 |
| 31 | 0.0000 | 19/9 | 15/13 |
| 32 | 0.0000 | 18/10 | 15/13 |
| 33 | 0.0000 | 21/7 | 16/12 |

| | | | |
|---|---|---|---|
| 34 | 0.0002 | 20/8 | 16/12 |
| 35 | 0.0000 | 12/9 | 10/11 |
| 36 | 0.0000 | 18/10 | 17/11 |
| 37 | 0.0000 | 9/19 | 6/22 |
| 38 | 0.0000 | 12/16 | 10/18 |
| 39 | 0.0000 | 9/12 | 6/15 |
| 40 | 0.0000 | 6/22 | 5/23 |

**Príloha III: výpočty analýzy technologicko-používateľského aspektu (polohy tela)**

Toto vyhodnotenie je na základe tabuľky zo súboru *"Protokol_experimentu_Brno.xlsx"*, viď elektronické prílohy.

**A. Všetky pozície (P1 až P5)**

POČET ENTIT = 5 POČET PRVKOV = 315

| Pozícia | Počet | Priemer | Nestranná var. |
|---|---|---|---|
| P1 | 63 | 77.8570 | 245.068 |
| P2 | 63 | 76.1901 | 230.136 |
| P3 | 63 | 65.2787 | 253.235 |
| P4 | 63 | 76.7725 | 196.204 |
| P5 | 63 | 75.7213 | 276.142 |

**1. ANALÝZA ROZPTYLU JEDNODUCHÉ TRIEDENIE**

**BARTLETT-TEST ZHODY VARIANCIÍ**

(*corrected test statistic*) B = 1.9633 P_value = 0.7425

- Zhoda všetkých rozptylov prijatá na hladine významnosti 0.01 aj na hladine významnosti 0.05

**(ANOVA) JEDNODUCHÉ TRIEDENIE - TEST ZHODY PRIEMEROV**

F = 6.9335 P_value = 0.000023

df_1 = 4 df_2 = 310 (df – počet voľností)

F- KRITICKA (0.01) = 2.401 F- KRITICKA (0.05) = 3.3802

*F > F krit.(0.01) > F krit.(0.05)* *P_value < 0.0001*

- Zhoda všetkých priemerov je zamietnutá na hladine významnosti 0.01 a aj na hladine významnosti 0.05. Priemery sú štatisticky významne rozdielne.

**2 TEST PÁROVEJ ZHODY ROZPTYLOV**

Pre párové testovanie zhody rozptylu bol použitý F-test. Rovnosť rozptylov všetkých 10 dvojíc (kombináciami pozícií P1, P2, P3, P4 a P5) sú prijaté na hladine významnosti 0.01 aj 0.05 (P-value > 0.05 > 0.01).

| F-test pre testovanie zhody rozptylu, P-value | | | | | |
|---|---|---|---|---|---|
| vs. | *P1* | *P2* | *P3* | *P4* | *P5* |
| *P1* | | 0.805299 | 0.897731 | 0.383692 | 0.639817 |
| *P2* | | | 0.707679 | 0.531865 | 0.475155 |
| *P3* | | | | 0.317702 | 0.734226 |
| *P4* | | | | | 0.181264 |
| *P5* | | | | | |

## 3 TESTY PÁROVÝCH ZHÔD PRIEMEROV

### SCHEFFEHO TEST

Tabuľka výpočtov pre Scheffého metódu mnohonásobného porovnávania.

| Párovanie | TT-statistic | p-value | Záver |
|---|---|---|---|
| P1 vs. P2 | 0.6038 | 0.9851964 | insignificant |
| P1 vs. P3 | 4.5555 | 0.0004661 | ** p<0.01 |
| P1 vs. P4 | 0.3929 | 0.9971547 | insignificant |
| P1 vs. P5 | 0.7738 | 0.9630557 | insignificant |
| P2 vs. P3 | 3.9516 | 0.0041474 | ** p<0.01 |
| P2 vs. P4 | 0.211 | 0.9997545 | insignificant |
| P2 vs. P5 | 0.1699 | 0.9998961 | insignificant |
| P3 vs. P4 | 4.1626 | 0.0020083 | ** p<0.01 |
| P3 vs. P5 | 3.7817 | 0.0072121 | ** p<0.01 |
| P4 vs. P5 | 0.3809 | 0.9974778 | insignificant |

Rovnosť dvojíc kombináciami P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05. V prípade dvojíc s P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05 (viď červeným v tabuľke vyššie).

### TUKEYHO HSD TEST

Tabuľka výpočtov pre Tukeyho metódu mnohonásobného porovnávania.

| Párovanie | Tukey HSD Q statistic | Tukey HSD p-value | Tukey HSD Záver |
|---|---|---|---|
| P1 vs P2 | 0.854 | 0.9851964 | insignificant |
| P1 vs P3 | 6.4424 | 0.0004661 | ** p<0.01 |
| P1 vs P4 | 0.5556 | 0.9971547 | insignificant |
| P1 vs P5 | 1.0943 | 0.9630557 | insignificant |
| P2 vs P3 | 5.5885 | 0.0041474 | ** p<0.01 |
| P2 vs P4 | 0.2984 | 0.9997545 | insignificant |
| P2 vs P5 | 0.2403 | 0.9998961 | insignificant |
| P3 vs P4 | 5.8868 | 0.0020083 | ** p<0.01 |
| P3 vs P5 | 5.3481 | 0.0072121 | ** p<0.01 |
| P4 vs P5 | 0.5387 | 0.9974778 | insignificant |

Rovnosť dvojíc kombináciami P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05. V prípade dvojíc s P3 sa rovnosť zamieta na hladine významnosti 0.01.

### T-TEST PÁROVEJ ZHODY PRIEMEROV (ŠTUDENTOV TEST)

Dvojvýberový t-test sa použil pri predpoklade rovnosti rozptylov. Z testu vyplýva rovnosť dvojíc kombináciami P1, P2, P4, P5 sú prijaté na hladine významnosti 0.01 aj 0.05. V prípade dvojíc s P3 sa rovnosť zamieta na hladine významnosti 0.01 aj 0.05 (viď červeným v tabuľke nižšie).

| Študentov T-test pre testovanie zhody priemerov, P-value | | | | | |
|---|---|---|---|---|---|
| vs. | *P1* | *P2* | *P3* | *P4* | *P5* |
| *P1* | | 0.351 | 0.000 | 0.543 | 0.274 |
| *P2* | | | 0.000 | 0.712 | 0.806 |
| *P3* | | | | 0.000 | 0.000 |
| *P4* | | | | | 0.538 |
| *P5* | | | | | |

**B. Pre pozície vynechaním P3**

POČET ENTIT = 4 POČET PRVKOV = 252

| Pozícia | Počet | Priemer | Nestranná var. |
|---|---|---|---|
| P1 | 63 | 77.8570 | 245.068 |
| P2 | 63 | 76.1901 | 230.136 |
| P4 | 63 | 76.7725 | 196.204 |
| P5 | 63 | 75.7213 | 276.142 |

### 1. ANALÝZA ROZPTYLU JEDNODUCHÉ TRIEDENIE

### BARTLETT-TEST ZHODY VARIANCIÍ

(*corrected test statistic*) B = 1.8516 P_value = 0.6038

- Zhoda všetkých rozptylov prijatá na hladine významnosti 0.01 aj na hladine významnosti 0.05

### (ANOVA) JEDNODUCHÉ TRIEDENIE - TEST ZHODY PRIEMEROV

F = 0.2256 P_value = 0.87855

df_1 = 3 df_2 = 248 (df – počet voľností)

F- KRITICKA (0.01) = 3.862 F- KRITICKA (0.05) = 2.641

*F < F krit.(0.01) < F krit.(0.05)* *P_value > 0.05*

- Zhoda všetkých priemerov je prijatá na hladine významnosti 0.01 a aj na hladine významnosti 0.05. Priemery pozícií P1, P2, P4 a P5 sú štatisticky zhodné.

**Príloha IV: tabuľka výsledkov miery zhôd podpisov pri falšovaní**

Toto vyhodnotenie je na základe tabuľky zo súboru *" Protokol_experimentu-VSE_(23-11-2017).xlsx"*, viď elektronické prílohy.

| *Data Index* | Zhoda podpisu A (For.) [%] | Počet pokusov podpisu A | Zhoda podpisu B (Ehl.) [%] | Počet pokusov podpisu B |
|---|---|---|---|---|
| *1* | **24** | 4 | **5** | 3 |
| *2* | **18** | 30 | **0** | 2 |
| *3* | **24** | 40 | **2** | 38 |
| *4* | **75** | 10 | **7** | 10 |
| *5* | **45** | 16 | **28** | 10 |
| *6* | **4** | 6 | **2** | 13 |
| *7* | **61** | 47 | **19** | 20 |
| *8* | **60** | 17 | **24** | 47 |
| *9* | **10** | 32 | **22** | 50 |
| *10* | **35** | 15 | **20** | 10 |
| *11* | **3** | 20 | **11** | 30 |
| *12* | **16** | 1 | **28** | 20 |
| *13* | **59** | 43 | **20** | 13 |
| *14* | **21** | 10 | **21** | 10 |
| *15* | **4** | 22 | **2** | 9 |
| *16* | **14** | 17 | **0** | 17 |
| *17* | **85** | 26 | **7** | 8 |
| *18* | **43** | 11 | **14** | 11 |
| *19* | **61** | 35 | **10** | 20 |
| *20* | **62** | 15 | **6** | 3 |
| *21* | **82** | 150 | **0** | 20 |
| *22* | **57** | 18 | **4** | 6 |
| *23* | **21** | 15 | **11** | 26 |
| *24* | **58** | 10 | **60** | 7 |
| *25* | **74** | 20 | **30** | 12 |
| *26* | **74** | 12 | **45** | 10 |
| *27* | **45** | 20 | **5** | 100 |
| *28* | **38** | 253 | **0** | 157 |
| *29* | **75** | 30 | **59** | 50 |
| *30* | **28** | 10 | **4** | 4 |
| *31* | **76** | 10 | **3** | 13 |
| *32* | **59** | 7 | **74** | 9 |
| *33* | **28** | 6 | **0** | 9 |
| *34* | **75** | 20 | **65** | 10 |
| *35* | **60** | 16 | **0** | 4 |
| *36* | **45** | 8 | **7** | 7 |
| *37* | **32** | 10 | **5** | 4 |
| *38* | **1** | 15 | **21** | 5 |
| *39* | **73** | 5 | **0** | 5 |
| *40* | **11** | 4 | **26** | 4 |
| *41* | **19** | 15 | **0** | 5 |
| *42* | **19** | 15 | **59** | 15 |
| *43* | **7** | 40 | **4** | 20 |
| *44* | **12** | 8 | **0** | 25 |
| *45* | **-** | - | **4** | 1 |
| *46* | **16** | 5 | **-** | - |
| *47* | **74** | 65 | **-** | - |
| *48* | **64** | 78 | **-** | - |
| *Počet* | **47** | **47** | **45** | **45** |

**B. časť pre testovanie hypotéz**

**1. Zhoda rozptylov**

BARTLETT-TEST: P-value = 0.0741 (prijatá zhoda rozptylov na hladine výz. 0.05 aj 0.01)

P(F<=f) obojstranná = 0.07448 (prijatá zhoda rozptylov na hladine výz. 0.05 aj 0.01)

P(F<=f) jednostranná =0.03724 (zamieta sa na hladine výz. 0.05 a prijatá na 0.01)

**2. Zhoda priemerov**

Dvojvýberový t-test pri predpoklade rovnosti rozptylov.

| | ***Zhoda podpisu A*** | ***Zhoda podpisu B*** | | |
|---|---|---|---|---|
| *Priemer* | 41.43 *[%]* | 16.31 *[%]* | | |
| *Rozptyl* | 680.16 | 396.45 | | |
| *Počet pozorovaní* | 47 | 45 | | |
| *Spoločný rozptyl* | 541.457 | | | |
| *Hypotetický rozdiel priemerov* | 0 | | | |
| *df - stupeň voľností* | 90 | | | |
| *t stat* | 5.174906 | | | |
| | **alfa =** | **0.05** | **alfa =** | **0.01** |
| *P(T<=t) jednostranná* | 0.000001 | | 0.000001 | |
| ***t** krit. jednostranná* | 1.661961 | | 2.368497 | |
| *P(T<=t) obojstranná* | 0.000001 | | 0.000001 | |
| ***t** krit. obojstranná* | 1.986675 | | 2.631565 | |

Hodnota testovacieho kritéria $t_{stat}$ je v oboch prípadoch porovnávaná s kritickou hodnotou $t_{krit.}$. Pri použitom t-teste nezávisle na hladine významnosti $\alpha = 0{,}05$ alebo 0,01 a nezávisle od toho, či sa jedná o jednostrannú alebo obojstrannú alternatívu je $\boldsymbol{t_{stat} > t_{krit}}$ . Preto hypotéza o rovnosti stredných hodnôt sa zamieta na hladine významnosti 0,05 aj na 0,01. Pravdepodobnosť chyby pri zamietnutí testovanej hypotézy je takmer nulová ( > 0,0001 %).

**Príloha V: odborný životopis**


*Titul, meno a priezvisko*: Ing. et Ing., František Hortai

*Dátum a miesto narodenia:* 21.02.1990, Nové Zámky

*E-mail:* hortai.frantisek@gmail.com

*Tel.:* SK: +421 910 269 333

CZ: +420 721 231 342


**Vzdelanie:**

*Od roku 2014* Vysoké učení technické v Brně, Fakulta podnikatelská - Řízení a ekonomika podniku (doktorské studium)

*2012 - 2015* Vysoké učení technické v Brně, Fakulta podnikatelská - Podnikové finance a obchod (magisterské studium)

*2012 - 2014* Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií - Kybernetika, automatizace a měření (magisterské studium)

*2009 - 2012* Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií - Automatizační a měřicí technika (bakalářské studium)

*2005 - 2009* Stredná priemyselná škola elektrotechnická S. A. Jedlika v Nových Zámkoch (ukončené maturitnou)

**Relevantné pracovné skúsenosti:**

*Od roku 2016* Ústav soudního inženýrství VUT v Brně, lektor předmětu: Operační a systémová analýza

*Od roku 2014* Fakulta podnikatelská VUT v Brně, Ústav informatiky - Prezenční doktorand a ostatní pedagogické práce. Vyučované předměty: Teoretická informatika, Informatika pro ekonomy, Operační a systémová analýza,

*2012 - 2013* Študentská sieť - Diákhállózat (Bratislava), občianske združenie - zástupca predsedu.

*2011 - 2013* Gombasecký letný tábor – manager infraštruktúry.

*2010 - 2013* Testovacie centrum ECDL ATC SK008 Nové Zámky – asistent.

*2010 - 2012* KAFEDIK - Studentský klub Ference Kazinczyho (Brno) – predseda.

**Ďalšie skúsenosti a stáže:**

| | |
|---|---|
| *2018 febr. – apríl* | Výskumná stáž na University of Vienna, Faculty of Business, Economics and Statistics. |
| *2017 febr. – máj* | Výskumná stáž na University of Vienna, Faculty of Business, Economics and Statistics. |
| *2016 nov. - dec.* | Výskumná stáž na Pázmány Péter Catholic University, Faculty of Information Technology and Bionics. |
| *2013 august a 2010 júl* | Praktická stáž v jadrovej elektrárni MVM Paksi Atomerőmű Zrt. (Maďarsko). |
| *2011 - 2015* | 3 Erasmus and Erasmus+ Youth in Action Programme - Youthpass for Youth Exchanges accomplished. |

**Kvalifikácie:**

| | |
|---|---|
| *2016* | Certifikát o absolvování kurzu zakladů vědecké prace v Akademii věd České republiky. |
| *2011* | CCNA (CISCO Networking Academy) Network Fundamentals, Routing Protocols and Concepts, LAN Switching and Wireless, Routing Protocols. |
| *2009* | Slovenská elektrotechnická spôsobilosť §21 - Elektrotechnik. |
| *2007* | ECDL - European Computer Driving Licence. |

**Osobné spôsobilosti:**

**Materinský jazyk:** Maďarský, Slovenský

**Ďalšie jazyky**:

| | **Porozumenie** | | | | **Hovorenie** | | | | **Písanie** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Počúvanie | | Čítanie | | Ústna interakcia | | Samostatný ústny prejav | | | |
| Český jazyk | C2 | Skúsený používateľ | C2 | Skúsený používateľ | C2 | Skúsený používateľ | C1 | Skúsený používateľ | C1 | Skúsený používateľ |
| Nemecký jazyk. | B2 | Samostatný používateľ | B2 | Samostatný používateľ | B2 | Samostatný používateľ | B1 | Samostatný používateľ | A2 | Používateľ základného jazyka |
| Anglický jazyk | C1 | Skúsený používateľ | C1 | Skúsený používateľ | C1 | Samostatný používateľ | B2 | Samostatný používateľ | B2 | Samostatný používateľ |

*Sebahodnotenie, úroveň podľa Spoločného európskeho referenčného rámca (CEF) (CEF)*

**Vodičský preukaz :** Kategórie A, B (skúsený vodič**)**

**IT znalosti:**

| | |
|---|---|
| MS Office | pokročilý používateľ. |
| MS Windows | pokročilý používateľ. |
| C / C++ | pokročilé programátorské zručnosti. |
| Java | základné programátorské zručnosti. |
| Android | základné programátorské zručnosti. |
| Matlab | pokročilé programátorské zručnosti. |

**Ocenenia:**

| | |
|---|---|
| *2017* | Štipendium od Sapientia Hungariae Alapítvány a ocenenie Collegium Talentum (sponzorované projektem NTP-HOTDKR-M-16-0001, Maďarsko) |
| *2017* | Výhra projektu špeciálneho študijného štipendia od Ministry of Human Capacities (Emberi Erőforrások Minisztériuma) a Eötvös Loránd Tudományegyetem v kategórii: Študent doktorského študijného programu. |
| *2015* | X. FTDK - študentská vedecká konferencia, výhra hlavnej ceny OTP Banky Slovensko (s témou: *The Use of Artificial Intelligence on Financial Markets*) |
| *2014* | IX. FTDK druhé miesto v kategórii na študentskej vedeckej konferencii postupom na XXXII. OTDK Information Sciences Section - reprezentant (s témou: *Image processing using Android device*) |

**Výskumné projekty:**

Spoluriešiteľ projektu: *Informační a znalostní management v éře Průmyslu 4.0*. Obdobie riešenia: 01. 01. 2018 - 31. 12. 2019, registrovaného na VUT pod číslem: FP-S-18-5524

Navrhovateľ a hlavný riešiteľ juniorského projektu specifického výzkumu: *Použití expertních metod a podpora ICT při řízení rizik v podnicích*, Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-J-17-4137. Zahájenie: 01. 01. 2017, úspešné ukončenie: 31. 12. 2017.

Spoluriešiteľ projektu: *Efektivní využití ICT a kvantitativních metod pro optimalizaci podnikových procesů*, Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-S-15-2787. Zahájenie: 01. 01. 2015, úspešné ukončenie: 31. 12. 2016.

**Príloha VI: zoznam všetkých publikácií**

***2018***

HORTAI, F. A felhasználók elektronikus hitelesítése és a biometriai rendszerek korlátai. *Alma Mater*, 2018, roč. 13, č. 3, s. 37-40. ISSN: 1339-102X.

***2017***

SMEJKAL, V., KODL, J., SIEGER, L., HORTAI, F., TESAŘ, P. Stability of a dynamic biometric signature created on various devices. In *Security Technology (ICCST), 2017 International Carnahan Conference on* (pp. 1-5). IEEE.

HORTAI, F. Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature. *Ekonomika Management Inovace*, 2017, roč. Vol. 9, č. 2, 2017, s. 72-89. ISSN: 1804-1299.

SMEJKAL, V., HORTAI, F., MOLNÁROVÁ, A. Risk and legal aspects of company's cyber security. In *Workshop specifického výzkumu 2017*. Brno: 2017. s. 50-61. ISBN: 978-80-214-5598-6.

SMEJKAL, V., HORTAI, F., MOLNÁROVÁ, A. Znižovanie rizika ako nástroj zvýšenia hodnoty firmy. In *Řízení rizik procesů spojených s technickými díly.* Praha: ČVUT v Praze, Fakulta dopravní, 2017. s. 224-233. ISBN: 978-80-01-06351-4.

SMEJKAL, V., KODL, J., SIEGER, L., HORTAI, F., TESAŘ, P. Stability of a dynamic biometric signature created on various devices. In *Security Technology (ICCST), 2017 International Carnahan Conference on* (pp. 1-5). IEEE.

SMEJKAL, V.; HORTAI, F. Biometric multi-factor authentication. INTERNATIONAL SCIENTIFIC JOURNAL SECURITY&FUTURE, 2017, roč. 1, č. 2, s. 65-68. ISSN: 2535-082X.

MOLNÁROVÁ, A. HORTAI, F. Value of Image as a Part of Company's Intangible Assets. In *Proceedings of The 29th International Business Information Management Association Conference*. Vienna, Austria, 3-4 scheduled on May 2017.

HORTAI, F. *Options and benefits of authentication system via dynamic biometric signature.* International Day of Science 2017, scheduled on 25th April 2017. Conference web site: www.mvso.cz/ids2017

***2016***

HORTAI, F.; MOLNÁROVÁ, A. Identification of Company's Critical Success Factors. Case Study of Google. In *Proceedings of the 28th International Business Information Management Association Conference: Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth.* Seville, Spain: 2016. p. 1856-1867. ISBN: 978-0-9860419-8- 3.

HORTAI, F. The Gold Commodity as a Value Holder and an Investment Instrument. In *Proceedings of the 28th International Business Information Management Association Conference: Vision 2020: Innovation Management, Development Sustainability, and*

*Competitive Economic Growth.* Seville, Spain. 2016. p. 3855-3866. ISBN: 978-0-9860419-8-3.

HORTAI, F. An Automated Algorithm for Generating Neural Networks for Stock Value Prediction. In *Proceedings of The 27th International Business Information Management Association Conference*. Milan, Italy: International Business Information Management Association (IBIMA), 2016, p. 1069-1077. ISBN: 978-0-9860419-6- 9.

***2015***

HORTAI, F. Low- cost data mining application via unused smartphone devices using computer vision and relevant data security issues. In *18 Annual International Conference Enterprise and Competitive Environment Conference Proceedings.* First edition. Brno: Mendel University in Brno, 2015, p. 304-313. ISBN: 978-80-7509-342- 4.

HORTAI, F. Dynamický biometrický podpis ako efektívny nástroj pre autentizáciu. In *QUAERE 2015*. Hradec Králové: MAGNANIMITAS, 2015. s. 1344-1352. ISBN: 978-80-87952-10- 8.

HORTAI, F. Model expertného systému pre investovanie do komodity zlato použitím fuzzy logiky. In *Sborník příspěvků z mezinárodní vědecké konference MMK 2015 MEZINÁRODNÍ MASARYKOVA KONFERENCE PRO DOKTORANDY A MLADÉ VĚDECKÉ PRACOVNÍKY*. Hradec Králové: MAGNANIMITAS, 2015. s. 560-569. ISBN: 978-80-87952-12- 2.

HORTAI, F. Képfeldolgozás Android-készülékkel - Rendszámtábla-felismerés kiértékelése. XXXII. OTDK Informatika Tudományi Szekció. Szeged: Szegedi Tudományegyetem Informatikai Tanszékcsoport, 2015. s. 84-85.

***2014***

HORTAI, F. *Porovnanie faktorov autentizácie*. 2014. Workshop specického výskumu Ústavu informatiky Fakulty podnikatelské VUT v Brně.

**Zoznam publikácií v recenznom riadení:**

SMEJKAL, V. SIEGER, L. KODL, J. HORTAI, F. TESAŘ, P. About the Abuse Options of the Dynamic Biometric Signature. ICCST 2018 (IEEE International Carnahan Conference on Security Technology).

**Príloha VII: elektronické médium pre elektronické prílohy**

V prípade vytlačenej verzie viď na elektronickom médiu, v prípade online verzie viď link: https://drive.google.com/drive/folders/1dxceUZb44VrtlzBnsxne6Q8h5a2qDCWV

Priečinky a súbory sú podľa nasledujúcej hierarchie:

- *Priečinok*: 5-3 Ekonomický aspekt
  - *Súbor*: Business Case_scanservice_Shared service center.xlsx
- *Priečinok*: 5-4 spoločenský a používateľský aspekt
  - *Priečinok*: Scan-papierových
    - *Súbor*: 1-P-SK.pdf
    - *Súbor*: 2-P-SK.pdf
    - *Súbor*: 2-P-SK.pdf
  - *Priečinok*: WEB
    - *Súbor*: Odkaz-na-webový-dotazník
  - *Súbor*: Dotazník DBP (CZ).pdf
  - *Súbor*: Dotazník DBP (SK).pdf
  - *Súbor*: Survey DBS (ENG).pdf
  - *Súbor*: Sumarum-Dotazník-DBP.xlsx
  - *Priečinok*: 5-5 technologický aspekt
  - *Súbor*: Protokol_experimentu_Olomouc-(bez-1-podpisu).xlsx
  - *Súbor*: Protokol_experimentu_Olomouc-(s-1-podpisom).xlsx
- *Priečinok*: 5-6 technologicko-používateľský aspekt
  - *Súbor*: Protokol_experimentu_Brno.xlsx
- *Priečinok*: 5-7 aspekt možných rizík
  - *Súbor*: Protokol_experimentu-VSE_(23-11-2017)-HF-V5.xlsx
- *Priečinok*: Datasheet prístrojov
  - *Priečinok*: (2017-05-09) Vyzkum OLOMOUC
    - *Súbor*: Signotec Alpha Pad .JPG
    - *Súbor*: Signotec Alpha Pad zad.JPG
    - *Súbor*: Signotec Delta Pad (1).JPG
    - *Súbor*: Signotec Delta Pad (2).JPG
    - *Súbor*: Signotec Delta Pad zad.JPG
    - *Súbor*: Signotec Delta Pad.JPG
    - *Súbor*: Signotec Gamma Pad .JPG

        - *Súbor*: Signotec Gamma Pad zad.JPG
        - *Súbor*: Signotec Omega Pad revize B .JPG
        - *Súbor*: Signotec Omega Pad revize B zad.JPG
        - *Súbor*: Signotec Omega Pad revize E zad.JPG
        - *Súbor*: Signotec Omega Pad revize E.JPG
        - *Súbor*: Signotec Sigma Lite Pad revize a2 .JPG
        - *Súbor*: Signotec Sigma Lite Pad revize a2 zad.JPG
        - *Súbor*: Signotec Sigma Pad revize B .JPG
        - *Súbor*: Signotec Sigma Pad revize B zad.JPG
        - *Súbor*: Signotec Sigma Pad revize E .JPG
        - *Súbor*: Signotec Sigma Pad revize E zad.JPG
    - *Priečinok*: (2017-05-09) Vyzkum OLOMOUC
        - *Súbor*: Signature Omega Pad (1).jpg
        - *Súbor*: Signature Omega Pad (2).jpg
        - *Súbor*: Signature Omega Pad (3).jpg
        - *Súbor*: Signature Omega Pad (4).jpg
        - *Súbor*: Signature Omega Pad (5).jpg
        - *Súbor*: Signature Omega Pad (6).jpg
        - *Súbor*: Signature Omega Pad (7).jpg
        - *Súbor*: Signature Omega Pad (8).jpg
        - *Súbor*: Signature Omega Pad (9).jpg
        - *Súbor*: Signature Omega Pad (10).jpg
    - *Súbor*: Vysvetlivky-Zdroje.pdf (aj v *.docx)
        - Pre archivačné účely sú webové stránky a ich obsah uložené v komprimovaných súboroch. Viď priečinky*: signotec Alpha Pad, signotec Delta Pad, signotec Gamma Pad, signotec Omega Pad, signotec Sigma LITE, signotec Sigma Pad*