VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA PODNIKATELSKÁ

Ústav informatiky

Ing. et Ing. František Hortai

DYNAMICKÝ BIOMETRICKÝ PODPIS JAKO EFEKTIVNÍ NÁSTROJ PRO VNITROPODNIKOVOU KOMUNIKACI

DYNAMIC BIOMETRIC SIGNATURE AS AN EFFICIENT TOOL FOR INTERNAL CORPORATE COMMUNICATION

Zkrácená verze PhD Thesis

Obor: Řízení a ekonomika podniku
Školitel: prof. Ing. Vladimír Smejkal, CSc. LL. M.
Oponenti:

Datum obhajoby:

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

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

KEY WORDS
Electronic communication, identification, authentication, authorization, biometrics, dynamic biometric signature, cybersecurity

MÍSTO ULOŽENÍ PRÁCE
Vysoké učení technické v Brně
Fakulta podnikatelská
Oddělení pro vědu a výzkum
Kolejní 2906/4
612 00 Brno

Knihovna FP VUT v Brně

ISBN 80-214-
ISSN 1213-4198

OBSAH

1 ÚVOD 5

2 ZDÔVODNENIE A ZAMERANIE DIZERTAČNEJ PRÁCE 6

3 TEORETICKÉ VÝCHODISKÁ A STAV VEDECKÉHO POZNANIA 7

4 CIELE, VÝSKUMNÉ OTÁZKY A HYPOTÉZY DIZERTAČNEJ PRÁCE 8

4.1 Ciele dizertačnej práce 8

4.2 Výskumné otázky a hypotézy 8

4.2.1 V.O. 5.1 Aký je legislatívny aspekt a normy DBP? *10*

4.2.2 V.O. 5.2 Aký je aspekt operačnej analýzy DBP? *10*

4.2.3 V.O. 5.3 Aký je ekonomický aspekt DBP? *10*

4.2.4 V.O. 5.4 Aký je spoločenský a používateľský aspekt DBP? *11*

4.2.5 V.O. 5.5 Aký je technologický aspekt DBP? *12*

4.2.6 V.O. 5.6 Aký je technologicko-používateľský aspekt pri DBP? *13*

4.2.7 V.O. 5.7 Aký je aspekt možných rizík zneužitia DBP? *14*

4.3 Súhrn a syntéza primárneho výskumu 16

5 PRÍNOS PRÁCE 18

6 ZÁVER 20

ZOZNAM POUŽITEJ LITERATÚRY A ZDROJOV 21

CURRICULUM VITAE 23

ABSTRAKT 29

1 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 a efektívne 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.

Táto práca je téza výslednej dizertačnej práce a slúži ako jej skrátená verzia. Práca sa delí na logicky nadväzujúce časti podľa názvov kapitol.

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 v dizertačnej práci. *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.

Základ dizertačnej práce bola 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. 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).

Táto časť v dizertačnej práci obsahuje rozsiahlu analýzu autentizačných faktorov a technológií overovania identity subjektov.

4 CIELE, VÝSKUMNÉ OTÁZKY A HYPOTÉZY DIZERTAČNEJ PRÁCE

4.1 CIELE DIZERTAČNEJ PRÁCE

Cieľom dizertačnej práce bol 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 *4.3 Súhrn a syntéza primárneho výskumu*. Pre ostatné skúmané hypotézy a výskumné otázky viď referencie v nasledujúcej kapitole.

4.2 VÝSKUMNÉ OTÁZKY A HYPOTÉZY

Výskumné otázky sú zaostrené na význam autentizačných technológií pre použiteľnosť v praxi. 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?* 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. Celkové vypracovanie viď v príslušnej kapitole dizertačnej práce 5.1.2.
- *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. V tom prípade, keď tieto podmienky nie je možné splniť, je doporučené zabezpečiť vhodnú doplnkovú alternatívu autentizácie. Celkové vypracovanie viď v príslušnej kapitole dizertačnej práce 5.1.3.

- *V.O. 3. Sú vhodnejšie použiť statické alebo dynamické biometrie komunikáciu v podniku?* 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, 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.
- *V.O. 4. Ktorá dynamická metóda je najvhodnejšia pre komunikáciu v podniku?* Stanovili sa okolnosti pre použitie na vnútropodnikovú komunikáciu v praxi a postupne sa argumentovali jednotlivé autentizačné metódy podľa empirických podmienok. 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. Celkové vypracovanie viď v príslušnej kapitole dizertačnej práce 5.1.5.
- *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 týchto 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.

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

Je silne deskriptívna štúdia, bez formulácie hypotéz. Základ tejto časti tvorí prieskum vzťahujúcej sa legislatívy (napr. GDPR, eIDAS) a normy daných technológií (napr. ISO). Hlavným cieľom bolo podrobne zhromaždiť, pochopiť a vysvetliť danú legislatívu a normy vzťahujúce sa na problematiku technológie a používania DBP. Vypracovanie výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.3.

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

Vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.4, kde bola zodpovedaná ako aj príslušná hypotéza:

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

Z vypracovania výskumnej otázky 5.2 bola 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.

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

Vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.5.

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 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. 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). Preto bol stanovený optimálny bod zabezpečenia, do ktorého sa ešte oplatí znižovať riziko u firiem, t. j. rentabilne investovať:

$$\sum C(min.) = Možná\ strata(Náklady) + Náklady\ na\ zníženie\ rizika$$

Aplikovaním zistených znalostí bol navrhnutý vzorec pre EE_{KT} a 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.

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

DBP spadá pod problematiku kybernetickej bezpečnosti a preto je vzorec EE_{KT} 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. Podľa implementácie treba vykalkulovať aj možné úspory vyplývajúce zo zvládnutia kybernetickej bezpečnosti. Preto pri racionálnej implementácie pri DPB sa predpokladá hodnota EE_{KT} väčšia ako 1.

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

Pre primárny zdroj údajov bol zrealizovaný dotazníkový prieskum. Celkové vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.6, kde boli zodpovedané nasledujúce V.O. a hypotézy:

- *H 5.4.I: Subjektívne je kybernetická bezpečnosť dôležitá pre ľudí alebo pre spoločnosti*. Hypotéza je **prijatá**. Z odpovedí 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*. Hypotéza je **zamietnutá**. Z odpovedí dotazníka vyplýva, že iba 27 % si myslí že má znalosti o kryptografických technológiách.
- *H 5.4.III: Ľudia majú reálne znalosti o kryptografických technológiách*. Hypotéza je **zamietnutá**. Spätná väzba kontroly znalostí ohľadne tejto problematiky ukázala, že respondenti majú spochybniteľné znalosti v danej tematike.

- *H 5.4.IV: Ľudia vedia aký je rozdiel medzi elektronickým rozpoznaním vlastnoručného podpisu ako obrázka a DBP*. Hypotéza je **zamietnutá**. Z odpovedí dotazníka vyplýva, že iba 40 % si **myslí** že pozná rozdiel.
- *V.O. 5.4.1: Je potrebné oboznámiť ľudí v prípade implementácie DBP?* V prípade implementácie DBP je racionálne oboznámiť budúcich používateľov s technológiou DBP a vysvetliť im princíp funkčnosti pre zabezpečenie subjektívnej dôvery v tejto technológii.
- *V.O. 5.4.2: Po neutrálnom oboznámení je pre ľudí DBP prijateľný?* Z odpovedí dotazníkového prieskumu vyplýva, že respondenti vo všeobecnosti majú pozitívny prístup k používaniu technológie DBP.

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

Výskum kontinuálne nadväzoval na publikované príspevky, ktoré sa konkrétne vzťahujú on-line DBP (Jain et al., 2002; Smejkal, Kodl, 2011; Smejkal, Kodl, Kodl Jr., 2013; Smejkal, Kodl, 2014; Smejkal et al., 2015; Smejkal et al., 2016). 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. Indukovaný experiment sa zameriava na možnosť prípadného vplyvu na kvalitu dát a stálosť DBP pri používaní rôznych snímacích zariadení rovnakou osobou. Celkové vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.7. Nasledujúce hypotézy boli formulované a vyriešené:

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*.

Z testovaní vyplýva, že nulová hypotéza *H 5.5.I.0* sa **zamieta**, a to na hladine významnosti 0.01 a aj na hladine významnosti 0.05. 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. **Prijala** sa 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.

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 tomto prípade bola **prijatá** 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

Jednalo sa o štatisticky reprezentatívnu vzorku. 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.

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

Z poznatkov z relevantnej vedeckej literatúry sekundárneho výskumu, ďalej z publikácií zmienených v časti 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. Celkové vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.8. Nasledujúce hypotézy a výskumné otázky boli formulované a zodpovedané:

I. časť predpokladala, 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.*

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*.

II. časť bola založená pre prípad prijatia alternatívnej hypotézy I. časti, preto boli 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)?* Za predpokladu, že stabilitu podpisov na jednotlivých

pozícií odráža variancia, resp. čím väčšia stabilita, tým menšia variancia, sa pozície z pohľadu rozptylov zhodujú. Z pohľadu celkových hodnôt sú pozície, ktoré sú si prakticky ekvivalentné. Z celkových výsledkov vyplýva, že signatári síce preukázali nižšiu priemernú zhodu podpisov v prípade jednej pozície, 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. Ďalej boli zistené rozdiely pri procesu vytvárania podpisu. Špecifikovali sa tieto rozdiely, ktoré môžu byť faktorom zmeny nižšej priemernej zhody pri pozícii tela podpisu. Z výskumu vyplýva, že optimálna poloha na podpisovanie DBP, nemusí byť špecifická, ale pozícia pre používateľa musí 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?* Výskum ukázal, že faktorom vplyvu sú 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.

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

Táto časť sa zameriava na riziká falšovania DBP a použiteľnosť v praxi. 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. Počas experimentu sa signatári snažili čo najlepšie

falzifikovať rôzne podpisy. 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 (vzorové podpisy boli písané pravou rukou). Výsledná vzorka svojou veľkosťou je štatisticky dostatočne reprezentatívna na analýzu.

Z výsledkov vyplývala aj odpoveď na otázku: aká má byť stanovená požadovaná miera zhody podpisu aby bol DBP považovaný za pravý? Celkové vypracovanie a metodológiu výskumnej otázky viď v príslušnej kapitole dizertačnej práce 5.9. Nasledujúce hypotézy a výskumné otázky boli formulované a zodpovedané:

Hypotézy I. časti predpokladali, 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.*

Z výsledkov testovania hypotéz vyplýva, že signifikantná korelácia medzi mierou zhody A a B neexistuje, preto možno nulovú hypotézu *H 5.7.I.0* o zhode „talentu“ napodobňovať všetky podpisy sa dá **zamietnuť** na hladine významnosti 0.05 aj 0.01 v prospech alternatívnej hypotézy *H 5.7.I.1* (hypotéza bola **prijatá**).

Hypotézy II. časti predpokladali, 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.*

Na základe testovania hypotéz a 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* (hypotéza bola **prijatá**).

Hypotézy III. časti predpokladali, 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.*

Na základe testovania hypotéz sa nulová hypotéza *H 5.7.III.0* **zamieta** (korelácia minimálne na hladine významnosti 0.01) a **prijíma** sa alternatívna hypotéza *H 5.7.III.1*.

Bola zodpovedaná aj 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?*

Na základe výsledkov experimentu, výsledkov získaných v minulosti z primárne dostupných dôveryhodných zdrojov, analýzy rizík, bezpečnostných politík a ďalších orientačných dokumentov organizácií, bola navrhnutá signifikantná požadovaná miera zhody pri DBP. Na reprezentačnom príklade bolo ukázané, aby signifikantná

požadovaná miera zhody DBP má byť škálovateľne/kaskádovo nastavený podľa relevantnosti používania.

4.3 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:

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.

5 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 prehľad 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.

6 ZÁVER

Táto téza slúži ako skrátená verzia mojej výslednej dizertačnej práce. Samotný výskum sa delil na sekundárny a primárny výskum. Sekundárna analýza mala 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 dizertačnej práce *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.

Zvlášť kapitola slúžila na vyhodnotenie analýzy a výskumu. Boli 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.

Piata 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 ZDROJOV

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

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

JAIN. A. K., GRIESS, F. D., CONNELL, S. D. (2002). On-line signature verification. In: *Pattern Recognition* 35, p. 2963 – 2972

KOCH, M., CHVÁTALOVÁ, Z. (2017). Information Systems Efficiency Model. *Journal of Systems Integration*, *8*(3), 3-9.

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.

PARKINSON-HELP. (2018). Online. URL: https://parkinson-help.cz/parkinsonova-nemoc-pn/priznaky-motoricke/poruchy-souvisejici-s-pohybem/

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.

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.

SMEJKAL, V. (2018). *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, s.r.o., 936 p. ISBN: 9788073807207.

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. (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., 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. (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.

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

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.

Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů*.

CURRICULUM VITAE

Osobné údaje

Titul, meno a priezvisko: Ing. et Ing., František Hortai

Dátum a miesto narodenia: 21.02.1990, Nové Zámky

E-mail: hortai.frantisek@gmail.com

web: https://sites.google.com/view/hortaif

Tel.: 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)

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: Slovenský, Maďarský

Ďalšie jazyky:

Anglický jazyk – doktorská skúška. Nemecký jazyk – maturita.

Sebahodnotenie, úroveň podľa Spoločného európskeho referenčného rámca (CEF) (CEF)

	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	C1	Samostatný používateľ	C1	Samostatný používateľ

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.

ŠTRUKTÚROVANÝ PREHĽAD PUBLIKAČNEJ ČINNOSTI

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).

ABSTRAKT

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.

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.

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.