VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV EKONOMIKY
FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF ECONOMICS

BEZPEČNOST ELEKTRONICKÉHO BANKOVNICTVÍ

SECURITY OF ELECTRONIC BANKING

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. JAN PAŘIL
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN LUHAN, Ph.D.
SUPERVISOR

BRNO 2015

(zde se nachází originální zadání práce)

Abstrakt

Hlavním zaměřením diplomové práce je elektronické bankovnictví a jeho bezpečnost. Práce obsahuje zhodnocení současného stavu zabezpečení elektronického bankovnictví, možné hrozby napadení elektronického bankovnictví a rizika prolomení zabezpečení. Další část vyhodnocuje dotazník, který zjišťoval spokojenost uživatelů s bezpečností elektronického bankovnictví. Závěrem budou doporučeny nové formy zabezpečení.

Abstract

The main focus of the thesis is an electronic banking and security. The work includes evaluation the current state of security of electronic banking, the possible threats of attack on electronic banking and risks of security breaches. The next part focus on user satisfaction with e-banking security using a questionnaire. At lesast will be recommended new forms of security.

Klíčová slova

Elektronické bankovnictví, bezpečnost elektronického bankovnictví, hrozby, spokojenost uživatelů

Key words

E-banking, e-banking security, threats, user satisfaction

Bibliografická citace diplomové práce:

PAŘIL, J. *Bezpečnost elektronického bankovnictví.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 116 s. Vedoucí diplomové práce Ing. Jan Luhan, Ph.D..

Čestné prohlášení

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

V Brně dne 15. ledna 2015 ……

podpis studenta

Poděkování

Tímto bych rád poděkoval panu Ing. Janu Luhanovi, Ph.D., za cenné připomínky a odborné rady, kterými přispěl ke zdárnému vypracování mé diplomové práce. Dále bych rád poděkoval všech respondentům, kteří vyplnili dotazník. Mé poděkování patří i rodině a přátelům za podporu během studia.

Obsah

1 Úvod

Díky velkému rozvoji využívání internetu se zvyšuje i využití elektronického bankovnictví. Elektronické bankovnictví zprostředkovává komunikaci mezi klientem a bankou. Klient si tak může z pohodlí svého domova zjistit zůstatek na svém účtu, zadat platbu, nastavit trvalé příkazy, inkasa a celkově má nepřetržitý přehled a přístup ke svým financím.

V dnešní uspěchané době je elektronické bankovnictví velkou úsporou času. Uživatelé nemusí trávit svůj čas na pobočkách banky a účet si mohou založit i klienti, kteří nemají pobočku v blízkosti svého bydliště. Výhodou pro banku je, že nemusí mít tolik kamenných poboček.

V posledních letech vstoupily na trh nové banky, jejichž elektronické bankovnictví je velice moderní – přehledné, jednoduché a uživatelsky přístupné. Z toho důvodu se snaží starší banky inovovat, modernizovat a zjednodušovat svá internetová bankovnictví, a udržet tak krok s nově příchozí konkurencí. Banky svá elektronická bankovnictví neustále vylepšují, vymýšlejí různé novinky a speciální funkce, na které se snaží nalákat nové zákazníky.

Bankovní instituce investují nemalé prostředky do rozvoje elektronického bankovnictví a jeho bezpečnosti. Právě oblast bezpečnosti, a tedy i jistoty pro klienta, tvoří bankám konkurenční výhodu.

Další potřebou řešit danou situaci, jsou narůstající útoky na banky a jejich elektronická bankovnictví. Hackeři se neustále pokoušejí novými metodami prolomit zabezpečení elektronických bankovnictví. Banky se tedy snaží udržet krok s těmito hackery, v lepším případě být o krok napřed. Toto ovšem vyžaduje značné úsilí a velké finanční náklady. Proto se banky snaží hledat kompromis mezi bezpečnostní technologií a náklady na její pořízení.

Úvodem se podívám, jak danou problematiku řeší současná literatura, jaká jsou možná rizika, zabezpečovací mechanismy a vývojové trendy budoucnosti. V rámci vlastní práce zjistím, jakou ochranu nabízí banky v České republice, zhodnotím jejich způsob zabezpečení a dopad na obsluhu internetového bankovnictví. V druhé části se zaměřím na bezpečnost bankovnictví z pohledu běžných uživatelů, klientů. Vytvořím dotazník, kde se zeptám na spokojenost klientů se zabezpečením jejich internetového bankovnictví. Na základě dotazníku vyhodnotím, jaký typ zabezpečení je pro klienty nejdůležitější a zjistím jejich pohled na stav současného elektronického bankovnictví.

Z těchto získaných dat navrhnu další možné formy zabezpečení. Uvedu jejich přínosy pro banky a náklady na jejich zavedení do provozu. Podívám se, jak tyto náklady ovlivní vývoj zisku u jednotlivých bank a jaká bude návratnost této investice. Zároveň uvedu možné přínosy ve zvýšení počtu klientů, při zavedení těchto nových forem zabezpečení.

2 Cíle práce, metody a postupy zpracování

2.1 Cíl práce

Hlavním cílem diplomové práce je přehled současné situace zabezpečení elektronického bankovnictví jednotlivých bank a návrhy možného zlepšení bezpečnosti. Srovnám bezpečnost z pohledu bank a jejich klientů.

2.2 Dílčí cíle práce

Zanalyzovat současnou situaci na základě rešerše dostupných zdrojů. Zaměřit se především na možnosti zabezpečení elektronického bankovnictví.

Dále shrnout nejdůležitější minulé útoky a napadení elektronického bankovnictví a zároveň popsat i možné hrozby, které tuto oblast provázejí.

Udělat přehled stávajícího zabezpečení bankovních institucí v České republice. Zjistiti jaké využívají formy zabezpečení, jak je inovují a jak varují uživatele.

Vytvořit dotazník spokojenosti klientů se zabezpečením elektronického zabezpečení, kde se budu dotazovat na spokojenost se současným stavem, a jaké inovace by dotazovaní uvítali.

V poslední řadě navrhnout další formy zabezpečení. Udělat kalkulaci na případné náklady na zavedení nových forem zabezpečení a navrhnout, jaké to bude mít přínosy v celkovém kontextu.

2.3 Metody a postupy zpracování

Po analýze daného problému, řešeného v literatuře, provedu zhodnocení současné situace, především na českém trhu. Bezpečnost elektronického bankovnictví porovnám jak z pohledu banky, tak z pohledu klienta. Pro sběr dat od uživatelů elektronických bankovnictví provedu dotazníkové šetření elektronickou metodou.

Navrhnu použití vybraných technologií, jejichž implementace může přispět k rozvoji bezpečnosti pro tuto oblast. Dále zhodnotím náklady na pořízení těchto technologií a dobu návratnosti investice. Zobrazím vliv investice na vývoj zisku. Jedna z použitých metod bude regresní analýza. Data použiji především z veřejně přístupných zdrojů a odborných odhadů.

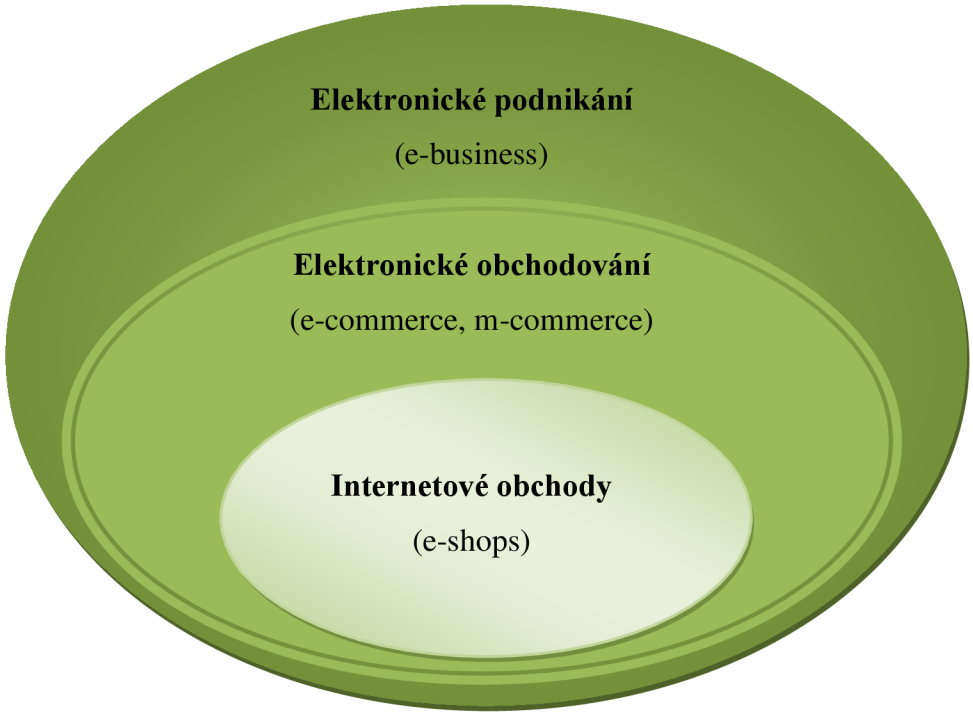
3 Teoretická východiska práce

3.1 Elektronické bankovnictví

Elektronické bankovnictví nebo-li e-banking je součástí e-commerce. Na obrázku níže uvádím rozdělení celého elektronického podnikání tzv. e- business.

E-business představuje hierarchicky nejvyšší úroveň pro podnikatelské aktivity realizované s využitím ICT. Zaměříme-li se na ryze obchodní aktivity, hovoříme o tzv. elektronickém obchodování označovaném jako e-commerce, v rámci kterého jsou jako jedny z klíčových komunikačních rozhraní internetové obchody (e-shopy) představované konkrétními webovými aplikacemi. (SUCHÁNEK, 2012)

Následující obrázek č. 1. znázorňuje hierarchické rozdělení e-business.



Obr. 1: Hierarchické rozdělení e-business, zdroj: SUCHÁNEK, 2012

S rozvojem nových technologií souvisí i rozvoj nových produktů v oblasti bankovnictví. Banky nabízejí širokou paletu produktů tzv. **přímého bankovnictví.** Jsou to služby, které umožňují komunikaci banky a klienta bez toho, aby klient musel banku

navštívit. Vše se děje buď pomocí telefonu, dnes již hlavně mobilního, resp. tzv. chytrého telefonu, nebo počítače a internetu.

Pojem elektronické bankovnictví – přímé, nebo také vzdálené, se vžil pro označení elektronické formy komunikace mezi bankami a jejich klienty. Při vyřizování svých bankovních operací nepřichází klient do osobního kontaktu s pracovníky banky, ale provádí operace ze svého terminálu nebo jiného technického zařízení, které je veřejně dostupné. Jde o trend, který jde ruku v ruce s rozvojem informačních a telekomunikačních technologií, s vyšší výkonností výpočetní techniky a snižováním ceny, za kterou je prodávána. Je to pojem, jehož aktuální obsah se vyvíjí spolu s informačními a komunikačními technologiemi. Nejlépe jej vystihuje pojem **vzdálené bankovnictví**. (CEED, 2006)

Internetové bankovnictví umožňuje jednoduše provádět bankovní operace on-line, a zaručuje tak nepřetržitý přístup do banky. Všechny svoje účty může klient obsluhovat z libovolného počítače dvacet čtyři hodin denně.

Pro využívání této služby postačí jen se přihlásit do systému banky na její webové adrese a po zadání všech hesel a elektronického klíče zadávat svoje příkazy. Každá operace musí být navíc stvrzena jedinečným klientovým podpisovým certifikátem, tj. elektronickou obdobou jeho vlastnoručního podpisu, který klient získá přímo prostřednictvím této služby. Všechna data, přenášená mezi počítačem klienta a jeho obchodní bankou, jsou šifrována. (KALABIS, 2012)

Obecně lze za platební produkty elektronického bankovnictví považovat veškeré produkty banky, při kterých je kontakt klienta s bankou nebo použití daného produktu prováděno elektronickou formou. Pro praktické účely je při vymezení platebních produktů elektronického bankovnictví možné vyjít ze zákona o platebním styku, který vymezuje dvě varianty elektronických platebních prostředků:

- **prostředek vzdáleného přístupu k peněžní hodnotě**, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem;

- **elektronický platební prostředek**, kterým je platební prostředek, jenž uchovává peněžní hodnotu v elektronické podobě a který je přijímán jako platební prostředek i jinými osobami než jeho vydavatelem. Peněžní hodnota uchovávaná na elektronickém peněžním prostředku se potom označuje jako **elektronické peníze**.

Toto rozšíření má zásadní význam. Zatímco v prvním případě se jedná pouze o nové možnosti využívání *klasických platebních prostředků,* v druhém případě jde o vznik nové formy peněz – elektronických peněz. (MÁČE, 2006)

3.1.1 Výhody a nevýhody elektronického bankovnictví

V následujících tabulkách jsou uvedeny hlavní výhody a nevýhody elektronického bankovnictví z pohledu klienta a banky.

Tab. 1: Výhody elektronického bankovnictví

Pro klienta:	Pro banku:
* Klient nemusí pro vykonávání bankovní operace fyzicky navštívit banku	* Banka může snížit množství a velikost svých poboček, a snížit tak své náklady
* Klient není omezen pracovní dobou banky	
* Klient nemusí komunikovat s bankou jen z jednoho místa	* Banka obsluhuje aplikaci internetového bankovnictví z jednoho centrálního pracoviště, čímž snižuje nároky na množství zaměstnanců
* Klient je obsloužen bez čekání a schůzek	
* Klient nemusí vyplňovat papírové formuláře a uvádět podpisový vzor	* Banka získává prostřednictvím aplikace internetového bankovnictví informace o chování klientů, a může tak lépe cílit reklamu a marketing
* Klient má informace o svých bankovních účtech a operacích neustále přístupné	

Zdroj: ŠENKÝŘOVÁ, 1998.

Hlavní výhodou pro klienta je dostupnost jeho účtu 24 hodin denně, 7 dní v týdnu. Klient si může vyřídit všechny základní operace z pohodlí domova a nemusí řešit otevírací dobu pobočky. Navíc se zákazník může přihlásit ke svému účtu z jakéhokoliv místa na světě, kde je přístup k internetu.

Z pohledu banky jsou menší náklady na pobočková místa, hlavně na četnost poboček. Na vývoj a spravování internetového bankovnictví stačí menší počet zaměstnanců, než kolik by banka musela mít poboček, aby obsloužila všechny svoje stávající klienty.

Tab. 2: Nevýhody elektronického bankovnictví

Pro klienta:	Pro banku:
* Klient musí mít potřebné technické vybavení	* Náklady na zřízení systému jsou relativně vysoké
	* Banka musí zajistit designované pracoviště a technické pracovníky
* Klient musí být počítačově gramotný	* Banka musí pravidelně investovat do vývoje a inovace systému
	* Banka musí být schopna pružně reagovat na technologické změny v oblasti
* Klient musí dbát na zabezpečení svého počítače	* Banka musí dbát na zabezpečení systému

Zdroj: ŠENKÝŘOVÁ, 1998

Jedním ze základních předpokladů klienta, který potřebuje využívat služeb elektronického bankovnictví, je možnost počítače a připojení k internetu a zároveň patřičná znalost obsluhy počítače. Dalším důležitým krokem ze strany klienta je dostatečné zabezpečení jeho počítače proti případným napadením.

Nevýhodou banky jsou vyšší náklady na vývoj, inovaci a správu systému internetového bankovnictví. Zároveň ale banka může snížit náklady na budování dalších poboček. Banka musí také investovat do zabezpečení internetového bankovnictví a musí dopředu předpokládat možné napadení jejího systému, aby těmto napadením předcházela a svého klienta co nejvíce ochránila. Dále je potřeba značných investic do

inovace a zdokonalení současných systémů a sledování moderních technologických trendů v oblasti informatiky a zabezpečovacích systémů.

3.2 Rizika elektronického bankovnictví

3.2.1 Riziko ze strany uživatele

Co dělá bankám největší starosti v oblasti narušení bezpečnosti? Klienti, přesněji jejich zabezpečené počítače. Jsou známy následující tři typy nejčastějších pokusů o narušení bezpečnosti. Jsou to počítačové viry a červi, dále útoky na systémy elektronické pošty v podobě nevyžádané pošty a spamu a také podvodné techniky k získání citlivých údajů, jako např. tzv. phishing a pharming. Ke všem těmto útokům dochází prostřednictvím počítačů klientů, kteří se tak stávají nevědomými poskytovateli citlivých informací a kanály vedoucími do nitra finančních institucí.

Přijmout zodpovědnost za bezpečnost počítačů svých klientů se bankám příliš nechce, přestože jsou finanční instituce právě těmito útoky přímo ohrožovány. Na otázku, zda by měly banky nést odpovědnost za zajištění ochrany počítačů svých klientů, kteří s nimi komunikují online, odpověděly dvě třetiny respondentů, že nikoliv. (SALMON, 2008)

Uživatel by samozřejmě měl také dbát na zabezpečení svého počítače. Nedoporučuji se připojovat do internetového bankovnictví pomocí počítačů v kavárnách a jiných veřejných místech, kde neznáme míru zabezpečení počítače a nevíme, jaké programy a viry může počítač obsahovat. Samozřejmostí by měl být pravidelně aktualizovaný počítač s aktuální verzí antivirového programu, anti-spyware program a kvalitní firewall. Důležitá je taktéž ochrana přístupových údajů a zvolení silného hesla. Heslo by mělo být kombinací čísel a písmen, v žádném případě datum narození apod. Na internetu existuje plno nástrojů, které umožní ověřit kvalitu hesla. (SEDLÁČEK, 2011)

3.2.2 Zneužití produktů přímého bankovnictví

Podvody lze obecně rozdělit do **pěti kategorií**:

- **„dobrovolné“ zaslání přihlašovacích údajů** – pod tuto metodu spadá tzv. phishing (phishingu jsme se podrobně věnovali v článku Rybičky, rybičky, rybáři jedou) a pharming (jde o jakýsi „vylepšený“ phishing, kdy se prohlížeč přesměruje na falešnou stránku i při ručním zadání);
- **„odchycení“ přihlašovacích údajů od uživatele podvodem** – trojské koně, spyware, spam;
- **„od třetích stran“** - získání hesel, PINů a dalších dat, např. o platební kartě, od subjektů, kde byly použity k úhradě (např. z obchodu);
- **„nabourání“ do systému**, tzv. hacking;
- **„rafinované útoky“** - násilné donucení, odposlechy atd. (BOUŠOVÁ, 2006)

Formy napadení elektronického bankovnictví, které se snaží zjistit přístupové údaje uživatelů internetového bankovnictví, jsou:

Pharming - jeho cílem je získat citlivé údaje bez vědomí klienta banky. Podvodník přitom využívá techniku upraveného překladu internetových adres, která přesměruje uživatele internetového bankovnictví na připravené podvodné stránky.

Phishing - pod ním se rozumí snaha o podvodné získávání citlivých údajů klienta (např. přístupových práv k internetovému bankovnictví). Jeho základem je nevyžádaný e-mail zaslaný ze zdánlivě důvěryhodného zdroje (např. z obchodní banky). Uživatel je požádán, aby zaslal svoje přístupová hesla ke službě internetového bankovnictví, nebo číslo své platební karty. Tyto informace pak podvodníkům umožní neoprávněný přístup k bankovním účtům tohoto klienta.

Smishing- je hrozba pro uživatele mobilních sítí. Jde o textovou zprávu (sms), která příjemce navede buď k zadání přístupových hesel ke svému účtu nebo platební

kartě, nebo k přihlášení do aplikace internetového bankovnictví, odkud si podvodníci sami stáhnou přihlašovací údaje.

Vishing- je další druh podvodu k získání přístupových práv do internetového bankovnictví. Podvod je zahájen telefonátem, který klienta motivuje, aby se ze svého počítače přihlásil do internetového bankovnictví. Klientův počítač ovšem sleduje hacker, který okopíruje pomocí webového formuláře klientem zadané kódy i hesla. (KALABIS, 2012)

Další pohled na možné způsoby napadení elektronického bankovnictví:

ATTACK VECTOR – (vektor útoku) metoda nebo nástroj, kterým mohou útočníci napadnout systémy. Spojení pochází původně z biologie, kde se tímto pojmem označuje jedinec přenášející infekci (bacilonosič).

BLACK HAT – (doslova černý klobouk) označuje zlého hackera, tj. takového, který hledá zranitelnost v systémech, zneužívá je a ve výsledku záměrně páchá škody. Motivy jednání mohou být různé – peníze, aktivismus, posílení vlastního ega, škodolibost aj.

BOTNET – anglické slovo vzniklé spojením slov robot a net (síť). Jde tedy o síť složenou z robotů, většinou z počítačů nakažených určitou malwarovou infekcí (nakaženým PC se pak říká zombie). V případě potřeby mohou útočníci použít kompromitované počítače ke koordinovanému útoku na vybraný cíl (třeba k útokům typu DDoS) nebo k rozesílání spamu .Provozovatel dokáže celý botnet centrálně řídit.

CRACKER – člověk, který prolamuje zabezpečení softwaru či sítí. Označení často popisuje Black Hat hackera. V druhém smyslu se tím označuje počítačový

odborník, který zbavuje proprietární software ochrany (například aby mohl daný program sám používat).

ČERVI – častý druh malwaru. Červi napadají systémy přes sítě (internet, intranet), a to bez vědomí uživatele, útočníkovi stačí využít některou známou nebo jím objevenou zranitelnost systému či určité aplikace třetí strany. Podobně jako vir je i červ s to se rozmnožit, jenomže na rozdíl od něj nenapadá další součásti systému, své kopie rozesílá pomocí komunikačních protokolů dále po síti. Červ má ve svém kódu sekundární část starající se o další činnost, například zablokování nějakého subsystému v hostitelském počítači, a může vytvořit backdoor, zadní vrátka, kterými se do systému dostává další malware.

DDoS – zkratka pro takzvané distribuované odepření služby. Velmi rozšířený typ útoků na webové servery, při němž útočníci zaplavují servery zbytečnými dotazy. Servery se pod jejich tíhou zahltí a přestanou fungovat.

HACKER – v původním a správném smyslu označení pro odborníka, kterého zajímá, jak dané systému fungují. Může jít o špičkového programátora nebo znalce sítí a bezpečnosti takových systémů. Avšak v médiích a obecně v populární kultuře se slovem hacker označuje člověk, který napadá počítače a sítě firem či států s vidinou páchání škod. Proto došlo k odlišení na WHITE HAT a BLACK HAT. Ten první s bílým kloboukem je hodný, ten s černou buřinkou zase zlý.

KEYLOGGING – označení pro odposlouchávání/zaznamenávání stisknutých kláves. Jestliže se útočníkovi podaří propašovat do systému oběti keylogger, může snadno získat hesla k různým účtům a další citlivé údaje.

MALWARE – obecné označení pro škodlivý software – řadíme sem viry, červy, trojské koně, sledovací programy (spyware) a mnohé další.

SCAREWARE – česky falešné antiviry. Zákeřný software (malware), který po instalaci nejprve postraší uživatele fiktivní existencí malwarové nákazy v systému

(trojský kůň, virus XYZ), následně mu nabídne řešení. Stačí vytáhnout platební kartu a koupit si pomoc od původce sharewaru. Často se jedná o prázdný software, který neplní žádné funkce, někdy však instaluje do systému oběti další malware (a je tedy sám původcem infekce).

SSH – komunikační protokol pro bezpečnou komunikaci a zároveň i program. Pomocí SSH lze mezi počítači vytvořit bezpečné spojení. Používá se k přístupu na vzdálený PC, k bezpečnému přenosu souborů, přeposílání portů nebo třeba pro VPN (virtuální privátní síť).

TROJSKÉ KONĚ – častý typ malwaru. Od virů a červů se trojské koně liší především tím, že se neumějí replikovat. Do systému se dostávají především společně s nějakým programem, který si uživatel nainstaluje, aniž tuší, že instalační soubor obsahuje i tento nechtěný dárek. Další cestou jsou zadní vrátka, která trojským koním otevřel červ. Trojský kůň má za úkol umožnit útočníkovi vzdálený přístup do počítače. Útočník dokáže s jeho pomocí spustit libovolný příkaz, trojský kůň může i odposlouchávat klávesnici (keylogging), udělat u počítače součást spamového boletu, sledovat chování uživatele nebo třeba odposlouchávat uživatelská hesla (tzv. sniffing, v rámci něhož dochází k získání přístupových údajů pro bankovní a jiné finanční instituce).

VIR – častý druh malwaru. Virem se označuje počítavý program, který se umí replikovat a šířit bez vědomí uživatele podobně jako biologický virus. Počítačový vir se při rozmnožování vkládá do různých spustitelných souborů a dokumentů. Mezi PC se šíří přes vyměnitelná média (např. přes flash disk) stažením infikovaného souboru nebo třeba přílohou e-mailu. (MISHA, 2013)

Konkrétní bezpečností požadavky elektronických platebních systémů se liší v závislosti na rysech jednotlivých systémů, obecně však mezi základní vlastnosti, které systémy musí vykazovat, patří důvěrnost, integrita, utajenost, autorizace, interoperabilita, dostupnost a spolehlivost. Stejně jako ve světě klasických peněz, i ve světě elektronických plateb stále existují rizika porušení důvěryhodnosti a bezpečnosti.

Cílem je realizovat takové kryptografické mechanismy a protokoly, které jsou a budou schopné tato rizika minimalizovat nebo zcela eliminovat. Uplatňované bezpečnostní politiky brání šifrováním zpráv porušování důvěrnosti odposlechem a elektronickými (digitálními) podpisy brání nepoctivým uživatelům, aby se podvodně vydávali za jiné osoby, nepoctivým obchodníkům, aby falšovali elektronické platební příkazy zákazníků. Velmi důležitým prvkem je také zajištění integrity přenášených dat. Základním předpokladem pro podporu serióznosti elektronických plateb je využívání licencovaného a optimalizovaného softwaru, který je schopen zajistit ochranu systému například proti trojským koňům (program, pomocí kterého může útočník monitorovat uživatelův počítač a zcizit např. důležité informace). (SUCHÁNEK, 2012)

Lze se proti těmto zákeřným útokům nějak bránit? Určitě ano, receptů existuje hned několik. Pravidelně aktualizujte svůj antivirový program doma i ve firmě (což většina Čechů podle ankety, kterou v srpnu prováděla společnost AVG, nedělá), kontrolujte své telefonní účty, pečlivě si pročítejte jednotlivé odkazy, na které chcete kliknout (někteří kyberzločinci sázejí na nepozornost uživatele a používají odkazy téměř shodné s legitimně existujícími stránkami, důležité je zde ovšem slovo téměř). (www.antivirovecentrum.cz 2013)

Ve svém internetovém bankovnictví nastavte nejlepší možné zabezpečení a také zaznamenávání všech operací (je-li to možné). Než si nainstalujete novou aplikaci, zjistěte si o ní a jejím původu více informací, čtěte uživatelská fóra.

Pokud objevíte neobvyklé chování svého počítače nebo telefonu, nebojte se to konzultovat s odborníky, případně to nahlásit na policii. Pokud vám totiž chce útočník „vyluxovat“ kapsu, nemusí na to vždycky jít jen přes nabourané internetové bankovnictví.

Konkrétním případem právě z Česka mohou být podvržené webové stránky mistrovství světa ve fotbale, kde se s neinformovanými uživateli z neoficiálních stránek uzavíraly smlouvy na služby za úplatu a zasíláním výhružných e-mailů z nich byly poté

peníze vymáhány. Zakoupené služby přitom byly ve stejné době na oficiálních stránkách mistrovství zdarma. (KRČMA, 2012)

3.3 Bezpečnostní opatření využívaná v bankovnictví

Ochrana internetového a mobilního bankovnictví proti moderním útočníkům není jednoduchá. Vyžaduje nejen důkladnou znalost jednotlivých forem útoků, ale také schopnost na daný útok vhodně reagovat, ochránit své klienty před jeho dopady a současně útok v co nejkratším čase eliminovat. Ochranu klientů před zneužitím jejich identity dokážou ve velké míře zajistit výše popsané technologie. Nicméně bez dokonalého know-how v oblasti internetového zločinu a bez schopnosti rychlé reakce kdekoliv na světě (útoky jsou většinou vedeny z úplně jiné země, než je cílová banka) není ochrana klientů a jejich účtů kompletní. Technologie je tedy vhodné doplnit právě o specializované služby (monitoring internetového podsvětí, rozpoznání připravovaného útoku, příprava banky na útok, eliminace útoku atd.), na které ale nemá v podstatě žádná banka dost kvalifikovaných lidí a většinou ani finančních zdrojů. (MATĚJŮ, 2013)

Maximální zabezpečení údajů ve vzdálené komunikaci je pro banku i pro klienty nejdůležitější z hlediska důvěry jejich klientů, partnerů, konkurence, veřejnosti a dobrého jména. Při tomto kontaktu se posílá mnoho informací, které jsou předmětem bankovního a firemního tajemství a které se nesmí cestou od klienta do zpracování žádným způsobem změnit, a ani nesmí být umožněno rozluštění obsahu při případném pasivním odposlechu a kopírování. (MÁČE, 2006)

Dobrou zprávou pro všechny je, že nejen technologie, ale i tyto specializované „anti e-fraud“ služby se dnes již dají plně outsourcovat. Špatnou zprávou naopak je, že stejně tak se dnes již dají plně outsourcovat služby útočníků. Kdokoliv, kdo umí alespoň trochu anglicky nebo rusky, si může přes internet objednat útok na vybranou banku a za pár set dolarů získat all-inclusive služby – od výroby trojského koně na vybranou banku až po výběr ukořistěných peněz a jejich zaslání na vaši adresu. (MATĚJŮ, 2013)

3.3.1 Zabezpečení bankou z pohledu klienta

Standardním bezpečnostním protokolem je TLS (Transport Layer Security protokol) definovaný v RFC-4246, který vychází ze známého protokolu SSL (Secure Sockets Layer). I tyto protokoly používají kombinaci symetrické kryptografie a certifikáty.

Praktickým použitím zabezpečení webových služeb (protokol http) je protokol http založený na praktickém uplatnění vrstvy SSL. (BUDIŠ, 2008)

K zabezpečení přístupu na webové stránky se používá speciální vrstva – protokol SSL. Takto zabezpečený web je označován jako HTTP, prohlížeče signalizují zabezpečené stránky například symbolem zámku ve stavovém řádku. Protokol SSL samotný se využívá například i pro ochranu elektronické pošty. Ve své podstatě se jedná o další vrstvu v síťové hierarchii, která přebírá data od aplikační vrstvy (v našem případě HTTP) a předává je příslušně chráněné nižší vrstvě (TCP/IP protokolu). (DOSEDĚL, 2004)

3.3.2 Uživatelské jméno a heslo

Obecně nejběžnějším a nejznámějším způsobem autentizace je uživatelské jméno či číslo a heslo. K potvrzení identity tedy uživateli internetového bankovnictví stačí znát tyto dva údaje. To je pro uživatele IB sice poměrně nenáročná, ale ne příliš bezpečná metoda. Zjistí-li tyto údaje cizí osoba, získá neomezený přístup k vašemu účtu, banka nemá šanci poznat, že se nejedná o „správného“ uživatele. I v případě, že jméno a heslo pečlivě střežíte, může být váš účet napaden. Existují totiž programy, které umí tzv. odečítat z klávesnice a šikovný hacker si údaje dokáže snadno zjistit. (BOUŠOVÁ, 2006)

3.3.3 Elektronický podpis

V Evropě směřoval vývoj ke standardizaci prostředí pro adaptaci bezpečné elektronické komunikace jako alternativy k obecně používané metodě založené na předávání papírových dokumentů. Cílem bylo vytvoření závazné směrnice EU

k elektronickému podpisu. Přibližně dva roky byly diskutovány její principy, zaměření a konkrétní pojmy. V říjnu 1997 byla Evropskému parlamentu předložena studie „O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování“. Výstupním dokumentem, dodnes prakticky závazným pro členské státy EU, je Směrnice Evropského parlamentu a Rady 1999/93 ES (dále jen směrnice) ze dne 13. prosince 1999. (BUDIŠ, 2008)

Implementace elektronického podpisu do českého právního řádu byla úspěšně provedena schválením zákona č. 227/2000 Sb., o elektronickém podpisu. O rok později následovala prováděcí vyhláška 366/2001 Sb., trvalo ale poměrně dlouho, než byla akceptována první certifikační autorita. Elektronický podpis dostal pod patronát speciální odbor Úřadu pro ochranu osobních údajů. V rámci reorganizace byl tento úřad začátkem roku 2003 pohlcen nově vznikajícím Ministerstvem informatiky, které tím převzalo zodpovědnost i za oblast elektronického podpisu. (DOSEDĚL, 2004)

Zákon o elektronickém podpisu definuje elektronický podpis jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. (BUDIŠ, 2008)

Elektronický podpis je jedním z nástrojů bezpečné elektronické komunikace. Nutnou podmínkou pro praktické využití elektronické komunikace je nastavení takových postupů, přístupů a principů, které bude možné považovat za rovnocenné běžné papírové agendě. (LIDINSKÝ, 2008)

Vyšší formou elektronického podpisu je **zaručený elektronický podpis**. Cílem jeho využití je nastavení takových procedur a procesů, které mohou být právně ekvivalentní klasickým, ručně psaným podpisům. Zaručený elektronický podpis splňuje následující požadavky:

1. Je jednoznačně spojen s podepisující osobou;
2. Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;

3. Byl vytvořen a připojen k datové zprávě pomocí prostředků, které může podepisující osoba udržet pod svou výhradní kontrolou;
4. Je k datové zprávě, ke které se vztahuje, připojen takovým způsob, že je možno zjistit jakoukoliv následnou změnu dat.

Jedinou doposud známou a obecně užívanou technologií, která umožňuje splnění výše uvedených podmínek, je takzvaný digitální podpis založený na využití kryptografických mechanismů. (BUDIŠ, 2008)

3.3.4 Certifikáty

Řešením problému správy, distribuce a uchovávání klíčů je využití takzvaného certifikátu veřejného klíče, zkráceně nazývaného certifikát. Certifikát lze z jistého úhlu pohledu chápat jako obdobu průkazu totožnosti, například občanského průkazu.

Certifikáty obsahují obvykle ve své nejjednodušší formě veřejný klíč. Jméno a další údaje zajišťující jednoznačnou identifikaci subjektu, kterému byl tento certifikát vydán. Běžně používané certifikáty též obsluhují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. (BUDIŠ, 2008)

Klientské certifikáty

Nejrozšířenějším typem certifikátu pro bezpečnou komunikaci po internetu je **komerční certifikát**. Toto označení se vžilo pro certifikáty, které nejsou spojeny se zákonem o elektronickém podpisu. Certifikátů tohoto typu se vydává v České republice desítky tisíc měsíčně, a je proto nejrozšířenějším typem. Komerční certifikáty mají široké uplatnění. Z technologického pohledu je možné použít komerční certifikáty pro zajištění autentizace komunikujících stran, šifrování (zajištění důvěrnosti) přenášených zpráv a elektronický podpis.

Certifikáty vydávané v souladu se zákonem o elektronickém podpisu se nazývají **kvalifikované**. Tyto certifikáty jsou určeny výhradně pro elektronický podpis.

Toto omezení použití kvalifikovaných certifikátů je dáno současnou českou legislativou, která i v tomto bodě vychází z evropských standardů. (BUDIŠ, 2008)

3.3.5 Čipové karty

Čipová karta musí obsahovat všechny potřebné algoritmy sloužící k vytvoření nebo ověření elektronického podpisu. Ve vztahu k procesu podepsání tak tvoří autonomní jednotku. Bezpečnost celého procesu elektronického podpisu datové zprávy se odvozuje od bezpečnosti prostředí, které s kartou komunikuje (překládá datovou zprávu k podepsání) a zabraňuje kompromitaci (vyzrazení) dat pro tvorbu elektronického podpisu. (BUDIŠ, 2008)

Multifunkční čipové karty

Čipová karta dnes také umožňuje současně nést více identifikačních nástrojů, jedná se o tzv. duální kartu. Tato karta je pak kromě čipu, který se využívá pro technologii elektronického podpisu, vybavena tzv. bezkontaktním čipem požadovaného standardu (případně i magnetickým proužkem). (BUDIŠ, 2008)

3.3.6 Autorizační kalkulátor, token

Autorizační kalkulačka je drobné elektronické zařízení, které dokáže generovat jednorázová hesla pro potvrzení operací. Kalkulačka tedy funguje na podobném principu jako SMS klíč. Kalkulačka je přenosná a je chráněna čtyřmístným heslem. Po zadání hesla a stisknutí příslušného tlačítka vygeneruje šestimístný kód, který klient aplikuje pro vstup do internetového bankovnictví. Pro každou aktivní transakci musí být vygenerováno nové číslo.
(BOUŠOVÁ, 2006)

Vzhledem k relativní jednoduchosti provedení a plošné dostupnosti rozhraní se začínají místo čteček čipových karet prosazovat USB tokeny (dongly, klíče). Takový USB token nabízí například Certifikační autorita PostSignum QCA (jedná se o iKey 4000 od Rainbow Technologies, které v roce 2004 pohltila firma SafeNet). Některé banky také umí použít token při přihlašování do internetového bankovnictví (třeba

UniCredit Bank nabízí kombinaci digitálního certifikátu a mezi jinými Rainbow iKey 2000 či 2032, iKey 2032 používá i Waldviertler Sparkasse). Poněkud odlišný token používá Volksbank.

Co všechny USB tokeny umí? Typické úlohy jsou:

- přihlášení k pracovní stanici (PC, OS);
- přihlášení do intranetu, extranetu, VPN;
- autentizace při vzdáleném přístupu;
- internetové bankovnictví, e-commerce, elektronické transakce a platby;
- přístup do (v podstatě libovolných) internetových aplikací;
- ukládání digitálních certifikátů a privátních klíčů, elektronický podpis;
- šifrování komunikace (e-maily apod.);
- obecně ukládání šifrovacích klíčů, šifrování dat.

(TOMEK, 2010)

Primárním požadavkem na hardwarové autentizační předměty (dále jen tokeny) je zajištění vyšší bezpečnosti oproti klasickému přihlašování jménem a heslem. Využití tzv. dvoufaktorové autentizace stupeň dosažené bezpečnosti nesporně zvyšuje. Prvním faktorem je fyzické vlastnictví tokenu. Útočník může získat přístup k počítači či ukrást notebook. Pokud ovšem zároveň nevlastní příslušný token, nemůže se vydávat za oprávněného uživatele.

Druhým faktorem je znalost PINu chránícího token před zneužitím. Token má zpravidla nastavitelný maximální počet neplatných zadání PINu. Překročením tohoto limitu dojde k zablokování tokenu. Znalost správného PINu je nezbytná pro aktivaci funkce tokenu. Útočník sice může odpozorovat PIN či heslo zadávané na klávesnici, není mu to ale moc platné – musel by také ukrást uživateli jeho token.

Pro hodnocení bezpečnosti tokenu je podstatné, jaký šifrovací algoritmus je v tokenu implementován, jaká je maximální délka šifrovacího klíče. Pozornost je dobré věnovat jednoduchosti používání tokenu a nárokům kladeným na uživatele. Zcela zásadní se stává široká využitelnost tokenu v různých aplikacích. (JELÍNEK, 2008)

3.4 Nové metody zabezpečení

3.4.1 BIOMETRIKA

Biometrika je založena na skutečnosti, že různé části lidského těla jsou pro každou osobu individuální, a mohou být tedy použity k její verifikaci. Požadavky bank na biometrické metody je možné shrnout do několika bodů zpracovaných britskou asociací APACS (Association for Payment and Clearing Services):

- **snadné pořízení vzorku** – změření osobního znaku a pořízení jejího vzorku nesmí být zatěžující nebo nepříjemné pro klienta, musí být levné, spolehlivé, rychle a snadno proveditelné bez zvláštních nároků na prostředí a zaškolení obsluhy;
- **snadné ověření vzorku** – ověření totožnosti držitele v obchodním místě musí být společensky přijatelné pro klienta i pro obchodníka, nesmí působit rozpaky a klást nároky na vybavení a znalost obsluhy;
- **nepřenositelnost** – měřený znak je unikátní osobní vlastností držitele karty a nemůže být ztracen nebo odcizen a zneužit;
- **nenapodobitelnost** – není možné napodobit verifikační znak.

Stabilnost – osobní znak je u dospělých osob dlouhodobě neměnný a je možné ho spolehlivě rozeznat. (JUŘÍK, 2003)

Biometrické identifikátory můžeme rozdělit do dvou skupin:

- psychologické (rozpoznávání otisků prstů, rozpoznávání tváře, geometrie prstu a ruky, skenování oční sítnice, skenování duhovky, rozpoznávání DNA);
- behaviorální (rozpoznávání hlasu, rozpoznávání kláves, rozpoznávání rukopisu). (FATIMA, 2011)

Nejznámější biometrické metody jsou:

Fotografie – ověření touto metodou je nejčastější u identifikačních průkazů (OP, pasy apod.). U platebních karet je umístění fotografie na přední nebo zadní stranu karty

používáno jako pomocný verifikační nástroj (např. u karet Citibank). Zkušenosti s touto metodou jsou však rozporuplné. V některých zemích došlo ke snížení ztrát se zneužitím odcizených karet (Německo), v jiných tato metoda nepřinesla žádné výsledky (Velká Británie). Někteří odborníci uvádějí, že řada obchodníků nevěnuje pozornost kontrole podpisu, je-li na kartě umístěna fotografie držitele, jíž se zákazník alespoň trochu podobá.

Otisk prstu – často používaná metoda pro identifikaci osob oprávněných ke vstupu do uzavřených zón. V bankovnictví problematicky použitelná vzhledem k policejnímu charakteru této metody. Současná zařízení rozpoznají, zda je k verifikaci použita živá nebo odumřelá tkáň (uříznutý prst).

Dynamický rozbor podpisu – je založen na principu výrazně individuálních rysů psaní. Klient se při pořizování vzorku podpisu podepisuje speciálním perem, které registruje rychlost, úhel a tlak při podpisu. Tyto rysy jsou pak při podpisu klienta v obchodním místě snímány a porovnávány se vzorkem. Metoda je schopna se do značné míry vyrovnat s odchylkami psaní při různých psychických a zdravotních stavech nebo změnách teplot prostředí.

Rozbor hlasu – metoda využívá rozbor vzorku hlasu oprávněné osoby. Při pořízení vzorku držitel karty obvykle vysloví řadu číslic od 1 do 10. Při použití karty je zařízením vyzván k vyslovení určitých náhodně vybraných čísel. Porovnáním se vzorkem dojde k ověření totožnosti. Tuto metodu používá např. First National Bank v Jihoafrické republice u bankomatů (včetně pojízdných) určených pro negramotnou část populace.

Záznam sítnice oka – tato metoda využívá jedinečné uspořádání očního pozadí člověka. Je však těžko použitelná v bankovnictví, protože pro uživatele představuje určité osobní omezení při verifikaci. Využívá se nejčastěji při ověření oprávnění k přístupu do vysoce utajených objektů.

Existují ještě další, zatím méně používané nebo vyvíjené metody identifikace (např. elektronické rozpoznání tváře, geometrie dlaně apod.). (JUŘÍK, 2003)

V tabulce níže uvádím jednotlivé metody identifikace a jejich náročnost na velikost záznamu dat.

Tab. 3 Náročnost identifikace metod na velikost záznamu dat (v bitech)

otisk prstu	300–1200
geometrie prstu	14
geometrie ruky	9
Iris	512
rozpoznání hlasu	1500
rozpoznání tváře	500–1000
ověření podpisu	500–1000
oční pozadí	96

Zdroj: JUŘÍK, 2003.

Základní pojmy biometriky

Verifikace – Uživatel zadá svoji identitu (pomocí hesla nebo karty) a následně poskytne své biometrické údaje, které se porovnají s daty uloženými v databázi. V databázi může být velké množství otisků, ale je porovnán pouze s tím, jenž je výstupem k ověření identity pomocí čipové karty nebo hesla atd. Verifikace je tedy porovnání 1:1.

Identifikace – Nepožaduje se, aby uživatel udal svoji identitu před tím, než bude jeho otisk porovnán. Uživatel tedy dá svůj otisk a ten se porovná s celou databází otisků, dokud nenajde shodu. Výstupem je pak identita uživatele (např. ID nebo jméno). Identifikace je často označována 1:N, protože se jeden otisk porovnává s velkým množstvím otisků.

Srovnání (Matching) – Srovnání biometrických vzorků, které nám určují stupeň shodnosti. Výsledkem je pak tzv. skóre (udává, jestli je vzorek shodný nebo ne).

- **Skóre**: Hodnota, která nám určuje stupeň shody dvou porovnávaných vzorů. Skóre může mít spoustu variací a není přesně dáno žádným standardem.

Shodnost vzorků nikdy nebude stoprocentní, proto je důležité, aby byly seřazeny všechny vzorky z databáze dle podobnosti se vzorem, podle kterého budeme srovnávat.

- **Mez**: Je hodnota, která je předem dána administrátorem. Vzorek, který má skóre nižší, je vyhodnocen jako vyhovující a zbytek za nevyhovující.

Pro přehledné srovnání různých biometrických metod můžeme použít například následující klasifikaci, kterou znázorňuje tab. 4.

Tab. 4: Porovnání biometrických metod

Biometrie	Bezpečnost	Přesnost	Náklady	Rychlost	Velikost čtečky
Krevní řečiště prstu	Vysoká	Vysoká	Nízké až střední	Vysoká	Malá až střední
Krevní řečiště dlaně	Střední až vysoká	Střední až vysoká	Nízké až střední	Střední	Malá až střední
Otisk prstu	Střední	Střední	Nízké	Střední	Malá
Črty obličeje	Nízká	Nízká	Střední	Střední	Velká
Oční duhovka	Vysoká	Vysoká	Střední až vysoké	Střední	Velká

Zdroj: autor.

Existují i další biometrické metody – např. identifikace člověka podle pachu, verifikace správnosti popisu, geometrie dlaně, podle dynamiky úhozů do kláves atd. Posuzovat jednotlivé biometrické metody není jednoduché a případná volba některé z nich závisí na mnoha faktorech. Především je třeba vyjasnit, kde a které biometrické systémy (technologie) lze v široké míře uplatnit, aby byly maximálně využity jejich přednosti a minimalizovány jejich zápory (zachování dlouhodobé přesnosti a spolehlivosti biometrické metody, náklady na pořizování biometrických dat a jejich kontrolu, ochrana biometrických dat před zcizením nebo znehodnocením atd.). Značná péče je věnována zejména ochraně biometrických dat použitých v podobě digitálního osobního průkazu. Krádeže osobních průkazů jsou např. ve Spojených státech

nejrychleji rostoucí oblastí kriminální činnosti, která ročně postihuje více než půl milionu osob. Hardware i software pro užívané biometrické identifikační technologie v současné době dodávají desítky světových firem.

V tabulce č. 5 uvádím srovnání použití jednotlivých metod při různých aktivitách.

Tab. 5: Použití biometrických metod

Aktivita	Otisk prstu	Krevní řečiště v prstu	Hlas	Dynamický podpis
Přímá identifikace a autentizace (Osobně na pobočce)	Ano	Ano	Ne	Ano
Vzdálená identifikace a autentizace (Přes webový prohlížeč)	Ne	Ne	Ano	Ne
Přímá autorizace (Osobně na pobočce)	Ano	Ano	Ne	Ano
Vzdálená autorizace (Přes webový prohlížeč)	Ne	Ne	Ano	Ne
Fyzický vstup (Do budovy, místnosti)	Ano	Ano	Ne	Ne

Zdroj: autor.

Budoucnost a biometrika

V budoucnu lze předpokládat růst využití biometrických údajů pro ověřování identity. Letos Apple udělal odvážný krok, když oznámil, že jeho nový iPhone 5s bude mít integrovaný otisk prstu jako autentizaci uživatele pro přístup do přístroje. Není důležité, že tato ochrana byla prolomena jen několik dní po jeho uvedení na trh, lidi to přinutilo mluvit o významu dvoufaktorové autentizace ve světě, kde se jednoduché přihlašování pomocí hesla stává stále větším archaismem. V důsledku tohoto obnoveného zájmu předpokládáme, že příští rok přidají druhý faktor autentizace do

svých zařízení další mobilní výrobci. Budeme také svědky nárůstu dalších forem ověřování, jako je skenování duhovky, rozpoznání obličeje nebo tetování. Pracuje se i na metodách, které jsme zatím viděli jen ve sci-fi filmech, jako jsou speciální vysílače identifikačního signálu, které je možné polknout a jejichž napájení je zajištěno díky žaludeční kyselině.

Biometrie – rychle zdokonalovaná počítačovými technologiemi – nepochybně zjednoduší prokazování identity osob. Převratné objevy lze očekávat při výzkumu DNA v lékařských vědách a v genovém inženýrství. Pokroky v těchto vědních oborech v budoucnu pravděpodobně přinesou i vhodné metody a zařízení použitelné k identifikaci jedince, např. podle DNA, ve větší šíři v praxi.

Průmysl se bude, jak uvádí známá agentura pro průzkum trhu Frost & Sullivan, orientovat především na snímání otisků prstů. Dosud dominující optické snímače však budou podle ní zřejmě vytlačeny polovodičovými kapacitními snímači, které dnes již mohou být lepší, menší a levnější než optické.

3.4.2 Splývání technologií a lidských komunit

Velmi pravděpodobně se objeví též systémy, které budou využívat k přípravě informací aktivní spolupráce „živého“ uživatele. Právě ten jim ze záplavy informací pomůže vybrat to podstatné. Chytré komerční projekty budoucnosti si to zajistí tak, aby uživatel měl sám zájem co nejlépe s aplikací spolupracovat a investovat do chodu systému, tedy teď již spíše komunity, svou vlastní práci. V komerčních aplikacích budoucnosti se tedy nemusí jednat jen o originalitu technického řešení; úspěšné projekty setřou velmi pravděpodobně hranice práce strojů a práce lidské. Těžko totiž bude možné striktně zahrnout výsledek koordinované práce člena komunity pouze do jedné z těchto kategorií. (DONÁT, 2000)

3.4.3 TV banking

Jako první spustila televizní bankovnictví v roce 2008 Era banka, která se chtěla co nejvíce přiblížit potřebám svých klientů, tudíž nabídla další produkt možného ovládání účtu. Důležité je zde zmínit, že se jedná o digitální přenos (co se týče televizí). Poštovní spořitelna tento produkt uvedla do chodu společně s Telefónicou O2 a jejich snahou bylo nabídnout další typ bankovnictví co největšímu okruhu lidí, a to převážně těm, kteří nemají zájem nebo se bojí ovládat svůj účet přes internet či mobilní telefon. (KRČMÁŘ, 2005)

Následující obrázek ukazuje, jak by mohlo vypadat ovládání účtu přes televizi. Jako příklad uvádím TV banking zahraniční Union Bank, která působí na Srí Lance.

Obr. 2 TV banking Union Banky na Srí Lance, zdroj: http://www.unionbnews.com

4 Analýza současného stavu

V této kapitole provedu analýzu zabezpečení jednotlivých bank. Na zabezpečení se podíváme ze dvou různých úhlů pohledu – jaké možnosti zabezpečení využívají jednotlivé banky a jak se na bezpečnost dívají samotní uživatelé.

Bankovní služby využívá 88 procent obyvatel České republiky, což je stejně jako na Slovensku. Žádnou banku nepoužívá 12 procent lidí – jde zejména o studenty a mladé lidi bez zaměstnání. (www.aktualne.cz, 2013)

Vyplývá to z průzkumu FMDS společnosti GfK, který probíhá na ročním vzorku 4000 respondentů v České republice ve věku od 15 do 70 let. Na Slovensku se průzkumu účastní 6000 lidí. (www.gfk.com, 2013)

Jen 56 % obyvatel Česka, kteří vlastní běžný účet, loni využilo i služby elektronického bankovnictví. Na Slovensku je to polovina klientů. Přesto se využití elektronického bankovnictví za posledních pět let zdvojnásobilo. Nejrozšířenější je jednoznačně internet banking, v posledních měsících získávají na popularitě i bankovní aplikace ve smartphonech. (www.gfk.com, 2013)

4.1 Útoky na el. bankovnictví

Společnost Cisco zveřejnila výsledky své pravidelné studie Annual Security Report, která sleduje aktuální stav bezpečnosti na internetu a nové trendy v této oblasti. Podle studie došlo během roku 2013 k 14 % nárůstu bezpečnostních hrozeb a zranitelností. Od roku 2000, kdy se jejich počet pravidelně sleduje, se jedná o nejvyšší dosažené hodnoty. Ovšem bez nadsázky můžeme tvrdit, že před rokem 2000 situace nemohla být horší, takže bezpochyby jde o nejhorší statistiky v celé historii IT. (www.cisco.cz, 2014)

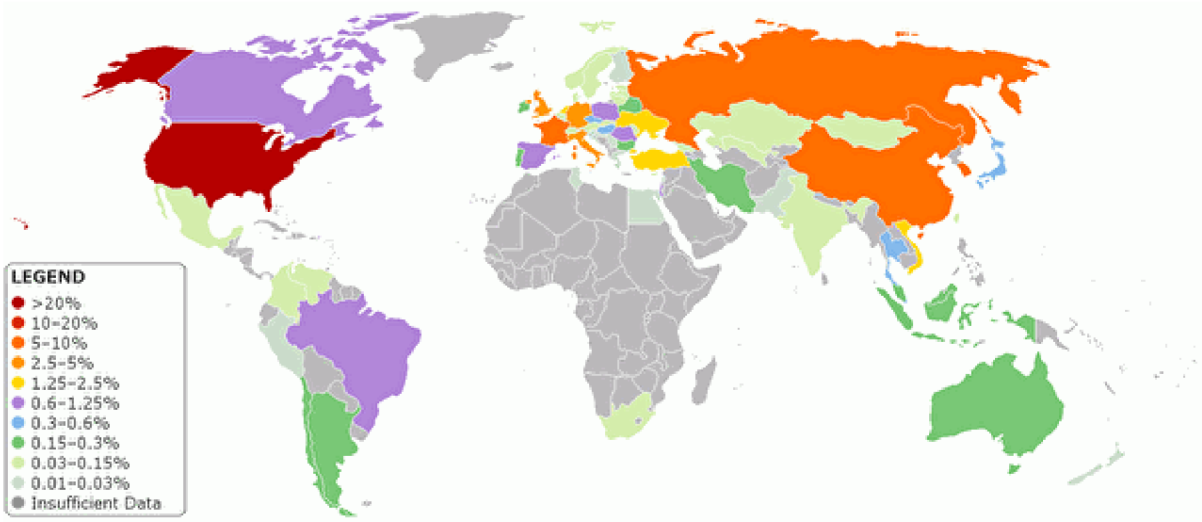
Nejčastějším malwarem šířeným prostřednictvím webu se v loňském roce staly víceúčelové trojské koně. Tvořily 27 % všech odhalených škodlivých kódů. Druhou

příčku zaujaly škodlivé skripty (23 %), následovaly trojské koně zaměřené na krádeže dat (22 %). (www.cisco.cz, 2014)

Renesanci zažívají DDoS útoky, ještě nedávno považované za ustupující trend. V současnosti však stoupá jak jejich počet, tak i závažnost. Často slouží také k maskování jiných, mnohem závažnějších útoků – jako je třeba kybernetická krádež provedená před, během nebo krátce po masivním DDoS útoku, který zcela zaměstná pracovníky IT bezpečnosti.

Poslední generace bankovního malwaru, která na sebe nenechala dlouho čekat, zcela eliminovala výše zmíněný nedostatek a k dokončení transakce již v podstatě nepotřebuje téměř žádnou součinnost ze strany klienta. Klient již nemusí žádný mTAN přepisovat, neboť škodlivý kód si ho obstará sám. Jediné, co musí klient udělat, je nainstalovat si do svého smartphonu aplikaci, která bude číst obsah zpráv a přeposílat je útočníkovi.

Nyní již můžeme pomalu očekávat další generaci bankovního malwaru, která bude víceméně jen zdokonalovat výše uvedený koncept. Lze očekávat silně polymorfní zašifrovaný kód využívající asymetrické kryptografie, který se bude v napadeném systému maskovat a bránit se odhalení. Je jisté, že C&C servery budou běžně navštěvované servery, a stejně tak i server sloužící jako drop zóna. K uložení příslušných údajů bude nepochybně využita steganografie. Samozřejmostí pak bude i perfektní čeština.



Obr. 3: Mapa světového malware, zdroj:trustwave.com.

Při posledním největším útoku označovaném jako Eurograbber bylo postiženo několik desítek tisíc klientů a z jejich účtů bylo odčerpáno několik desítek miliónů EUR. Útoky ale probíhaly i mimo EU, zasaženi byli i klienti větších bank v zemích bývalého SSSR, dále pak USA a Austrálie.

Situace došla již tak daleko, že Česká národní banka vydala k dané problematice vlastní materiál s doporučeními všem klientům používajícím elektronické bankovnictví jako prostředek nahrazující návštěvu pobočky. *"Česká národní banka soustavně prosazuje a dohlíží na to, aby jednotlivé banky při poskytování svých služeb průběžně vyhodnocovaly s nimi spojená rizika a přijímaly opatření na jejich omezení. Bezpečnost každého vzdáleně ovládaného účtu však nezávisí pouze na zabezpečení informačních systémů jednotlivých bank, ale také na péči a pozornosti, kterou věnuje bezpečnosti samotný klient,"* odůvodňuje ČNB svůj dohled v dané věci. (ww.cnb.cz, 2012)

Trojici největších tuzemských bank, ČSOB, Komerční banku a Českou spořitelnu, ale i Českou národní banku a některé menší napadli hackeři. Téměř na celé dopoledne jim vyřadili z provozu webové stránky. Nefungovalo internetové ani mobilní bankovnictví.

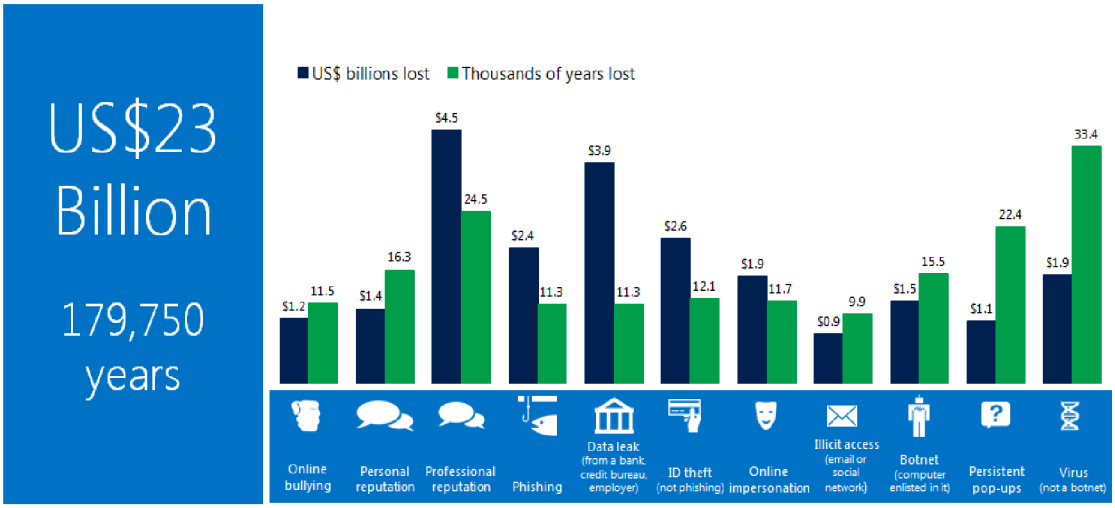
Jak potvrdili zástupci bank, za problémy byl útok hackerů. Podle informací ČSOB byl útok veden ze zahraničí.

Útoky z října 2013 byly vedeny prostřednictvím takzvaného trojského koně, který se snaží obejít autentizaci klientů českých bank, aby si mohli útočníci z jejich účtů posílat peníze. A protože většina tuzemských zákazníků internetového bankovnictví používá ověřovací SMS zprávy, snaží se útočníci napadnout i jejich mobilní telefony. Zpravidla k tomu dochází tak, že jsou klienti nevědomky přesměrováni do falešného internetového bankovnictví, kde jsou vyzváni k instalaci škodlivého mallwaru do svých smartphonů. (www.businessworld.cz, 2013)

Podle odborníků na kybernetickou bezpečnost je nejnovější útok o to rafinovanější a nebezpečnější. „Snaží se obejít i standardně používanou dvoufaktorovou autentizaci, proto může být cílem hackerů v podstatě kterýkoli uživatel internetového bankovnictví v Česku," říká Jan Matoušek, náměstek České bankovní asociace (ČBA), která před útoky varovala s tím, že podobné hackerské aktivity nedávno zaznamenala ve Velké Británii, Portugalsku, Turecku a dalších zemích na území Evropy. (www.cba.cz, 2013)

Při příležitosti Dne bezpečnějšího internetu 2014 byly představeny výsledky již třetího ročníku průzkumu Microsoft Computing Safety Index (MCSI). Průzkum vyčíslil, že rizika na internetu stojí oběti v průměru až 23 miliard dolarů ročně a teoretický čas na nápravu vzniklých škod představuje časové náklady dosahující řádu 200 000 let. Nejvyšší újmu s sebou nese poškození profesní reputace, kdy se průměrná ztráta pohybuje okolo 535 dolarů na osobu. Mezi další „nejdražší", a tím i nejnebezpečnější rizika pak patří krádeže ID, úniky dat z bank a od zaměstnavatelů, online šikana nebo phishing.

Průzkum byl proveden mezi 10 500 respondenty z 20 zemí, jejichž obyvatelé tvoří 60 % celosvětových uživatelů internetu. Níže uvádím grafické znázornění, kolik dolarů v průměru stojí jednotlivá rizika dle uvedeného průzkumu. (Microsoft Computing Safety Index, 2013)



Obr. 4: Náklady na odstranění škod při prolomení bezpečnosti, zdroj: Microsoft Computing Safety Index 2013

Dle průzkumu jsou škody při prolomení bezpečnostních bariér u bank vyčísleny na 200 amerických dolarů na osobu a celosvětově škody dosahují výše 3,9 bilionu amerických dolarů. Po ztrátě a poškození profesní reputace je to druhá nejvyšší vyčíslená škoda. Časové náklady jsou jedny z nejnižších, ale i tak dost vysoké, a to 11 300 let.

4.1.1 Největší útoky na české servery v historii:

30. září 2008 – DDos útok, při kterém byly servery zahlceny velkým množstvím dotazů a nefungovaly, postihl zpravodajské weby Blesk.cz a DenikSport.cz, které patří vydavatelství Ringier.

29. května 2011 – Hacker napadl den před zahájením písemné části státních maturit internetové stránky s ukázkovými testy a informacemi o zkoušce. Nefungovaly ani stránky organizace Cermat, která maturity zajišťuje. Útočníci nahráli na web vlastní obsah.

Leden a únor 2012 – Během schvalování kontroverzní dohody proti padělatelství ACTA napadli lidé hlásící se k hnutí Anonymous celou řadu českých webů. Terčem útoku byly internetové stránky autorských organizací (Ochranného svazu

autorského, Mezinárodní federace hudebního průmyslu IFPI či Intergramu), ale i web ODS nebo stránky Poslanecké sněmovny ČR a vlády. Intenzita a druh útoků byly různé; vedle zahlcení serverů se hackerům například podařilo získat osobní data tisíců členů ODS.

14. října 2012 – Internetovou stránku brněnských komunistů napadli hackeři z hnutí Anonymous. Téměř na den na ně umístili nápis, podle něhož jsou voliči KSČM „omezení idioti“. Web pozměnili po krajských volbách, a to v reakci na úspěch komunistů, jehož v nich dosáhli.

16. listopadu 2012 – Hackeři získali databázi z webu exekutorské komory a data umístili na internetu. Skupina Czechurity na svém webu uvedla, že zabavila databázi, neboť exekutoři zabavují majetek občanům. Web komory byl na krátkou dobu po oznámení útoku mimo provoz.

Březen 2013 – Od 4. března napadli neznámí útočníci pomocí DDoS útoku, kdy zahltili servery obrovským množstvím požadavků, nejprve velké české zpravodajské weby. V úterý byl terčem útoku také portál Seznam.cz i další stránky. Dnes čelí napadení stránky českých bank včetně internetového bankovnictví.

4.2 Přehled zabezpečení u jednotlivých bank

V dnešní době se banky snaží co nejlépe chránit data svých klientů. Důležité je zvolit mezi jednoduchým uživatelským prostředím a maximální mírou zabezpečení. Jednotlivé banky používají různé stupně zabezpečení různým způsobem a s různým důrazem. Každá z možností, které se nabízejí, má svoje výhody i nevýhody z pohledu banky i klienta.

Klient se do internetového bankovnictví musí zpravidla dvoufaktorově autentizovat, to znamená, že nejprve zadá své uživatelské jméno a heslo (faktor z kategorie „něco ví“) a poté jednorázové heslo, které mu přijde na mobil (faktor

z kategorie „něco má“). Tím je splněn požadavek na dvoufaktorovou autentizaci, tak jak ho definuje ve svém doporučení FFIEC. (www.businessworld.cz, 2013)

Nezávislé autentizační faktory můžeme rozdělit do třech kategorií, které se liší způsobem, jakým ověřují totožnost uživatele. Jednotlivé varianty lze pak kombinovat s celou řadou technologií lišících se uživatelským pohodlím a spolehlivostí, s jakou dokážou přesně určit, koho do systému pustit a koho ne. Mezi metody přihlášení pak patří nejčastěji kombinace:

- **něco vím** – něco, co uživatel musí znát. Typická jsou přístupová hesla, správná kombinace znaků, pro bankomaty nebo mobilní telefony PIN kódy a také správné odpovědi na „bezpečnostní otázky“.
- **něco jsem** – tato třída zahrnuje využívání biometrických senzorů pro snímání otisků prstů, sítnice a duhovky nebo algoritmy pro měření charakteristiky chování, jako rytmus psaní nebo identifikace hlasu.
- **něco mám** – něco, co uživatel vlastní. Patří mezi ně fyzické klíče, průkazy totožnosti a také komunikační zařízení, například hardwarový token, standardní mobilní telefon nebo smartphone.

Nejčastějším a neznámějším příkladem využití dvoufaktorové autentizace v internetových službách je kombinace faktoru „něco vím“ ve formě hesla se zasíláním SMS zpráv na mobilní telefon (něco mám) nebo využitím aplikace pro tvorbu jednorázových hesel ve smartphonech. Hlavní výhoda tohoto systému spočívá v tom, že mobilní telefon vlastní skoro každý, a odpadá tak nutnost koupit si nebo instalovat novou platformu, která by sama o sobě plnila pouze funkci dalšího autentizačního faktoru. Ke svému profilu se tedy přihlásíte pouze v případě, že znáte heslo a máte u sebe svůj mobilní telefon, jehož prostřednictvím získáte jednorázové heslo umožňující přístup k vašemu účtu. Útočník, který by chtěl zneužít vaši identitu, by musel nejen získat vaše heslo, ale také mobil, bez něhož by neměl šanci se k vašemu účtu přihlásit.

Většina bank je chráněna proti napadení svých systémů účinnou kombinací hardwarových a softwarových obranných prvků, jako jsou firewally, detektory průniku

nebo oddělením jednotlivých informačních systémů od přístupu z internetu. Účinnost těchto ochran je pravidelně kontrolována vzhledem k bezpečnostním politikám banky.

V rámci přehledu zabezpečení jednotlivých bank se budeme zabývat konkrétními metodami jednotlivých bank.

4.2.1 Informovanost klienta

Každá banka na svém webu uvádí návod jak správně používat elektronické bankovnictví.

Nejčastěji banky uvádějí bezpečnostní zásady využívání elektronického bankovnictví. Tyto zásady se týkají hlavně přihlašování a používání elektronického bankovnictví. Nejčastější únik dat klienta nebo napadení elektronického bankovnictví je způsoben pochybením na straně uživatele. Proto je velmi důležité, aby uživatel dodržoval tyto bezpečnostní zásady, a předešel tak možným ohrožením. Při nedodržení těchto pravidel nemusí být brán zřetel na pozdější reklamace zneužití klientova elektronického bankovnictví třetí osobou.

K celkovému bezpečí patří i maximální ochrana osobního počítače používaného pro internetové bankovnictví. To znamená udržování aktuálních bezpečnostních oprav u operačního systému, zapnutí antivirové kontroly (včetně pravidelně aktualizovaných souborů) a v neposlední řadě i aktivování a správné nastavení brány firewall v operačním systému.

Jako příklad uvádím bezpečnostní pravidla od Citi Bank:

1. *Používejte jen vlastní počítač, notebook, tablet nebo chytrý telefon. Pro přístup na internetové bankovnictví nepoužívejte neznámých počítačů, kde neznáte úroveň zabezpečení a stavu takového počítače.*

2. *Zajistěte pravidelnou aktualizaci operačního systému, prohlížeče, používaných aplikací a jiného programového vybavení. Nepoužívejte k přístupu na*

internetové bankovnictví počítač, který nemá nejnovější bezpečnostní instalace. I přenosné zařízení typu tabletu nebo chytrého telefonu je nutné pravidelně aktualizovat.

3. *Používejte programy, které jsou určené pro ochranu Vašeho počítače, jako jsou antivirové programy, anti-spywarové programy a v neposlední řadě i aktivní osobní firewall. Tyto programy jsou k dispozici i pro tablety a chytré telefony.*

4. *Používejte jen bezpečné heslo/PIN, kterému věnujete pozornost ve formě pravidelné změny.*

5. *Ochraňujte své heslo/PIN, nezapisujte si jej a nikomu takové ověřovací údaje nesdělujte. Používejte T-PIN jen k ověření Vámi provedeného hovoru na linku CitiPhone.*

6. *Neotevírejte nedůvěryhodné e-maily, neklikejte na vložené odkazy, nestahujte podezřelé přílohy, které obdržíte v rámci Vaší elektronické pošty a kde nebyla provedena anti-virová kontrola.*

7. *Nikdy nereagujte na emailové žádosti, které mohou žádat Vaše přihlašovací údaje ve formě hesla, PINu nebo jiného ověřovacího prvku a nikdy neposílejte v emailu žádná hesla nebo jiné přihlašovací údaje.*

8. *Nenavštěvujte neznámé stránky a nestahujte z internetu neznámé soubory, které mohou obsahovat škodlivý mallware nebo jiný nežádoucí software. Vždy využívejte jen oficiální aplikace pro Váš operační systém (iOS, Android, Windows, apod.), které jsou dostupné na aplikačních marketech.*

9. *Využívejte zasílání zpráv o provedených transakcích (CitiAlerts) a sledujte historii svého přihlašování. Zajímejte se o bezpečnostní rizika a trendy k bezpečnému používání Vašeho počítače, tabletu nebo chytrého telefonu.*
   (www.citibank.cz, 2011)

Časté je upozornění na podezřelé emaily, tzv. **Phishing**. V těchto e-mailech, které vypadají, jako by přicházely z některé ze známých firem, se jejich odesílatelé snaží získat přístup k důvěrným datům klientů (např. čísla účastníků služby eBanking, PIN, TAN, popř. čísla kreditních karet).

V případě tzv. Phishingu, nového umělého slova odvozeného z výrazů "password" a "fishing", je cestou e-mailu požadováno sdělení klientských údajů nebo je v e-mailu uveden odkaz na falešnou internetovou stránku. Tam je pak požadováno zadání osobních přístupových údajů nebo důvěrných informací, které jsou pak předávány nepovolaným osobám.

Při pročítání těchto bezpečnostních zásad jednotlivých bank najdeme vždy kontakt na infolinku banky a návod jak postupovat v případě napadení elektronického bankovnictví nebo jen podezření na jeho zneužití.

4.2.2 Zabezpečení přístupu bankou

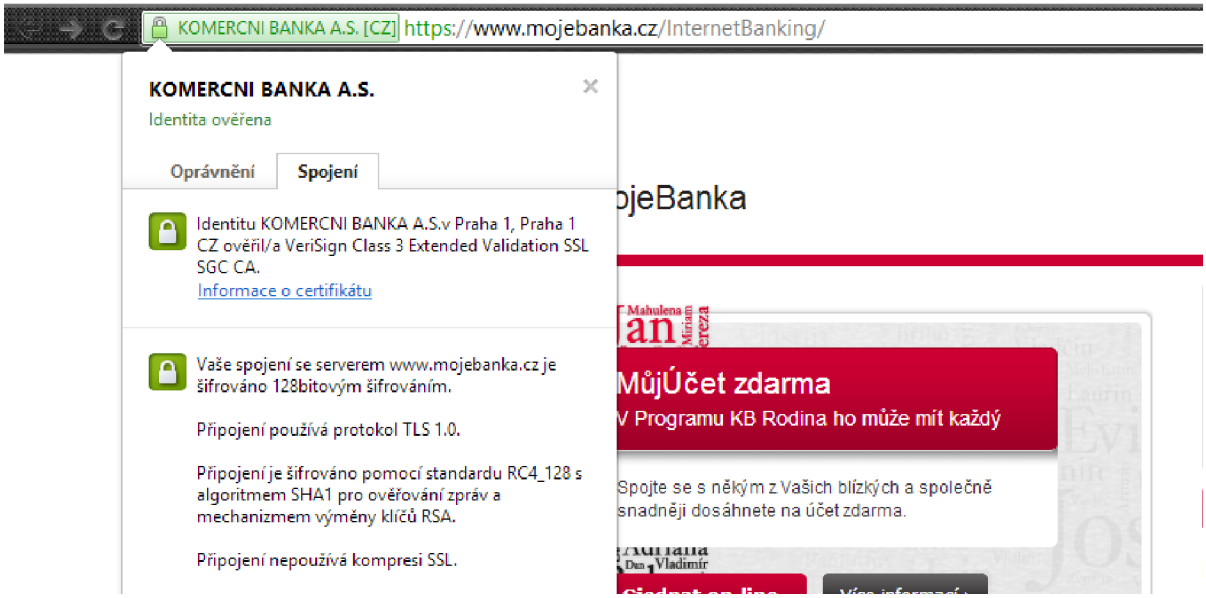
Identita banky je ověřována tzv. SSL certifikátem, který bance vydává nezávislá instituce (nejčastěji VeriSign). Klient tak má jistotu, že stránky, jejichž prostřednictvím komunikuje s bankou, patří skutečně jí. Přenos citlivých dat je ve všech bankách řešen SSL šifrováním (obvykle ikona žlutého visacího zámku na stavové liště) na vysoké úrovni a lze jej považovat za dostatečně bezpečný.

Zde uvádím, jakým způsobem interpretuje bezpečnost Česká spořitelna: „*Pro základní bezpečnost Vašich příkazů musí být zajištěno, aby příkaz k bankovní operaci nebyl nikým modifikován. K tomuto účelu je použito silné 128bitové šifrování komunikace s bankou po Internetu pomocí technologie SSL. Pro navázání šifrované komunikace je navíc použit certifikát serveru banky vydaný důvěryhodnou certifikační autoritou, který zajistí, že skutečně komunikujete s bankou a ne s někým, kdo se za aplikaci internetového bankovnictví pouze vydává.*“ (Česká spořitelna, 2013)

Zabezpečení přihlášení do internetového bankovnictví České spořitelny.

Obr. 5: Zabezpečení přihlašovacích stránek České spořitelny, zdroj: www.csas.cz

Jako další příklad uvádím využití https protokolu Komerční banky.



Obr. 6: Zabezpečení přihlašovacích stránek Komerční banky, zdroj: www.kb.cz

4.2.3 Autentizace klienta

První bariérou proti zneužití je způsob, jakým se do elektronického bankovnictví přihlašujeme. Banka po ověření klientského čísla (resp. přihlašovacího jména) a autentizačního kódu (resp. hesla) zjistí, kdo se přihlásil k internetovému bankovnictví. Úspěšně ověřená identita klienta se pak následně používá ke kontrole oprávnění k manipulaci s účtem. Dále se k autentizaci využívá také digitálních certifikátů v počítači, na digitální kartě nebo speciálním tokenu anebo autentizace prostřednictvím SMS zpráv. Každá z těchto metod má svoje výhody i nevýhody. Po

úspěšném ověření klient vstoupí do prostředí internetového bankovnictví a zde zadává jednotlivé příkazy a pokyny.

Pro přihlášení do internetového bankovnictví nebo potvrzení transakce požadují mnohé banky po svém klientovi zadání čísla mTAN (mobile Transaction Authentication Number), které mu zasílají přes síť mobilního operátora ve formě SMS na jeho mobilní telefon.

Přehled autentizačních metod

Kvalita jakéhokoliv automatizovaného přístupového systému je závislá téměř výhradně na kvalitě autentizačního mechanismu. Je-li identita autorizovaného uživatele ověřena v rozsahu povolené odchylky, je systémem zprostředkován přístup do prostředí s řízeným přístupem, v opačném případě je přístup zamítnut. Existuje velké množství metod zabezpečujících autentizaci uživatele, které tvoří základ přístupových systémů. Mechanismus ověřování identity uživatele je obecně založen na tom:

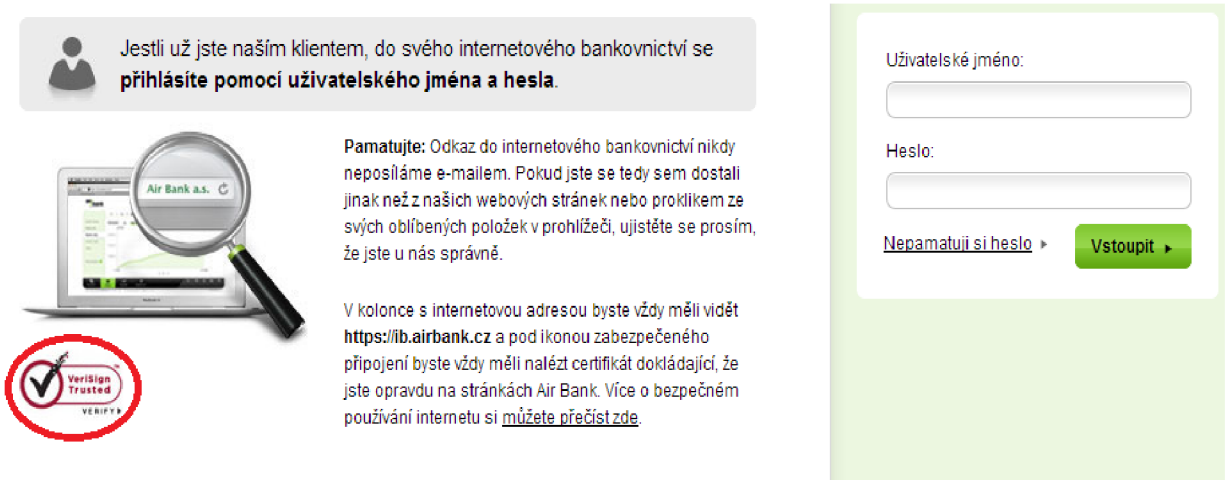
- co zná pouze uživatel – například heslo,
- co uživatel vlastní – například autentizační předmět,
- co je pro uživatele charakteristické – například otisk prstu.

Ve stejném duchu pak říkáme, že je použita:

- autentizace heslem (autentizace založená na znalosti hesla),
- autentizace předmětem (autentizace založená na vlastnictví předmětu) a
- biometrická autentizace (autentizace založená na biometrických charakteristikách člověka).

(BOUŠOVÁ, 2006)

Zde uvádím příklad přihlašovací stránky Airbank. U přihlášení jsou uvedeny bezpečnostní pokyny a vidíme i ověřovací logo VeriSign, Inc.



Obr. 7: Zabezpečení přihlašovacích stránek AirBank, zdroj: www.airbank.cz

4.2.4 Autorizace transakcí

Elektronický podpis dovoluje, aby klient mohl provádět finanční transakce vzdáleně, pomocí počítače. Tento mechanismus dovoluje odesílateli zprávy (klientovi) „podepsat“ zprávu elektronickým podpisem tak, že příjemce zprávy (bankovní server) může jednoznačně prokázat, že zprávu odeslal a podepsal právě tento klient. Ve spojení se smlouvou o vzájemném uznávání elektronických transakcí, kterou uzavřela banka s klientem, může bankovní server jednoznačně prokázat, že klient transakci provedl, a klient se nemůže zbavit zodpovědnosti za provedenou transakci. Mechanismus elektronického podpisu také jednoznačně určí, zda zpráva byla odeslána skutečně klientem a nikoli případným útočníkem (definice samozřejmě platí i v opačném vztahu).

Obrázek níže ukazuje podobu autorizační sms pro potvrzení transakce zadané přes elektronické bankovnictví Servis 24 od České spořitelny.

Obr. 8: Potvrzení transakce pomocí autorizační sms, zdroj: www.csas.cz.

Následující tabulka ukazuje, jakým mechanismem (nad standardní přihlašovací jméno a heslo) jsou peníze v internetovém bankovnictví chráněny.

Tab. 6: Přehled zabezpečení internetového bankovnictví

BANKA	ZABEZPEČENÍ INTERNETOVÉHO BANKOVNICTVÍ (IB)
Air Bank	Banka může přihlášení ověřit pomocí SMS v případě, že vyhodnotí riziko zneužití. První platba po přihlášení do internetového bankovnictví je autorizována přes SMS, další, které zákazník provede do určitého časového limitu a pouze v aktuálním přihlášení, jsou autorizovány prostřednictvím přihlašovacího hesla.
Citibank	K zabezpečení IB slouží autentizační kalkulátor. Ten vyžaduje zadání PIN kódu a následně zobrazí automaticky vygenerovaný kód.
Česká spořitelna	Možné jsou dvě varianty zabezpečení. Volit lze z klasického zabezpečení autorizace plateb SMS, to je možné doplnit o zasílání SMS i pro potvrzení přihlášení. Druhou možností je certifikát na čipové kartě, kterým se klient přihlašuje a autorizuje transakce.
ČSOB	Ověřování SMS nebo čipovou kartu při při login i při platbě.
Equa bank	Potvrzování plateb pomocí SMS. Klienti mohou zvolit také ověřování přihlášení pomocí SMS.
Fio banka	Možnost volby nebo kombinace z klasického zajištění pomocí SMS při platbách a ze speciální aplikace, která generuje unikátní klíče chráněné dalším heslem.
GE Money Bank	První variantou je klasické zajištění plateb pomocí SMS, k tomu si dobrovolně můžete přidat autentizační SMS pro potvrzení přihlášení.

	Druhou možností je speciální certifikát, který si nainstalujete do počítače a do kterého se následně přihlašujete přes identifikační číslo a heslo. Platby je v takovém případě nutné potvrdit digitálním podpisem.
Komerční banka	Nutný je osobní certifikát, kterým se klient, který se používá pro autentizaci a autorizaci uživatele při přihlášení do aplikace, pro podpis platebních příkazů apod. Samotný certifikát může být uložen jako soubor v počítači, na USB, na CD/DVD nebo na čipové kartě. Platby se dále potvrzují pomocí SMS.
LBBW Bank	První možností je klasické zabezpečení plateb pomocí SMS. Druhou variantou je autentikátor a autorizační/platební karta. Při přihlášení do systému se v takovém případě používá přihlašovací jméno a jednorázové heslo – OTP, které vygeneruje autentikátor. Platby je pak třeba podepsat speciálním kódem.
mBank	Potvrzování plateb pomocí SMS.
Oberbank	Oberbank má zabezpečené transakce pomocí kódů TAN (transakční autorizační kód): Šestimístný kód TAN slouží jako osobní elektronický podpis. Klient obdrží obálku s 99 transakčními autorizačními kódy, přičemž každý z nich lze použít pouze jednou na jednu transakci. Hned poté TAN pozbývá platnost. Čísla může používat v libovolném pořadí. Jakmile spotřebujete 70 TANů, automaticky se objedná další obálka s 99 novými kódy.
Poštovní spořitelna	Nabízí stejné možnosti jako její matka ČSOB. Ale s tím rozdílem, že nadále je přihlašování do IB autentizováno pomocí SMS jen v případě, že si to klient zvolí.
Raiffeisenbank	Klienti mohou vybírat z několika možností. K dispozici je klasické potvrzování plateb kódem z SMS. Druhou možností je podpisový certifikát, tedy heslem chráněný šifrovaný soubor, který je uložen v počítači nebo na přenosovém disku. Další možností jsou například potvrzovací kódy zasílané v šifrované SMS. Umožňuje to technologie SIM Toolkit, kterou je dnes vybavena většina mobilních telefonů. Přístup k mobilnímu elektronickému klíči v telefonu je chráněn speciálním osobním identifikačním číslem (BPIN).
UniCredit Bank	IB zabezpečeno buď bezpečnostním klíčem v podobě malého kalkulátoru (hardware token) nebo mobilním bezpečnostním klíčem (jednorázové kódy zaslané na mobilní telefon pomocí SMS). Obě varianty slouží pro zabezpečení přihlášení do internetového bankovnictví (autentifikace) a pro podepisování transakcí (autorizace).
Sberbank	IB Sberbank využívá zabezpečení pomocí elektronického klíče – tzv. tokenu. Prostřednictvím kombinace přístupového jména, vlastního PIN a token kódu ověřena identita uživatele. Token každou minutu automaticky generuje nový jednorázový autorizační klíč, tzv. token kód, s omezenou časovou platností.
Waldviertler Sparkasse (rakouská banka působící v jižních Čechách)	Ověřování přes SMS nebo čipovou kartu při přihlášení do IB i při platbě.
Wüstenrot hypoteční banka	Potvrzování plateb pomocí SMS.
Zuno Bank	Potvrzování plateb pomocí SMS.

Zdroj: Aktuálně.cz

4.2.5 Tokeny a čipové karty

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace u služby Internet Banking a slouží k přihlášení a autorizaci aktivních operací. Elektronický klíč je z důvodu maximálního zabezpečení uložen na kryptografickém USB klíči – **Tokenu**, který je chráněn před zneužitím PIN kódem. Vysoká míra zabezpečení je dána skutečností, že samotný elektronický podpis je také generován přímo v čipu Tokenu a jeho generování nelze spustit bez znalosti PIN kódu k Tokenu.

Na obrázku níže uvádím přehled nejčastěji používaných tokenů a čipových karet společnosti RSA.

Obr. 9: Přehled základních RSA SecurID tokenů, zdroj: www.emc.com.

Vysoký standard zabezpečení představuje klientský **certifikát na čipové kartě**. V čipové kartě je bezpečně uložen tajný osobní klíč klienta a každá zpráva od klienta bance je tímto klíčem přímo v kartě podepsána (tedy doplněna o unikátní kód, který je odvozen z obsahu zprávy a tajného klíče). Tajný osobní klíč klienta nelze z karty nijak získat ani uhodnout, proto bez této karty není možné elektronický podpis klienta padělat. Banka přijme zprávu od klienta jen po ověření elektronického podpisu podle certifikátu, který klientovi ke kartě vydala.

4.2.6 Jiné formy zabezpečení

V souvislosti se stále se rozvíjejícími možnostmi a růstem uživatelů internetového bankovnictví banky přicházejí s řadou konceptů a modelů jak ještě zvýšit zabezpečení přístupu k účtu, aniž by to významně ovlivnilo funkčnost a uživatelskou přívětivost. Systémy internetového bankovnictví obsahují také řadu doplňkových funkcí pro posílení bezpečnosti.

Již při samotném přihlášení nabízejí vybrané banky možnost napsat své heslo místo na běžné klávesnici na tzv. **elektronické (grafické) klávesnici**. Klávesnici v tom případě vidíte na obrazovce počítače a jednotlivé znaky vybíráte myší. Tím se zabezpečíte proti speciálním pirátským programům, které dokážou sledovat, jaké znaky „zadáváte“ na klávesnici při přihlašování do internetového bankovnictví.

Na následujícím obrázku je uvedena grafická klávesnice České spořitelny.

Obr. 10: Přihlašovací stránka České spořitelny, zdroj: www.csas.cz

Zajímavým způsobem je i přístup k zamezení operací s účtem u ING. V případě jejich bezhotovostního ING Konta klient při založení konta přesně vepíše čísla účtů, na které bude možné peníze převádět. Změna těchto údajů je pak možná pouze dodatkem smlouvy s využitím podpisového vzoru případně osobně s ověřením totožnosti. I když tedy ING využívá pro zabezpečení svého účtu pouze PID, PIN a heslo, přístup k účtu

útočníkovi umožní zaslání účtů předem definovaných, a není tedy možné peníze poslat na jakýkoliv jiný účet.

4.3 Dotazník spokojenosti klientů se zabezpečením

Vytvořil jsem dotazník spokojenosti klientů se zabezpečením elektronického bankovnictví. Tento dotazník byl poslán elektronicky, vybrané skupině respondentů pracujících v bankovnictví. Jedná se tedy o odbornou veřejnost, pro kterou nebylo nutné dotazník detailně specifikovat.

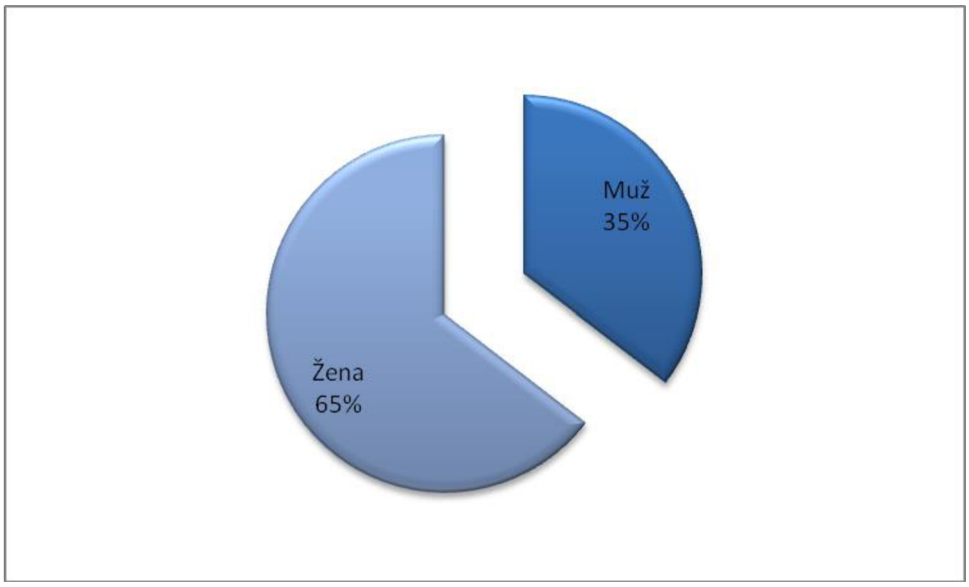
Vyhodnocení odpovědí uvádím níže. Celkový počet odpovídajících respondentů je 113.

4.3.1 Vyhodnocení odpovědí:

Tab. 7: Odpovědi na ot.: Jste?

Muž	**40**
Žena	**73**

Zdroj: autor.



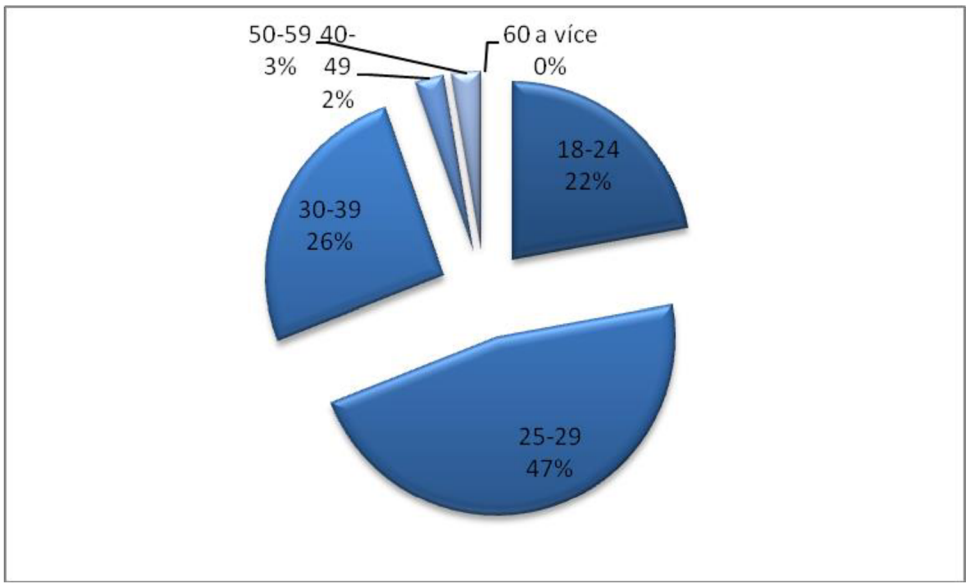
Graf 1: Vyhodnocení otázky č. 1. Zdroj: autor.

Celé dvě třetiny odpovědí byly od žen. 90 % žen využívá internetové bankovnictví aktivně. 100 % mužů využívá aktivně internetové bankovnictví.

Tab. 8: Odpovědi na ot.: Vaše věková kategorie je?

18–24	**25**
25–29	**53**
30–39	**29**
40–49	**3**
50–59	**3**
60 a více	**0**

Zdroj: autor.



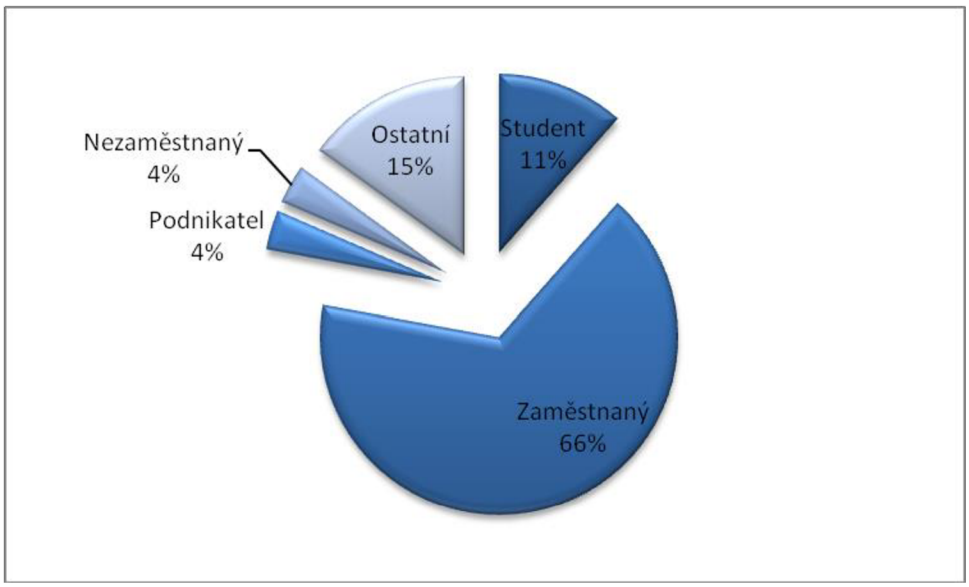
Graf 2: Vyhodnocení otázky č. 2. Zdroj: autor.

Z průzkumu vyplývá, že většina respondentů je ve věku mezi 18 a 39 lety. To může být způsobeno tím, že rozmach elektronického bankovnictví souvisí především s rozvojem internetu, který se začal rozšiřovat v posledních letech.

Tab. 9: Odpovědi na ot.: Do jaké skupiny se řadíte?

Student	**13**
Zaměstnaný	**75**
Podnikatel	**4**
Nezaměstnaný	**4**
Ostatní	**17**

Zdroj: autor.



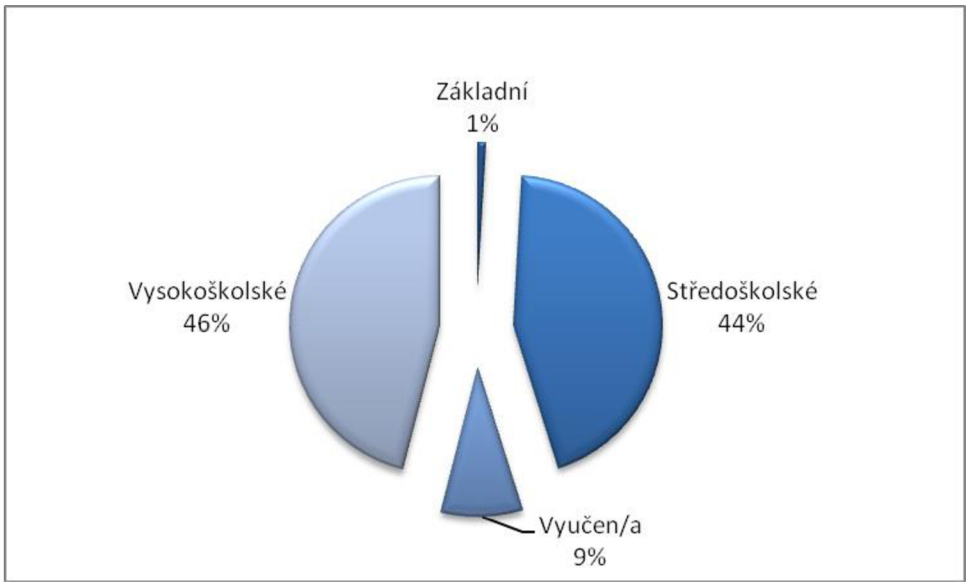
Graf 3: Vyhodnocení otázky č. 3. Zdroj: autor.

Většina respondentů je v pracovním poměru, a to celé dvě třetiny. Zhruba čtvrtina jsou studenti a ostatní. V rámci skupiny ostatní se nejčastěji objevovaly odpovědi, že jsou dotazovaní na mateřské dovolené.

Tab. 10: Odpovědi na ot.: Jaké je Vaše nejvyšší dosažené vzdělání?

Základní	**1**
Středoškolské	**50**
Vyučen/a	**10**
Vysokoškolské	**52**

Zdroj: autor.



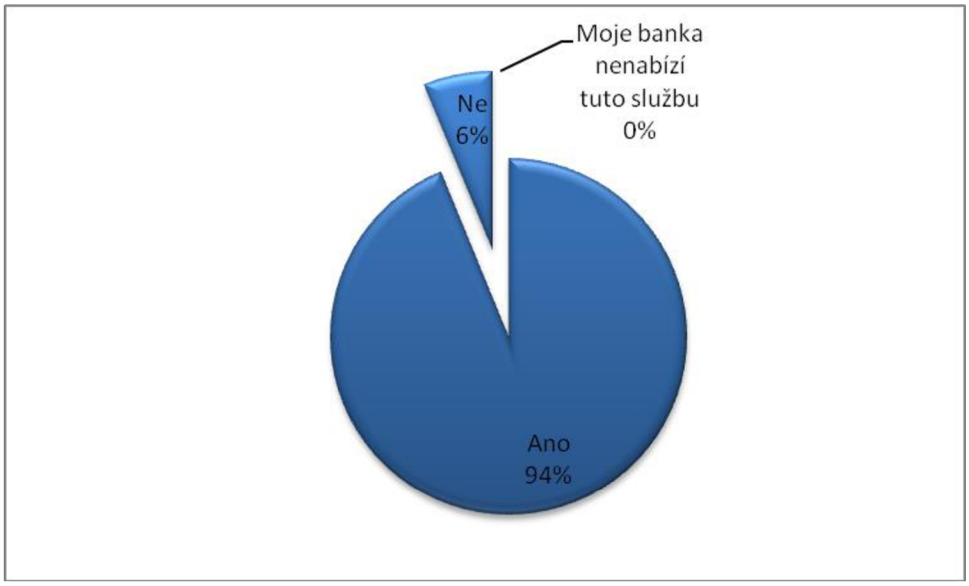
Graf 4: Vyhodnocení otázky č. 4. Zdroj: autor.

90 % respondentů má středoškolské a vysokoškolské vzdělání. Pro 70 % dotazovaných s vysokoškolským diplomem je zabezpečení velmi důležité. Stejné tomu je i u středoškoláků.

Tab. 11: Odpovědi na ot.: Využíváte elektronické bankovnictví?

Ano	**106**
Ne	**7**
Moje banka nenabízí tuto službu	**0**

Zdroj: autor.



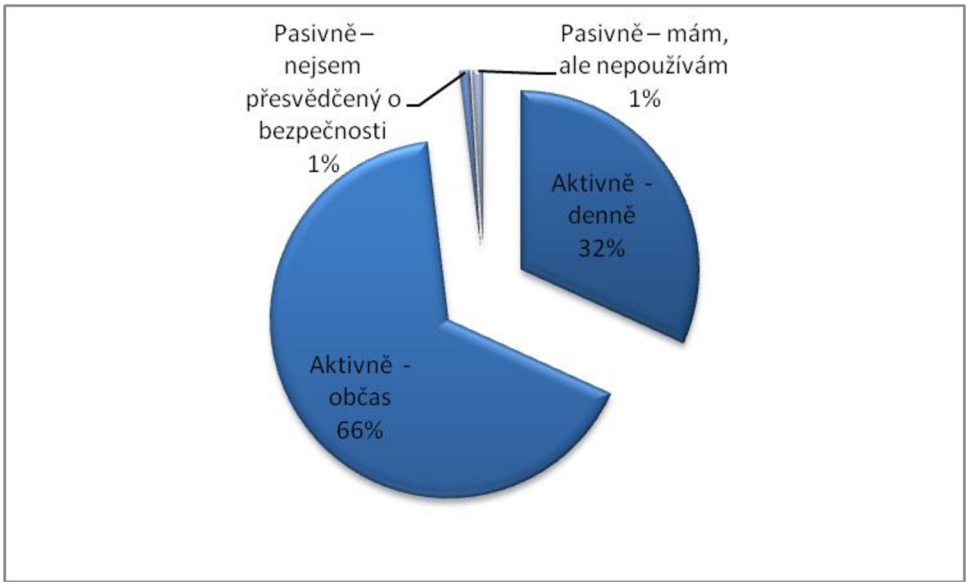
Graf 5: Vyhodnocení otázky č. 4. Zdroj: autor.

Elektronické bankovnictví využívá 94 % dotazovaných. Pouze 7 dotazovaných elektronické bankovnictví svojí banky nevyužívá. V dotazníku dále nepokračovalo pouze 5 respondentů. Nikdo neodpověděl, že jeho banka nenabízí elektronické bankovnictví. Je tedy patrné, že v dnešní době elektronické bankovnictví nabízí každá banka.

Tab. 12: Odpovědi na ot.: Jak využíváte elektronické bankovnictví?

Aktivně – denně	**34**
Aktivně – 1 x týdně	**71**
Pasivně – nejsem přesvědčený o bezpečnosti	**1**
Pasivně – mám, ale nepoužívám	**1**

Zdroj: autor.



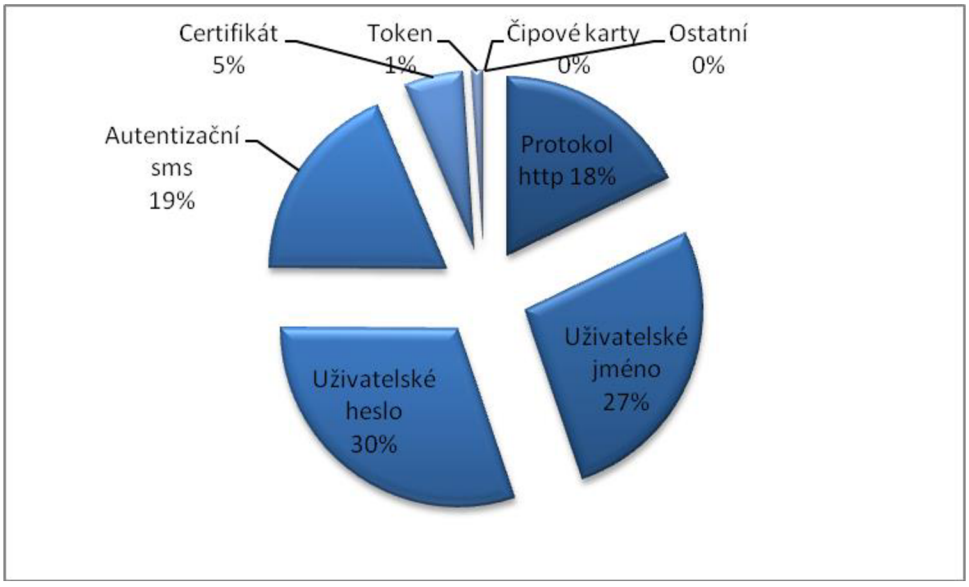
Graf 6: Vyhodnocení otázky č. 5. Zdroj: autor.

Aktivně používá elektronické bankovnictví většina lidí, celých 98 %. Méně jak jednou týdně se do el. bankovnictví přihlašuje 1 % respondentů, protože nejsou přesvědčeni o bezpečnosti el. bankovnictví. Zbylé 1 % el. bankovnictví nepoužívá.

Tab. 13: Odpovědi na ot.: Jaký typ zabezpečení Vaše banka využívá pro vstup do el. bankovnictví?

Protokol http (zabezpečení přihlašovací stránky do el. bankovnictví bankou)	**53**
Uživatelské jméno pro vstup do el. bankovnictví	**80**
Uživatelské heslo pro vstup do el. bankovnictví	**90**
Autentizační sms (pro vstup do el. bankovnictví)	**55**
Certifikát (soubor dat vytvořený bankou a uložený v PC, na USB nebo čipové kartě)	**16**
Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)	**3**
Čipové karty (nutné pro vstup a ovládání el. bankovnictví)	**0**
Ostatní	**0**

Zdroj: autor.



Graf 7: Vyhodnocení otázky č. 6. Zdroj: autor.

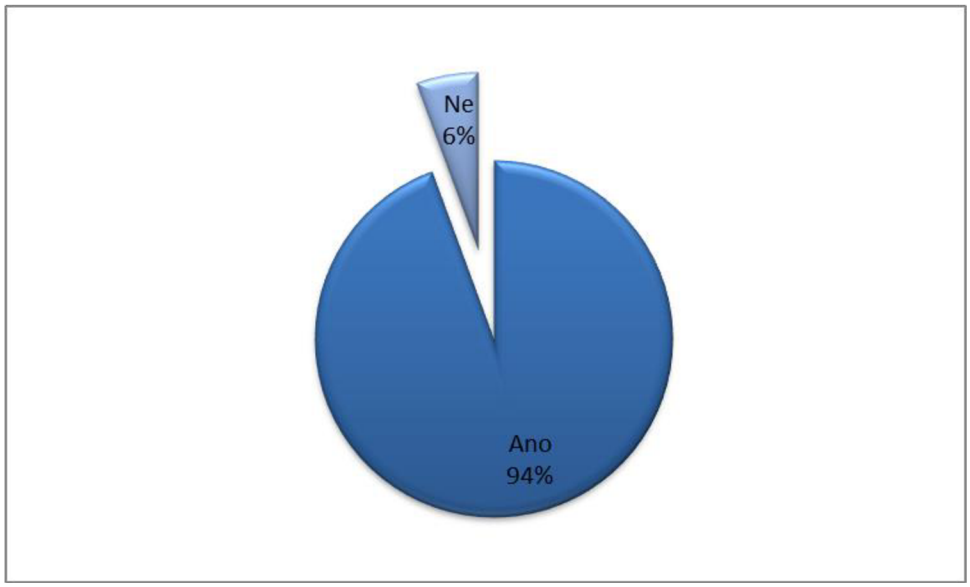
Podle uživatelů el. bankovnictví využívá jejich banka pro vstup ve většině případů uživatelské jméno a uživatelské heslo. Méně využívané jsou autentizační sms pro přihlášení.

5 % uživatelů jejich banka nabízí i certifikát pro vstup do el. bankovnictví. Téměř nevyužívané jsou Tokeny a čipové karty.

Tab. 14: Odpovědi na ot.: Je pro Vás toto zabezpečení dostačující?

Ano	**101**
Ne	**6**

Zdroj: autor.



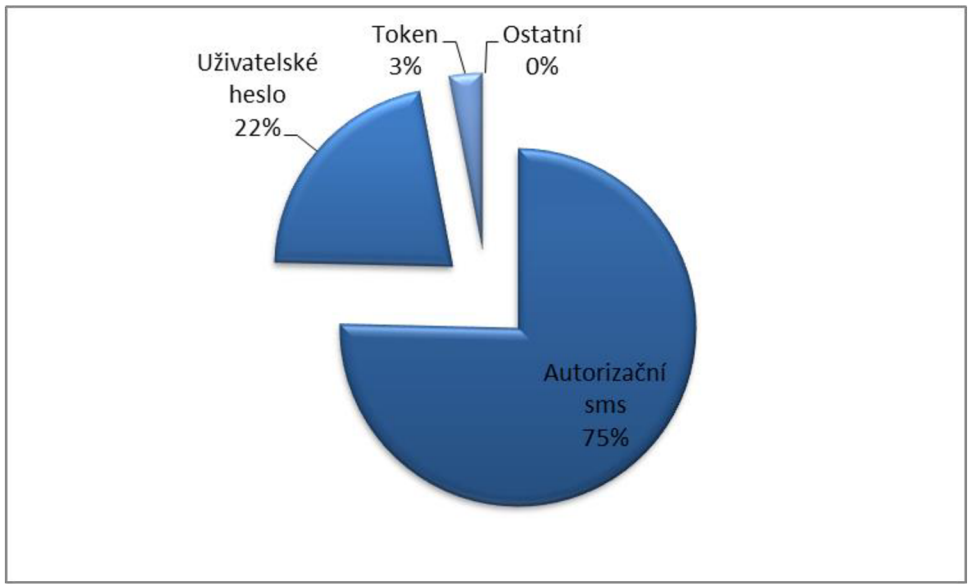
Graf 8: Vyhodnocení otázky č. 7. Zdroj: autor.

Téměř většina dotazovaných vyjadřuje spokojenost se zabezpečením vstupu do elektronického bankovnictví.

Tab. 15: Odpovědi na ot.: Jaký typ zabezpečení Vaše banka využívá pro potvrzení plateb?

Autorizační sms (pro ověření transakce)	**101**
Uživatelské heslo pro potvrzení platby	**29**
Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)	**4**
Ostatní	**0**

Zdroj: autor.



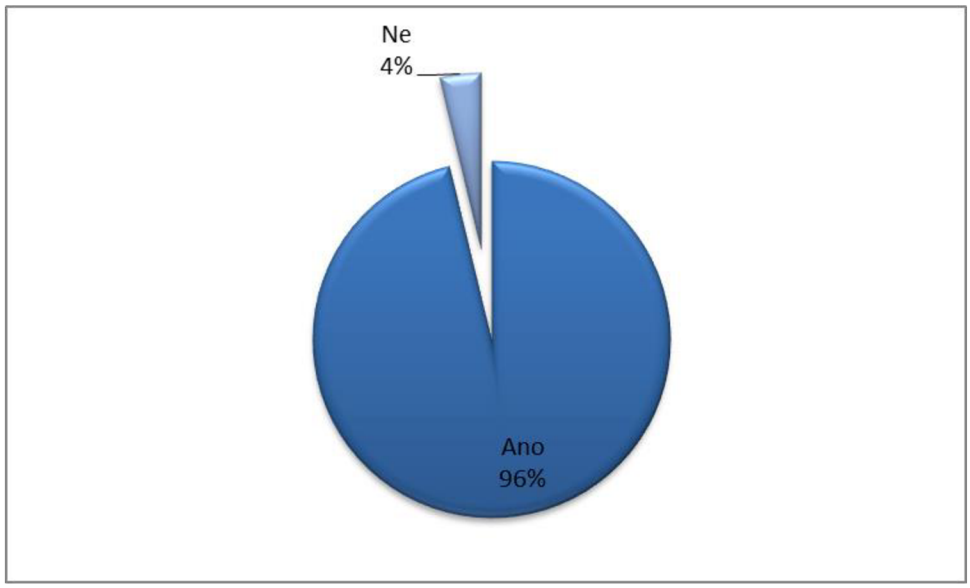
Graf 9: Vyhodnocení otázky č. 8. Zdroj: autor.

Nejvíce využívaným prvkem pro potvrzení plateb jsou autorizační sms. Uživatelské heslo pro potvrzení je využíváno u 29 respondentů. Z dotazníku vyplývá, že ve 26 případech jsou současně využívány obě formy zabezpečení. Žádný jiný zabezpečovací prvek pro ověření el. transakce respondenti neuvedli.

Tab. 16: Odpovědi na ot.: Je pro Vás toto zabezpečení dostačující?

Ano	**107**
Ne	**4**

Zdroj: autor.



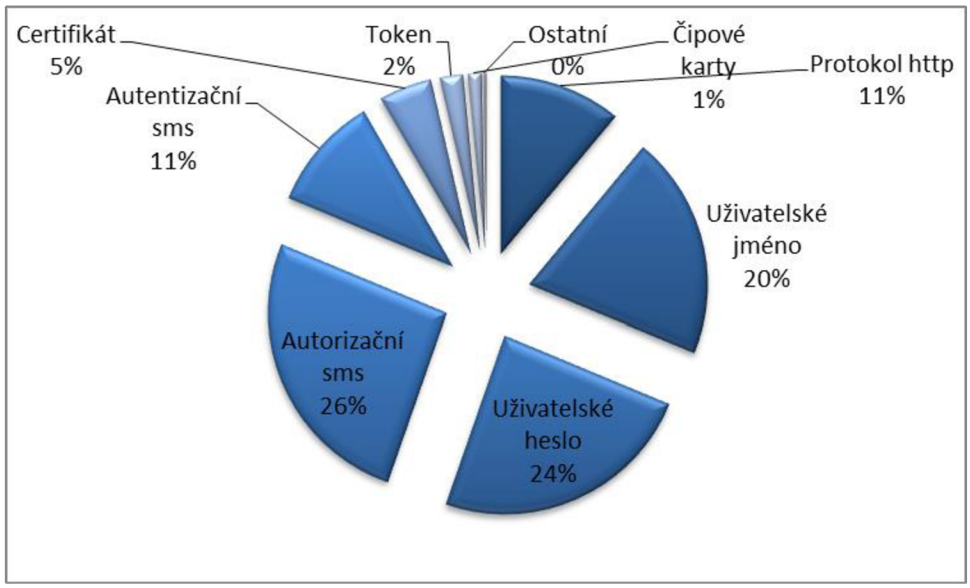
Graf 10: Vyhodnocení otázky č. 9. Zdroj: autor.

Znovu se potvrdilo, že pro téměř všechny je zabezpečení dostačující.

Tab. 17: Odpovědi na ot.: Jaký typ zabezpečení je pro Vás důležitý?

Protokol http (zabezpečení přihlašovací stránky do el. bankovnictví bankou)	**37**
Uživatelské jméno pro vstup do el. bankovnictví	**68**
Uživatelské heslo pro vstup do el. bankovnictví nebo pro potvrzení platby	**81**
Autorizační sms (pro ověření transakce)	**87**
Autentizační sms (pro vstup do el. bankovnictví)	**35**
Certifikát (soubor dat vytvořený bankou a uložený v PC, na USB nebo čipové kartě)	**16**
Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)	**7**
Čipové karty (nutné pro vstup a ovládání el. bankovnictví)	**4**
Ostatní	**1**

Zdroj: autor.



Graf 11: Vyhodnocení otázky č. 10. Zdroj: autor.

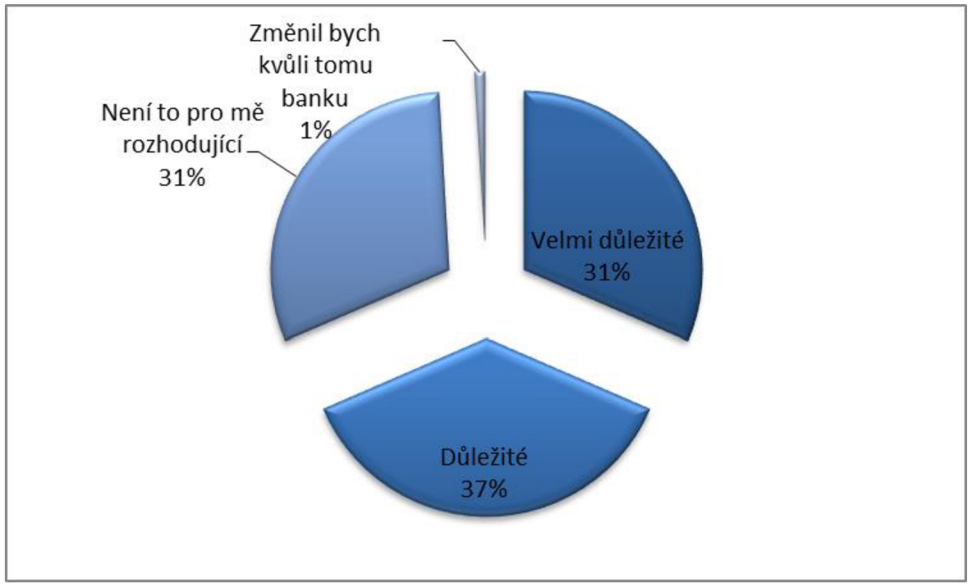
Nejdůležitějšími zabezpečovacími prvky jsou autorizační sms a uživatelské heslo, dále uživatelské jméno a autentizační sms. Nejméně důležité je zabezpečení pomocí tokenů a čipových karet.

86 % uživatelů volí kombinaci mezi uvedenými zabezpečovacími prvky. Nejčastější kombinací je uživatelské jméno a heslo samostatně a společně s ověřovacími sms zprávami.

Tab. 18: Odpovědi na ot.: Jak je pro Vás zabezpečení důležité při výběru banky?

Velmi důležité	**34**
Důležité	**40**
Není to pro mě rozhodující	**33**
Změnil bych kvůli tomu banku	**1**

Zdroj: autor.



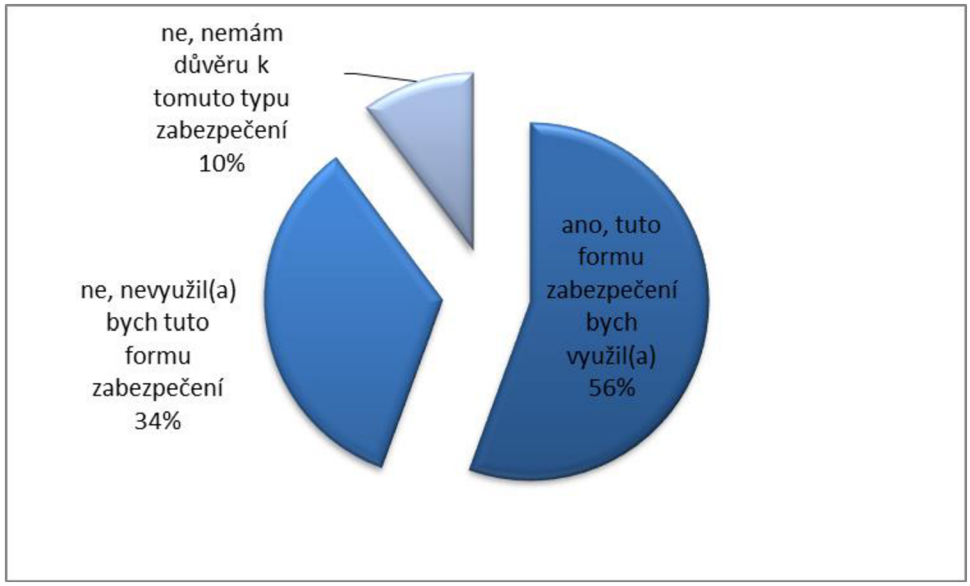
Graf 12: Vyhodnocení otázky č. 11. Zdroj: autor.

Je patrné, že pro celých 68 % je celková bezpečnost el. bankovnictví důležitá. Zbylých 32 % dává přednost i jiným faktorům při výběru banky, zabezpečení pro ně není rozhodující. Změnu banky by nikdo kvůli bezpečnosti provedl jen jeden.

Tab. 19: Vybral(a) byste si banku, která by Vám nabídla metodu otisku prstu jako formu zabezpečení?

ano, tuto formu zabezpečení bych využil(a)	**60**
ne, nevyužil(a) bych tuto formu zabezpečení	**37**
ne, nemám důvěru k tomuto typu zabezpečení	**11**

Zdroj: autor.



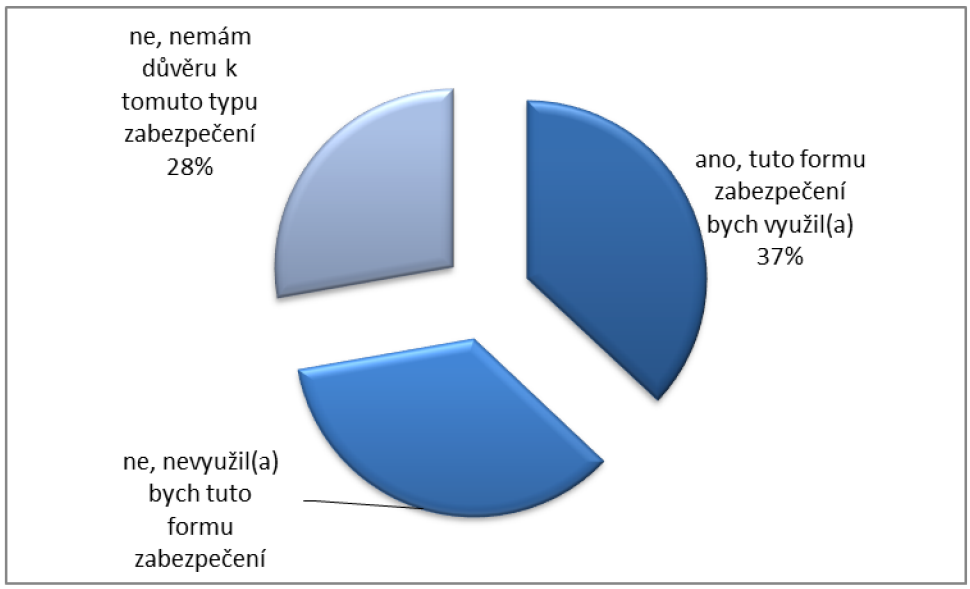
Graf 13: Vyhodnocení otázky č. 12. Zdroj: autor.

Přes polovinu dotazovaných by využilo jako další formu zabezpečení otisk prstu. Několik dotazovaných by ovšem tento typ zabezpečení nejraději využilo s pomocí např. mobilního telefonu, tedy bez použití dalších speciálních zařízení.

Tab. 20: Vybral(a) byste si banku, která by Vám nabídla metodu identifikace pomocí čipu na občanském průkazu nebo pasu jako formu zabezpečení?

ano, tuto formu zabezpečení bych využil(a)	**40**
ne, nevyužil(a) bych tuto formu zabezpečení	**38**
ne, nemám důvěru k tomuto typu zabezpečení	**30**

Zdroj: autor.



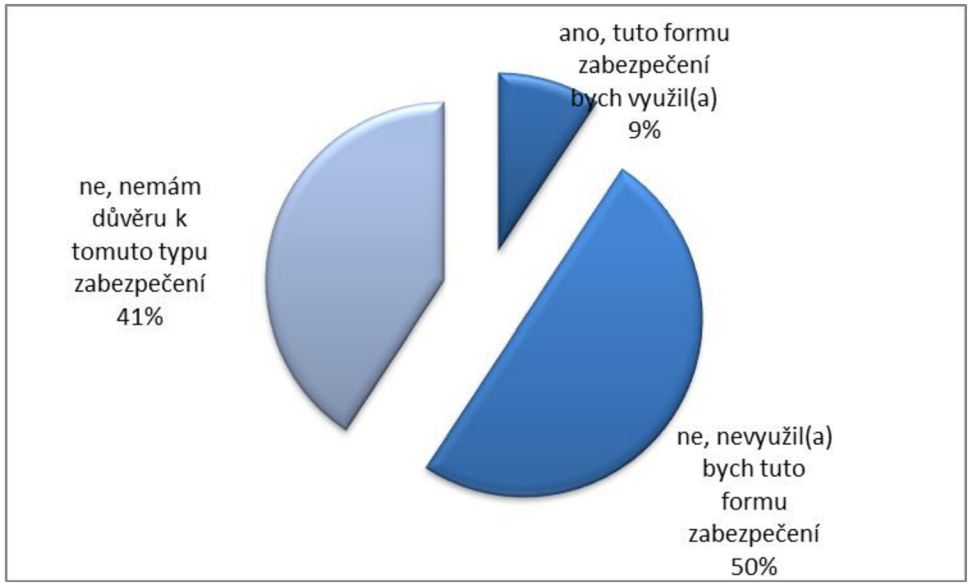
Graf 14: Vyhodnocení otázky č. 12. Zdroj: autor.

U této otázky je míra využití menší. Metodu identifikace pomocí čipu na občanském průkazu by využila zhruba třetina dotazovaných. Zbylé dvě třetiny by tuto formu vůbec nevyužily.

Tab. 21: Vybral(a) byste si banku, která by Vám nabídla metodu ověření pomocí rozpoznávání hlasu jako formu zabezpečení?

ano, tuto formu zabezpečení bych využil(a)	**10**
ne, nevyužil(a) bych tuto formu zabezpečení	**54**
ne, nemám důvěru k tomuto typu zabezpečení	**44**

Zdroj: autor.



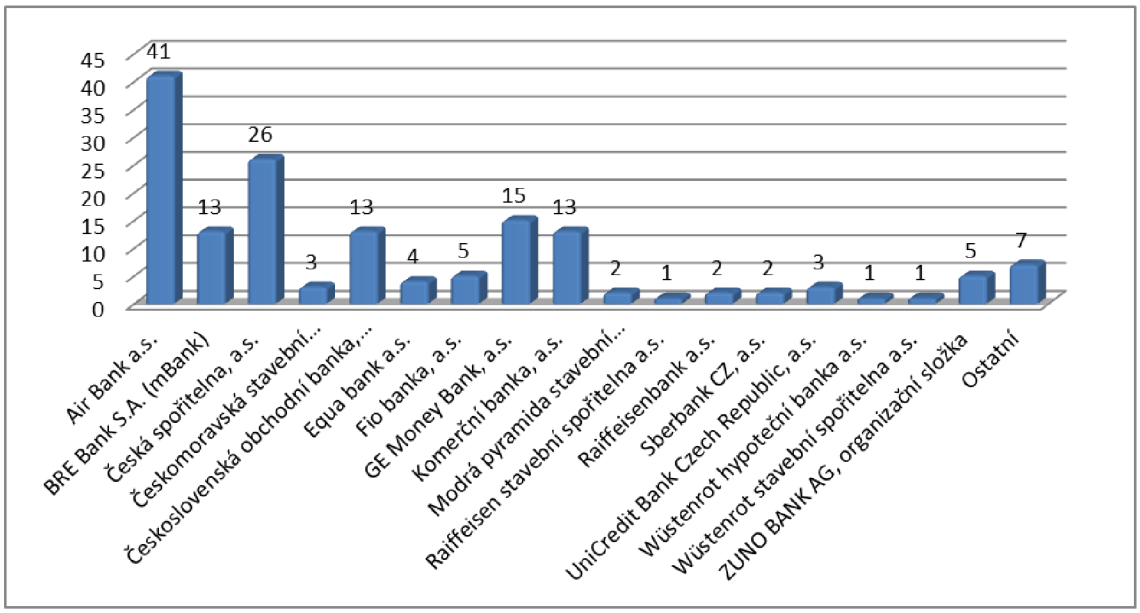
Graf 15: Vyhodnocení otázky č. 12. Zdroj: autor.

Celých 91% respondentů by nevyužilo tuto metodu. Může to být i způsobeno tím, že neznají proces rozpoznávání hlasu a jeho bezpečnostní prvky. Tento proces je zatím nejméně využívaný všeobecně.

Tab. 22: Odpovědi na ot.: Jakou banku nyní využíváte?

Air Bank a.s.	**41**
BRE Bank S. A.	**13**
Citibank Europe plc, organizační složka	**0**
Česká spořitelna, a.s.	**26**
Českomoravská stavební spořitelna, a.s.	**3**
Československá obchodní banka, a.s.	**13**
Equa bank, a.s.	**4**
Evropsko-ruská banka, a.s.	**0**
Fio banka, a.s.	**5**
GE Money Bank, a.s.	**15**
Hypoteční banka, a.s.	**0**
Komerční banka, a.s.	**13**
LBBW Bank CZ, a.s.	**0**
Modrá pyramida stavební spořitelna, a.s.	**2**
Oberbank AG – pobočka Česká republika	**0**
Raiffeisen stavební spořitelna, a.s.	**1**
Raiffeisenbank, a.s.	**2**
Raiffeisenbank im Stiftland eG pobočka Cheb, odštěpný závod	**0**
Sberbank CZ, a.s.	**2**
Stavební spořitelna České spořitelny, a.s.	**0**
UniCredit Bank Czech Republic, a.s.	**3**
Waldviertler Sparkasse Bank AG	**0**
Wüstenrot hypoteční banka, a.s.	**1**
Wüstenrot stavební spořitelna, a.s.	**1**
ZUNO BANK AG, organizační složka	**5**
Ostatní	**7**

Zdroj: autor.



Graf 16: Vyhodnocení otázky č. 13. Zdroj: autor.

Nejvíce respondentů využívá nové banky jako Air Bank a mBank. Z dotazníku dále vyplývá, že velké banky jako Česká spořitelna, Ge Money bank a Komerční banka jsou klienty používané. Může to být i z toho důvodu, že nové banky si na elektronickém bankovnictví zakládají a bezpečnost je u nich na vysoké úrovni. 35 uživatelů má kombinaci více bank i kvůli rozložení bezpečnosti.

Zajímavosti plynoucí z dotazníku

Zajímavé je, že pouze 46 % uživatelů odpovědělo, že jejich banka využívá protokol https k zabezpečení přihlašovací stránky do elektronického bankovnictví. Toto zabezpečení ovšem využívají všechny banky. Z toho vyplývá, že většina uživatelů neví, jaké formy zabezpečení jim banka nabízí.

Zajímavé je, že všechny 3 formy nového zabezpečení by si vybrali pouze 2 dotazovaní. Právě jednu možnost by si vybralo 40 % všech respondentů. Naopak 27 % dotazovaných by si nevybralo žádnou novou formu zabezpečení. Z hlediska nedůvěry se jedná o 38 % lidí, kteří vyjádřili nedůvěru ve zmiňované nové formy zabezpečení.

Z výše uvedeného vyplývá, že i když banky nabízí různé formy zabezpečení, tak o nich uživatelé ve většině případů nevědí nebo je nevyužívají. Otázkou tedy je, zda je z pohledu banky přínosné vynaložit prostředky na rozvoj zabezpečení elektronického bankovnictví, když by jej klienti ani nevyužili.

14 % uživatelů, pro které není zabezpečení elektronického bankovnictví důležité, by si vybralo alespoň jednu formu nového zabezpečení.

5 Vlastní návrhy řešení

5.1 Další metody zabezpečení

V této části práce navrhuji možnosti zabezpečení, které se zatím v sektoru bankovnictví nevyskytují nebo jen minimálně. Jedná se především o technologie ověřující totožnost klienta a pomáhající jednoznačnější identifikaci klienta. Tyto technologie jsou dnes již běžně dostupné a využívané v jiných sektorech.

5.1.1 SignPad

České banky se učí využívat biometrické údaje. Zatím nelze hovořit o skenování sítnice oka či snímání otisku prstu, ale „pouze“ o zaznamenávání klientova podpisu. Jako první tuto technologii začala při svém vstupu na trh používat Air Bank, nyní se k ní přidává i jedna z větších bank – GE Money Bank.

Výhoda využití biometrických podpisů je jasná – zákazníci z banky nebudou odcházet s deskami plnými papírů, ale všechny dokumenty v plném znění včetně dodatků najdou kdykoliv online ve svém internetovém bankovnictví. „Každý sedmý klient musel kvůli ztrátě smlouvy žádat o její kopii. To bude brzy minulostí, protože všechny dokumenty najdou zákazníci během pár kliknutí,“ dodal Štěpán Pittauer, projektový manažer GE Money Bank. (PITTAUER, 2014)

Pro pořízení biometrického podpisu je potřeba, aby se klient podepsal na takzvaném SignPadu. Pro správné vyhodnocení a uložení potřebných biometrických údajů je potřeba takových podpisů šest. Napodobit standardní biometrický podpisový vzor je prakticky nemožné. Podpis navíc nelze použít na jiném dokumentu, protože by se neshodovala časová razítka podpisu a dokumentu. (SCHWARZMANN, 2014)

Obr. 11: Singpad, zdroj: www.svethardware.cz.

Co kdyby ale klient podepisoval dokument elektronicky? V tomto případě připraví pracovník banky dokument smlouvy k podpisu a klient jej podepíše prostřednictvím speciálních modulů. Jako modul si lze představit tablet, na kterém je viditelný text smlouvy a řádek k podpisu, který klient podepíše perem se speciálním hrotem. Dokument může okamžitě putovat k oprávněné osobě, vzdálené třeba i stovky kilometrů daleko, k elektronickému podpisu za banku. Z pohledu obsluhy jsou rozhodující efektivita, rychlost, a tím pádem i produktivita. Pokud se zvyšují tyto parametry, je obsluha spokojená, protože plní svá kritéria, podle nichž je hodnocena. A co může být pro banku výhodnější než spokojený klient, kterého obsluhuje spokojený personál – a navíc v rámci navazujících procesů dochází ke snížení nákladů a časové náročnosti jednotlivých operací. Dalšími výhodami jsou již jen takové „drobnosti“ jako snížení rizik spojených s jednoznačnou identifikací osob, posílení prevence proti falšování identit a neoprávněným změnám obsahu dokumentů.

A jak jsme na tom v porovnání se světem? V Asii či Americe existují různá řešení využívající více či méně tento koncept. A s dalším rozvojem potřebných technologií přichází na trh stále více firem, které nabízejí buď přímo balíkové řešení, nebo na míru postavený projekt, který využívá stejné či podobné prvky. Existují již i první implementace této technologie ve střední a východní Evropě. Příkladem za všechny je slovenská Tatra banka, která využívá na svých pobočkách digitalizované podpisy. A k úplnému nahrazení papírových tisků nemají daleko internetové banky jako ZUNO či Air Bank. (VERECKÝ, 2013)

Jak to funguje z hlediska legislativy?

Dynamický biometrický podpis je akceptován se stejnou právní validitou jako podpis kvalifikovaným certifikátem. Z hlediska komunitárního práva je určujícím předpisem direktiva 1999/93/EC. Elektronický podpis je tam definován dostatečně obecně tak, že zahrnuje i dynamický biometrický podpis.

Z hlediska českého práva je klíčovým zákonem 227/2000 Sb., o elektronickém podpisu. Podle paragrafu 2 tohoto zákona jsou elektronickým podpisem *"údaje v elektronické podobě, které jsou připojené k datové zprávě, nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. Tato definice zahrnuje i dynamický elektronický podpis.*

5.1.2 Technologie snímače otisků prstů

Senzor se skládá ze dvou hlavních částí, tj. zdroj světla a zobrazovací systém. Tyto systémy využívají více osvětlovacích soustav o rozdílných vlnových délkách. Světlo pak projde pod povrch kůže, tím pádem senzor umožňuje shromáždit více identifikačních údajů z prstu.

Na obrázku níže uvádím multispektrální zobrazovací technologii společnosti Lumidigm, která je schopna snímat a zpracovat vlastnosti prstu i pod povrchem kůže.

Obr. 12: Multispektrální obraz od společnosti Lumidigm, zdroj: www.comfis.cz.

Multispektrální biometrické snímače

Multispektrální zobrazovací technologie je schopna snímat a zpracovat vlastnosti prstu i pod povrchem kůže. Senzor se skládá ze dvou hlavních částí, kterými jsou zdroj světla a zobrazovací systém. Tyto systémy využívají více osvětlovacích soustav o rozdílných vlnových délkách. Světlo projde pod povrch kůže a senzor umožní shromáždit více identifikačních údajů z prstu.

- **Extrémní podmínky prostředí**

Multispektrální technologie může spolehlivě fungovat za extrémních podmínek okolního prostředí (stříkající a tekoucí voda, vliv okolního světla, apod.), což u standardně používaných technologií způsobuje velké problémy.

- **Nevýrazné otisky**

U některých osob se může stát, že jejich otisky jsou nevýrazné, tj. pokud rozdíly mezi "hřebeny" a "údolími" otisku prstu jsou minimální, nebo jsou zaneseny špínou.

Může se tedy stát, že potřebné identifikační údaje z otisku budou neúplné a tudíž nepoužitelné. Multispektrální technologie je schopna tento obraz z otisku dotvořit, a tudíž zabránit odmítnutí identifikace.

- **Slabé stisknutí prstu**

Při slabém stisknutí dochází u běžných snímačů k odmítnutí identifikace z důvodů malého počtu potřebných údajů. Multispektrální technologie však dokáže dotvořit přesný obraz otisku, což řeší problém s potenciálně zamítnutou identifikací.

- **Detekce proti útoku**

Tradiční snímače nejsou vždy plně spolehlivé a lze je s určitou pravděpodobností obejít. Existují mnohé materiály, ze kterých je možno vytvořit umělý otisk prstu, který bude mít stejný tvar papilárních linií, jako u jiné osoby.

Multispektrální technologie založená na spektrální analýze obrazu používá více vlnových délek světla k identifikaci otisku. Ty snímají biometrické údaje i pod povrchem kůže a tím zabraňují neoprávněné osobě s falešným otiskem správné identifikaci pod jiným uživatelským účtem. Technologie tak umožňuje rozpoznat otisk živé či mrtvé osoby a jiných organických a syntetických materiálů.

Multispektrální technologie dokáže odhalit i situaci, kdy má identifikovaná osoba na svém otisku prstu nanesenou tenkou vrstvu, na které je otisk cizí osoby. Při přitlačení otisku k senzoru dochází v tomto místě prstu k odkrvení. Toto odkrvení je snímačem, který snímá i údaje pod povrchem otisku, detekováno a lze pak jednoduše určit, jestli jde o skutečný otisk nebo o falsifikát.

Propočet nákladů pro čtečku otisků prstů

Pro ukázku jsem zvolil čtečku otisků prstů iEvo, která má, dle mého názoru potřebnou specifikaci z hlediska bezpečnosti pro ověření klientů. Na obrázku 13 uvádím registrační biometrickou čtečku otisků prstů iEvo.

Obr. 13:Biometrická čtečka otisků prstů iEvo s USB, zdroj: www.tzk-sro.cz.

Biometrická čtečka otisků prstů iEvo s USB výstupem pro rychlou registraci prstů u PC. Pořizovací cena 18 500 Kč s DPH. Podrobnosti a specifikace čtečky uvádím v tabulce níže.

Tab. 23: Specifikace čtečky otisků prstů iEvo

Biometrická technologie	otisk prstu
Technologie snímače	optická multispektrální
Ověřované prvky	pouze prst
Vestavěná čtečka	ne
Kapacita paměti vzorů	--
Připojení k PC	USB
Software pro správu	iEvo SW (v dodávce čtečky)
Napájecí napětí	5 Vss
Odběr	500 mA
Výstup	USB
Pracovní teplota	-10 - 50° C
Použití v exteriéru	ne
Rozměry – výška	100 mm
Rozměry – šířka	83 mm
Rozměry – hloubka	50 mm

Zdroj: www.tzk-sro.cz

Kalkulace pořizovacích nákladu čtečky otisků prstů pro Air Bank:

Tab. 24: Pořizovací náklady na čtečku iEVO pro Air bank:

Pořizovací náklady čtečky otisků prstů pro Air bank		
cena v Kč	počet kusů	částka
18 500	250	4 625 000

Zdroj: autor.

Metoda propočtu pořizovacích nákladu čtečky otisků prstů pro Air Bank:

- cena biometrické čtečky otisku prstů iEvo je 18 500 Kč s DPH
- počet 10 kusů čtečky na jednu pobočku krát 25 poboček aktuální stav k 30.6. 2014
- kalkulace uvedena v tabulce č.24

Tab. 25: Doba návratnosti investice pro Air bank:

Doba návratnosti pro Air bank								
	zisk na 1 klienta v Kč	počet klientů	zisk	zvýšení rok	zvýšení den	návratnost		
aktuální stav	517	300 000	155 100 000	0		dny	měsíc	rok
zvýšení o 1%	517	303 000	156 651 000	1 551 000	4 249	1 088	36	3
zvýšení o 3%	517	309 000	159 753 000	4 653 000	12 748	363	12	1
zvýšení o 5%	517	315 000	162 855 000	7 755 000	21 247	218	7	1
zvýšení o 7%	517	321 000	165 957 000	10 857 000	29 745	155	5	0,4
zvýšení o 10%	517	330 000	170 610 000	15 510 000	42 493	109	4	0,3
zvýšení o 56%	**517**	**468 000**	**241 956 000**	**86 856 000**	**237 962**	**19**	**1**	**0,1**

Zdroj: autor.

Metoda propočtu doby návratnosti:

- zisk na 1 klienta je vypočten jako celkový zisk banky (výnosy – náklady) dělený počtem klientů
- návratnost je vypočtená jako čas, za jak dlouho zvýšení zisku pokryje pořizovací náklady, vypočteno na dny a měsíce, roky a dny
- zisk a počet klientů jsou údaje zjištěné z veřejně dostupných dat
- zvýšení počtu klientů o 1 %, 3 %, 5 %, 7 % a 10 % jsou odhady pro přehlednost, jak by se vyvíjela návratnost počáteční investice při těchto úrovních přílivu nových klientů
- zvýšení počtu klientů o 56 % vyplývá z dotazníku, kde 56 % dotazovaných kladně odpovědělo na využití této technologie
- propočet uveden v tabulce č. 25 a stejný propočet je použitý v tabulce č. 27

Kalkulace pořizovacích nákladu čtečky otisků prstů pro Českou spořitelnu:

Tab. 26: Pořizovací náklady na čtečku iEVO pro Českou spořitelnu:

Pořizovací náklady čtečky otisků prstů pro Českou spořitelnu		
cena v Kč	počet kusů	částka
18 500	6 530	120 805 000

Zdroj: autor.

Metoda propočtu pořizovacích nákladu čtečky otisků prstů pro Českou spořitelnu:

- cena biometrické čtečky otisku prstů iEvo je 18 500 Kč s DPH
- počet kusů 10 kusů čtečky na jednu pobočku krát 653 poboček aktuální stav k 31.12. 2013
- kalkulace je uvedena v tabulce č. 26

Tab. 27: Doba návratnosti investice pro Českou spořitelnu:

Doba návratnosti pro Českou spořitelnu								
	zisk na 1 klienta v Kč	počet klientů	zisk	zvýšení rok	zvýšení měsíc	návratnost		
aktuální stav	2119	5 300 000	11 230 700 000			dny	měsíc	rok
zvýšení o 1%	2119	5 353 000	11 343 007 000	112 307 000	307 690	393	13,1	1,1
zvýšení o 3%	2119	5 459 000	11 567 621 000	336 921 000	923 071	131	4,4	0,4
zvýšení o 5%	2119	5 565 000	11 792 235 000	561 535 000	1 538 452	79	2,6	0,2
zvýšení o 7%	2119	5 671 000	12 016 849 000	786 149 000	2 153 833	56	1,9	0,2
zvýšení o 10%	2119	5 830 000	12 353 770 000	1 123 070 000	3 076 904	39	1,3	0,1
zvýšení o 56%	**2119**	**8 268 000**	**17 519 892 000**	**6 289 192 000**	**17 230 663**	**7**	**0,2**	**0**

Zdroj: autor.

Výpočet rentability investice

Na základě vzorce pro výpočet rentability investice spočítám rentabilitu pro obě banky. Vzorec pro výpočet je:

ROI = Zisk / pořizovací náklady

Tab. 28: Výpočet rentability pro čtečku otisků prstů:

	zisk	počáteční investice	ROI
Air bank	155 100 000	4 625 000	**34**
Česká spořitelna	11 230 700 000	120 805 000	**93**

Zdroj: autor.

Z tabulky vyplývá, že je rentabilita investice vyšší pro Českou spořitelnu. Tento propočet jen potvrzuje fakt, že je i doba návratností kratší pro Českou spořitelnu.

Vliv nových klientů na vývoj zisku

Podle statistických dat České národní banky mají všechny české domácnosti založených 11,7 milionů účtů u tuzemských bank. Za předpokladu dotazníkového šetření jako reprezentativního vzorku, by tuto formu zabezpečení využilo 56 % dotazovaných. To by znamenalo 6 552 000 nových klientů. Kalkulaci zvýšení zisku, pro jednu i druhou banku, při zvýšení počtu klientů o tuto částku uvádím v tabulce č. 29.

Tab. 29: Vliv nových klientů na vývoj zisku u čtečky otisků prstů:

banka	zvýšení o 56%	zisk na 1 klienta v Kč	počet klientů	zisk	% zvýšení zisku
Air bank	6 552 000	517	6 852 000	3 542 484 000	2 284
Česká Spořitelna	6 552 000	2 119	11 852 000	25 114 388 000	224

Zdroj: autor.

Na základě této úvahy, kdy by si každá z bank ukrojila z celkového trhu stejný díl, při implementaci čtečky občanských průkazů, je patrné, že pro Air bank je procentuální zvýšení zisku zásadnější a 10 krát vyšší než u České spořitelny. Zároveň můžeme předpokládat, že pokud by v takovém množství přešla část trhu k jedné bance, tak by to mělo i za důsledek poklesu klientů druhé banky.

Výpočet regresní analýzy

V této části graficky zobrazím vliv investice na vývoj zisku. Souvislost mezi proměnnými je vyjádřená modelem, v kterém vystupují dva druhy proměnných. Proměnné nezávislé (regresory) se většinou značí x_1, x_2, • • •, x_n a závislé proměnné (regresanty) se značí y_1,y_2,... ,y_n. Ve výpočtech jsme použili n = 4.

Pro výpočty byly použity následující vzorce:

Aritmetický průměr:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

$$\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$$

Odhad regresní přímky:

$$b_2 = \frac{n\sum_{i=1}^{n} x_i\, y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} x_i}$$

$$b_1 = \bar{y} - b_2\bar{x}$$

$$\tilde{\mu}(x) = b_1 + b_2 x$$

Tyto výpočty a vzorečky byly použity v celé této kapitole i v kapitole 5.1.3 výpočtu regresní přímky pro čtečku čipu na občanském průkazu.

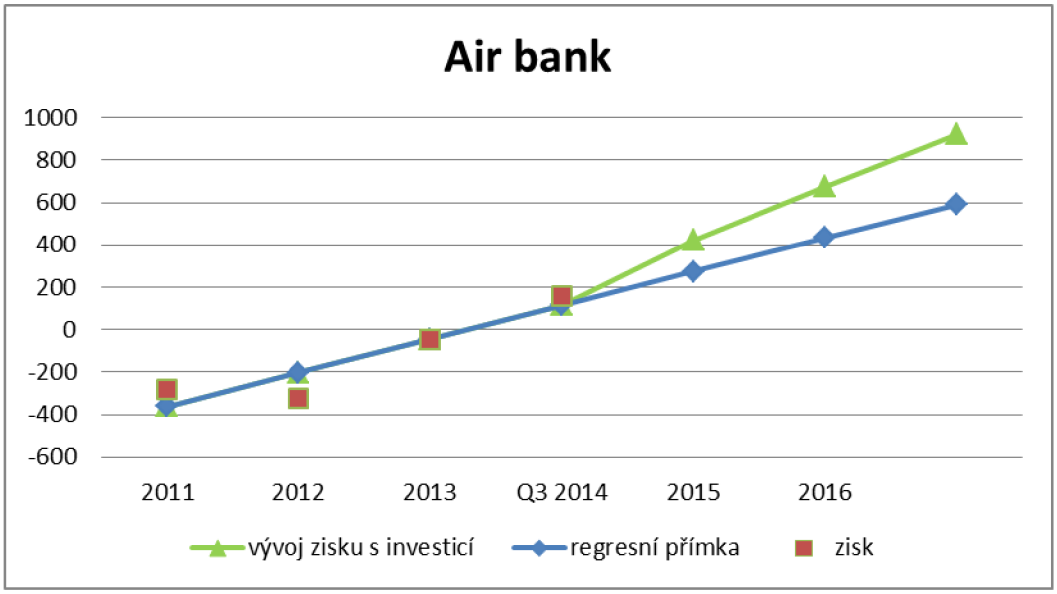
V následující tabulce č. 30 je zobrazen výpočet pro určení regresní přímky. Jako výchozí data používám zisk Air bank a České spořitelny za roky 2011 – 2014. Prognóza je dále vypočítaná na 3 roky (do roku 2017).

Tab. 30: Výpočet regresní přímky pro Air bank:

Air bank							
x=pořadí roku	1	2	3	4	5	6	7
rok	2011	2012	2013	Q3 2014	2015	2016	2017
y = zisk	-282	-323	-45	155			
reg. přímka	-362,1	-203,2	-44,3	114,6	273,5	432,4	591,3
zvýšení o 56 %					**423**	**675**	**922**

Údaje jsou uvedeny v mil. Kč, zdroj: autor.

Níže zobrazuji regresní přímku pro Air bank graficky, v porovnání s investicí.



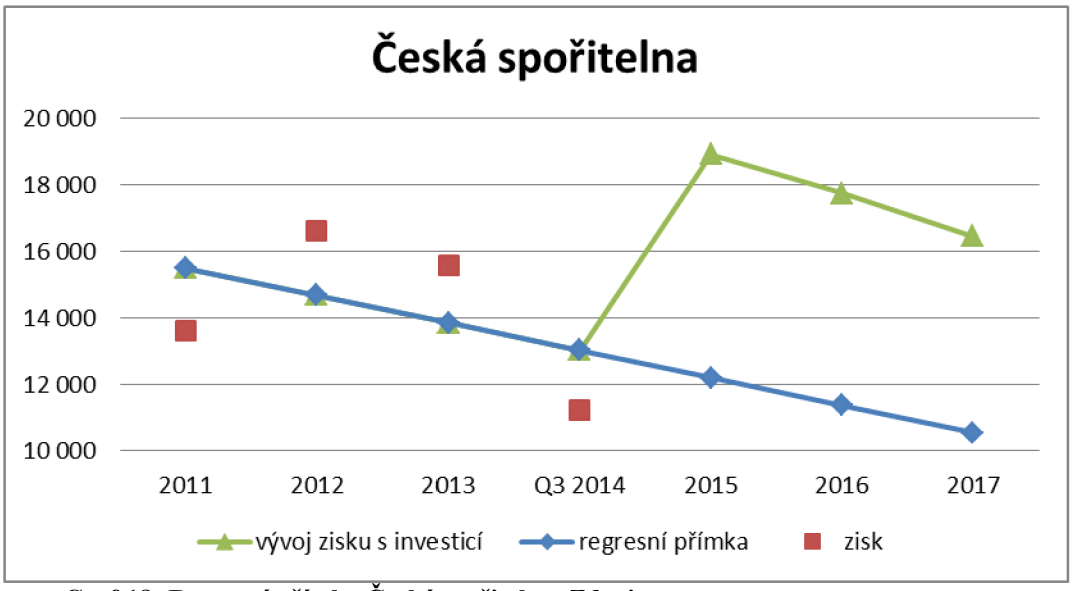
Graf 17: Regresní přímka Air bank. Zdroj: autor.

Tab. 31: Výpočet regresní přímky pro Air bank:

Česká spořitelna							
x=pořadí roku	1	2	3	4	5	6	7
rok	2011	2012	2013	Q3 2014	2015	2016	2017
y = zisk	13 638	16 612	15 588	11 230			
reg. přímka	15 504	14 679	13 855	13 030	12 205	11 380	10 555
zvýšení o 56 %					**18 919**	**17 753**	**16 466**

Údaje jsou uvedeny v mil. Kč, zdroj: autor.

Níže zobrazuji regresní přímku pro Českou spořitelnu graficky, v porovnání s investicí.



Graf 18: Regresní přímka České spořitelny. Zdroj: autor.

Závěr:

Metoda ověření klienta pomocí otisku prstu je jednou ze základních biometrických metod. Tato metoda je už využívaná v jiných institucích, kde je ochrana věcí a dat velmi důležitá. Díky tomu jsou již známé všechny výhody a nevýhody této metody. Proto by použití pro banku mělo být velkým přínosem z hlediska bezpečnosti.

Pro srovnání jsem vybral 2 banky. Relativně novou (3 roky na trhu) Air Bank a stálici na trhu Českou spořitelnu. Každá z těchto bank má tedy rozdílné pořizovací náklady, rozdílný zisk z 1 klienta, rozdílný počet klientů a pro každou banku má implementace těchto zařízení jiný přínos. Pro srovnání jsem použil pouze počáteční náklady na pořízení zařízení, které mohu jednoznačně vyčíslit pro každou banku. Samozřejmě je třeba zahrnout i další náklady, jako např. na instalaci zařízení, ovládací software a mzdu pracovníků, kteří budou zařízení uvádět do provozu. Pro Českou spořitelnu budou tyto dodatečné náklady za jisté daleko vyšší než pro Air bank s menším počtem poboček.

Z propočtů nákladů na pořízení čtečky otisku prstu je patrné, že čím větší banka s více pobočkami, tím větší počáteční investice. Zatímco pro Airbank je počáteční náklad ve výši 4,6 milionu Kč, tak pro Českou spořitelnu je to 120,8 milionu Kč. Toto je pouze náklad na pořízení čtecího zařízení. Je tedy patrné, že Česká spořitelna má

náklady 26 krát vyšší než Air bank. Co se týče počtu klientů, má Česká spořitelna oproti Air bank 17 krát více klientů a zisk na jednoho klienta pouze 4 krát vyšší.

Z pohledu rentability nákladů dané investice v porovnání se ziskem na jednoho klienta, vychází Air bank 0,3 % a České spořitelně 0,05 %. Za těchto podmínek je tedy efektivnější investice pro Air bank, i když tedy časová návratnost vychází lépe pro Českou spořitelnu. Samozřejmě je to i díky tomu, že při zvýšení počtu klientů např. o 1 % se u Air bank zvýší počet klientů o 3 000, ale o 53 000 u České spořitelny.

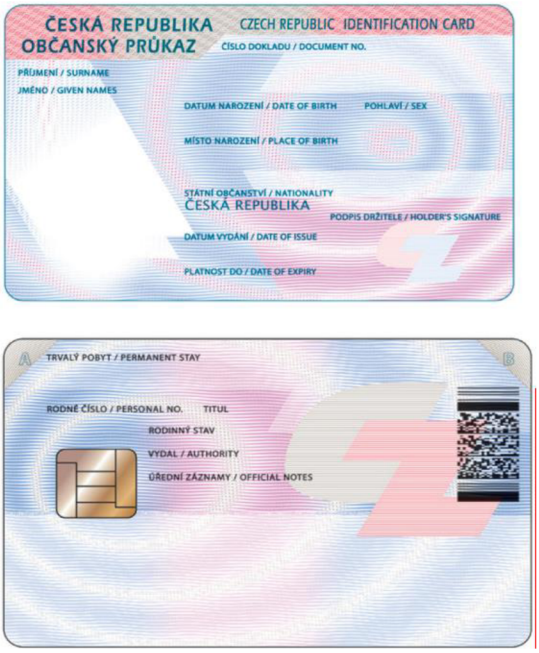
5.1.3 Čip na občanském průkazu

Od ledna 2012 se v České republice vydávají nové občanské průkazy, o tyto OP mohou žádat i občané mladší 15 let. V ČR se v této době vydávají tři typy občanských průkazů:

- Se strojově čitelnými údaji s kontaktním čipem, ve které je uloženo číslo OP a elektronický podpis. Cena těchto průkazů je 500,- Kč. Čip je založen na technologii Java Card 2.2.2. Paměť čipu je 128 kB ROM. Čip zatím uchovává pouze číslo OP a lze do něj nahrát elektronický podpis, tuto službu zajišťují akreditovaní poskytovatelé certifikačních služeb. Neoprávněný zápis dat do čipu je klasifikováno jako přestupek, za který lze uložit pokutu do 100 000,- Kč.

- Se strojově čitelnými údaji bez čipu. Výměna na starých OP za nové je zdarma, avšak pokud občan průkaz ztratí, zaplatí za nová 100,- Kč. Základní komunikace je založena na použití strojově čitelné zóny, která je ve formě 2D čárového kodu. Současně při převzetí nového občanského průkazu si občan zvolí bezpečnostní heslo PIN, které bude používat při komunikaci s informačními systémy veřejné správy. PIN kod bude složen 4-10 číslic. Tento kod se ukládá v zašifrované podobě v evidenci OP. Elektronickou identifikaci bude moci držitel OP zablokovat.

- Bez strojově čitelných údajů bez čipu. Tyto průkazy se vydávají pouze tehdy, pokud držitel ztratí OP nebo dojde ke katastrofě či mimořádné události.



Obr. 14: Občanský průkaz s čipem, zdroj: www.lupa.cz.

Využití čipového průkazu je zatím minimální, spíše žádné. Do budoucna by se na čip mohly ukládat základní údaje klienta, jako je jméno, adresa, rodné číslo, pohlaví, číslo občanského průkazu, klientův podpisový vzor, případně další. Klient si při vyřízení průkazu volí svůj jedinečný bezpečnostní kód, který pak může používat při každé identifikaci. Banky by opatřily svoje pobočky čtečkou těchto průkazů, klient by pak při návštěvě banky jednoduše vložil svůj občanský průkaz do čtečky, proběhla by identifikace průkazu, klient by zadal svůj bezpečnostní kód a v systému banky by se rovnou načetly všechny klientovy údaje a klient by byl tímto způsobem identifikován.

Princip této identifikace by byl na stejné bázi jako při používání platební karty, kdy používá klient ke své identifikaci plastovou platební kartu a svůj nastavený PIN kód.

Německé čipové občanské průkazy – eID

Od 1. listopadu 2010 vydává Spolkové ministerstvo vnitra nový identifikační dokument ve formátu plastové karty formátu ID1 s bezkontaktním elektronickým čipem, který je označován zkratkou „IDD“. Za vydání nového dokladu je stanoven poplatek 28,80 € pro osoby od 24 let s platností na 10 let a 22,80€ pro osoby pod 24 let s platností na 6 let.

1 + 14 - vícebarevné giloše
2 + 15 - mikrotext
3 + 16 - UV – potisk
4 - OVI (opticky variabilní barvy)
5 - holografický portrét
6 - 3D Spolková orlice
7 - kinematické pohybové struktury
8 - makro písmo
9 - inverze kontrastu
10 - strojově kontrolovatelná struktura
11 - integrační technika barvy (Innosec Fusion®)
12+20 - laserové gravírování
13 - taktilní vlastnosti laserového gravírování
17 - logo personálního dokladu
18 - melírované vlákna
19 - ražba na povrchové vrstvě
21 - sklopný obrázek laserový
22 - strojově čitelná zóna (MRZ)
23 - personalizovaný bezpečnostní proužek

Všechna data vytištěná na kartě jsou též uložena v čipu.

Data, která je možné držitelem uvolnit pro on-line funkce:

- Jméno a příjmení
- Datum a místo narození
- Adresa a PSČ
- Pseudonym
- akademické tituly

Společně s uvolněnými údaji je současně zaslána informace o platnosti dokladu. Dále se na německých eID mohou ukládat otisky prstů. Uložení otisků prstů žadatele je

volitelná (dobrovolná) funkce, pouze vyjmenované státní úřady mohou použít otisky prstů a to výhradně pro identifikaci. Otisky nejsou uloženy v žádné databázi a po výrobě karty jsou smazány ze systému a zůstávají pouze na kartě

Propočet pro čtečku občanských průkazů

Pro ukázku jsem zvolil čtečku čipů na občanských průkazech GemPC Twin USB, která má, dle mého názoru, potřebnou specifikaci z hlediska bezpečnosti pro ověření klientů. Na obrázku 15 uvádím čtečku čipů na občanských průkazech GemPC Twin USB.

Obr. 15: Čtečka GemPC Twin USB, zdroj: : www.tzk-sro.cz.

Tento typ čtečky je vyroben z čistě průhledného ale zároveň robustního plastu. Díky průhlednosti čtečky je možné vidět téměř celou plochu vložené čipové karty a tak lze snadno rozeznat typ karty nebo držitele karty. Tvar čtečky je uzpůsoben pro co nejjednodušší vložení/vyjmutí čipové karty. Rozměr čtečky je jen o trochu větší než čipová karta, takže na pracovním stole nezabírá zbytečně moc místa. V tabulce č. 32 uvádím technické parametry čtečky.

Tab. 32: Specifikace čtečky otisků prstů iEvo

Čtečka se k PC připojuje USB kabelem, dlouhým 1,5 m
Čtečka je určena pro provoz na MS Windows, Linux, Mac a dalších OS
Čtečka je kompatibilní se standardy:
ISO/IEC 7816-1,2,3,4 (kontaktní karty)
ISO 7816 Class A, B a C (5 V, 3 V, 1.8 V)
Microsoft Windows Hardware Quality Labs (WHQL), Windows Logo Program WLP 2.0
USB 2.0 Full speed certified
CCID - Chip Card Interface Device 1.0 (USB & ExpressCard readers)
Čtečka garantuje 100.000 vložení čipové karty

Zdroj: www.tzk-sro.cz

Propočet pro Air Bank:

Tab. 33: Pořizovací náklady na čtečku čipu OP pro Air bank:

Pořizovací náklady čtečky čipu pro Air bank		
cena v Kč s DPH	počet kusů	částka
680	250	**170 000**

Zdroj: autor.

Metoda propočtu pořizovacích nákladu čtečky otisků prstů pro Air Bank:

- cena zařízení GemPC Twin USB je 680 Kč s DPH
- počet kusů 10 kusů čtečky na jednu pobočku krát 25 poboček aktuální stav k 30.6. 2014
- kalkulace je uvedena v tabulce č. 33

Tab. 34: Doba návratnosti investice pro Air bank:

Doba návratnosti pro Air bank							
	zisk na 1 klienta v Kč	počet klientů	celkem	zvýšení rok	zvýšení den	návratnost	
aktuální stav	517	300 000	155 100 000			dny	měsíc
zvýšení o 1%	517	303 000	156 651 000	1 551 000	4 249	40	1,3
zvýšení o 3%	517	309 000	159 753 000	4 653 000	12 748	13	0,4
zvýšení o 5%	517	315 000	162 855 000	7 755 000	21 247	8	0,3
zvýšení o 7%	517	321 000	165 957 000	10 857 000	29 745	6	0,2
zvýšení o 10%	517	330 000	170 610 000	15 510 000	42 493	4	0,1
zvýšení o 37%	**517**	**411 000**	**212 487 000**	**57 387 000**	**157 225**	**1**	**0,0**

Zdroj: autor.

Metoda propočtu:

- zisk na 1 klienta je vypočten jako celkový zisk banky (výnosy – náklady) dělený počtem klientů
- návratnost je vypočtená jako čas, za jak dlouho zvýšení zisku pokryje pořizovací náklady vypočteno na dny a měsíce, roky a dny
- zisk a počet klientů jsou údaje zjištěné z veřejně dostupných dat
- zvýšení počtu klientů o 1 %, 3 %, 5 %, 7 % a 10 % jsou odhady pro přehlednost, jak by se vyvíjela návratnost počáteční investice při těchto úrovních přílivu nových klientů
- zvýšení počtu klientů o 37 % vyplývá z dotazníku, kde 37 % dotazovaných kladně odpovědělo na využití této technologie
- kalkulace je uvedena v tabulce č.34 a stejný propočet je použitý i v tabulce č. 36

Propočet pro Českou spořitelnu:

Tab. 35: Pořizovací náklady na čtečku čipu OP pro Českou spořitelnu:

Pořizovací náklady čtečky otisků prstů pro Českou spořitelnu		
cena v Kč	počet kusů	částka
680	6530	**4 440 000**

Zdroj: autor.

Metoda propočtu pořizovacích nákladu čtečky otisků prstů pro Českou spořitelnu:

- cena zařízení GemPC Twin USB je 680 Kč s DPH
- počet kusů 10 kusů čtečky na jednu pobočku krát 653 poboček aktuální stav k 31.12. 2013
- kalkulace je uvedena v tabulce č. 35

Tab. 36: Doba návratnosti investice pro Českou spořitelnu:

Doba návratnosti pro Českou spořitelnu							
	zisk na 1 klienta v Kč	počet klientů	celkem	zvýšení rok	zvýšení den	návratnost	
aktuální stav	2119	5 300 000	11 230 700 000			dny	měsíc
zvýšení o 1%	2119	5 353 000	11 343 007 000	112 307 000	307 690	14	0
zvýšení o 3%	2119	5 459 000	11 567 621 000	336 921 000	923 071	5	0
zvýšení o 5%	2119	5 565 000	11 792 235 000	561 535 000	1 538 452	3	0
zvýšení o 7%	2119	5 671 000	12 016 849 000	786 149 000	2 153 833	2	0
zvýšení o 10%	2119	5 830 000	12 353 770 000	1 123 070 000	3 076 904	1	0
zvýšení o 37%	**2119**	**7 261 000**	**15 386 059 000**	**4 155 359 000**	**11 384 545**	**0**	**0**

Zdroj: autor.

Výpočet rentability investice

Na základě vzorce pro výpočet rentability investice spočítám rentabilitu pro obě banky. Vzorec pro výpočet je:

ROI = Zisk / pořizovací náklady

Tab. 37: Výpočet rentability pro čtečku čipu na OP:

	zisk	počáteční investice	ROI
Air bank	155 100 000	170 000	**912**
Česká spořitelna	11 230 700 000	4 440 400	**2529**

Zdroj: autor.

Z tabulky vyplývá, že je rentabilita investice vyšší pro Českou spořitelnu.

Vliv nových klientů na vývoj zisku

Podle statistických dat České národní banky mají všechny české domácnosti založených 11,7 milionů účtů u tuzemských bank. Za předpokladu dotazníkového šetření jako reprezentativního vzorku, by tuto formu zabezpečení využilo 37 % dotazovaných. To by znamenalo 4 329 000 nových klientů. Kalkulaci zvýšení zisku, pro jednu i druhou banku, při zvýšení počtu klientů o tuto částku uvádím v tabulce.

Tab. 38: Vliv nových klientů na vývoj zisku u čtečky otisků prstů:

banka	zvýšení o 37%	zisk na 1 klienta v Kč	počet klientů	zisk	% zvýšení zisku
Air bank	4 329 000	517	4 629 000	2 393 193 000	1 543
Česká Spořitelna	4 329 000	2 119	9 629 000	20 403 851 000	182

Zdroj: autor.

Na základě této úvahy, kdy by si každá z bank ukrojila z celkového trhu stejný díl, při implementaci čtečky občanských průkazů, je patrné, že pro Air bank je procentuální zvýšení zisku vyšší a to 8,5 krát více než u České spořitelny.

Výpočet regresní analýzy

Tyto výpočty a vzorečky jsou použity z předchozí kapitoly 5.1.2 výpočtu regresní přímky pro čtečku otisku prstu.

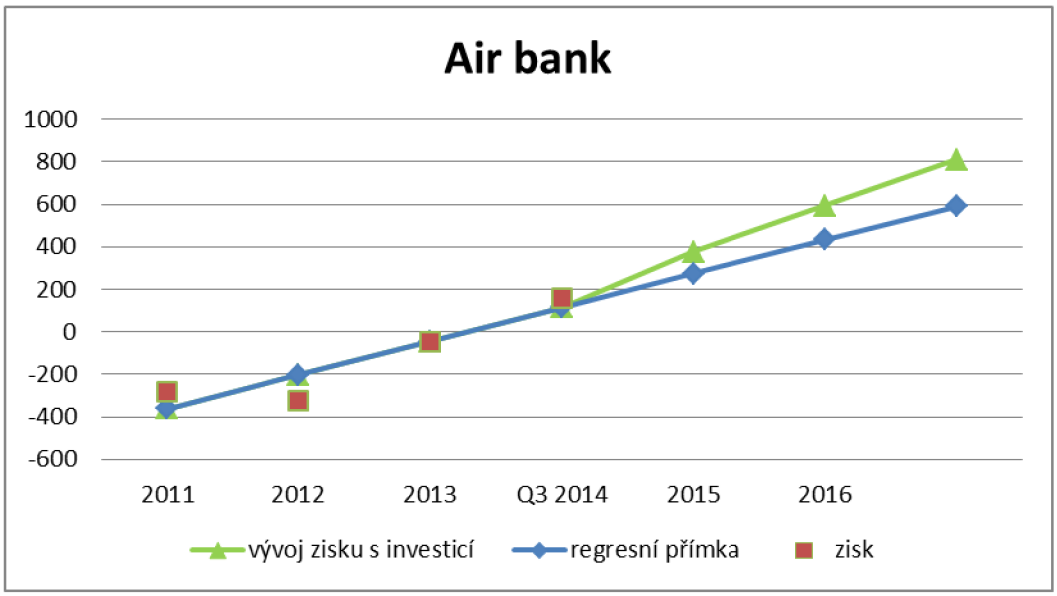
V následující tabulce je zobrazen výpočet pro určení regresní přímky. Jako výchozí data používám zisk Air bank a České spořitelny za roky 2011 – 2014. Prognóza je dále vypočítaná na 3 roky (do roku 2017).

Tab. 39: Výpočet regresní přímky pro Air bank:

Air bank							
x=pořadí roku	1	2	3	4	5	6	7
rok	2011	2012	2013	Q3 2014	2015	2016	2017
y = zisk	-282	-323	-45	155			
reg. přímka	-362,1	-203,2	-44,3	114,6	273,5	432,4	591,3
zvýšení o 37 %	-362,1	-203	-44	114,6	**375**	**592**	**810**

Údaje jsou uvedeny v mil. Kč, zdroj: autor.

Níže zobrazuji regresní přímku pro Air bank graficky, v porovnání s investicí.



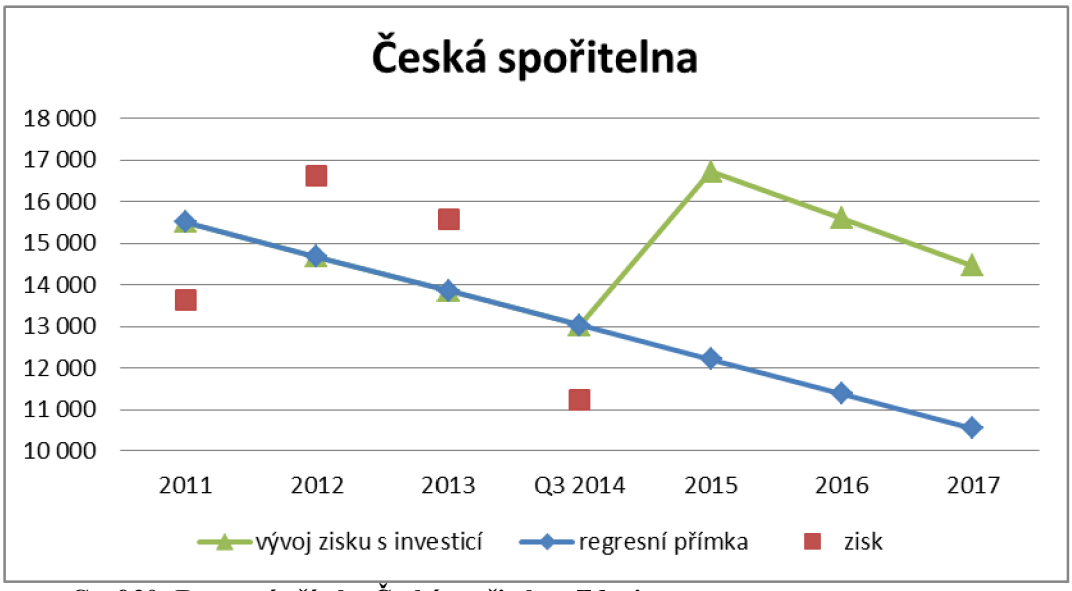
Graf 19: Regresní přímka Air bank. Zdroj: autor.

Tab. 40: Výpočet regresní přímky pro Českou spořitelnu:

Česká spořitelna							
x=pořadí roku	1	2	3	4	5	6	7
rok	2011	2012	2013	Q3 2014	2015	2016	2017
y = zisk	13 638	16 612	15 588	11 230			
reg. přímka	15 504	14 679	13 855	13 030	12 205	11 380	10 555
zvýšení o 37 %	15 504	14 679	13 855	13 030	**16 716**	**15 591**	**14 461**

Údaje jsou uvedeny v mil. Kč, zdroj: autor.

Níže zobrazuji regresní přímku pro Českou spořitelnu graficky, v porovnání s investicí.



Graf 20: Regresní přímka České spořitelny. Zdroj: autor.

Závěr:

Využití čipu na občanských průkazech má hned několik výhod, ale zároveň i úskalí. V první řadě se podíváme na hlavní úskalí, které je ve využívání čipových občanských průkazů. Os roku 2020 se už nebudou sice vyskytovat staré formáty OP, ale u nových OP není zatím povinný elektronický čip. Uvažujme tedy variantu, že už většina klientů čipovou OP používá. Další nevýhodou je zároveň cena čipové OP, která je v současné době 500 Kč. V poslední řadě je tu nákladovost na pořízení čtecích zařízení pro čipy na OP a implementace do bankovního softwaru.

Uvažujme tedy, že čipové OP jsou využívané klienty. Hlavní výhody využití čipů v OP jsou následující:

- úspora času při obsluze klienta (načtení dat z OP do systému, rychlé vyhledání klienta v systému, vyšší počet obsloužených klientů)
- snížení chybovosti (údaje se načtou automaticky, nehrozí chyba překlepu nebo špatného opsaní údajů pracovníkem)
- zvýšení bezpečnosti (systémová identifikace klienta, rozpoznání neplatných, padělaných nebo odcizených dokladů)

Pro srovnání jsem vybral banky 2. Relativně novou (3 roky na trhu) Air Bank a stálici na trhu Českou spořitelnu. Každá z těchto bank má tedy rozdílné pořizovací

náklady, rozdílný zisk z 1 klienta, rozdílný počet klientů a pro každou banku má implementace těchto zařízení jiný přínos. Pro srovnání jsem použil pouze počáteční náklady na pořízení zařízení, které mohu jednoznačně vyčíslit pro každou banku. Samozřejmě je třeba zahrnout i další náklady např. na instalaci zařízení, ovládací software a mzdu pracovníků, kteří budou zařízení uvádět do provozu. Pro Českou spořitelnu budou tyto dodatečné náklady za jisté daleko vyšší než pro Air bank s menším počtem poboček.

V tabulkách výše jsou uvedené náklady na pořízení těchto čtecích zařízení. Zatímco Air Bank má v tuto dobu pouze 577 Kč zisk na jednoho klienta a Česká spořitelna 2 119 Kč. Pro Českou spořitelnu vychází rychlejší doba návratnosti investice do čteček čipových OP. U Air Bank je při nárůstu 3 % počtu klientů díky pořízení a využívání čteček doba návratnosti 13 dnů u České spořitelny při stejném nárůstu 5 dnů. V tomto případě se však jedná hrubý odhad, protože nemůžeme vyčíslit, jaký zisk by to přineslo při dalším využití uspořeného času.

Z dotazníku vyplývá, že by čtečku OP využilo 37 % dotazovaných, to znamená pro Air bank i Českou spořitelnu okamžitou návratnost investice při zvýšení klientů o tuto procentuální část.

Z pohledu rentability nákladů dané investice v porovnání se ziskem vychází Air bank 912 a Česká spořitelna na 2 529. Za těchto podmínek je tedy efektivnější investice pro Českou spořitelnu.

Pokud by se ovšem jednalo o 37% zvýšení počtu potenciálních klientů z celého trhu, tak by u Air bank došlo ke zvýšení zisku o 1 543 %, oproti stávajícímu stavu. Naopak u České spořitelny pouze k 182 % zvýšení. Procentuální zvýšení zisku vychází 8,5 krát lépe pro Air bank.

Časová návratnost a rentabilita je ve prospěch České spořitelny. Pokud by se ovšem jednalo o zvýšení počtu klientů z celého trhu, je investice přínosnější pro Air bank.

5.1.4 Hlasová biometrie

Ve zkratce se jedná o soubor metod založených na měření a analýze jedinečných charakteristik člověka. Právě faktu, že každý člověk je jiný, tato metodika využívá. Biometrie tak zkoumá a porovnává otisky prstů, oční duhovky a sítnice, DNA, dále třeba charakteristiky chůze, písma či hlasu. Nejznámější biometrickou metodou je bezpochyby ověřování pomocí otisků prstů. Při ověření osoby je porovnáván sejmutý otisk prstu s otiskem dotyčného uloženým v databázi. Na stejném principu funguje i hlasová biometrie. Ze vzorku hlasu se vytváří tzv. hlasový otisk, který obsahuje typické charakteristiky daného hlasu. Tento otisk je pak následně porovnáván s otiskem z databáze.

Myšlenka autentizace hlasem není nová, tato metoda byla vyvinuta již roku 1970. Technologie však od té doby udělaly značný pokrok. Jak je tedy možné, že hlasová verifikace není dnes více využívána? Možnou příčinou může být řada rozšířených omylů a mýtů, které se k hlasové verifikaci vztahují. Hlasová verifikace je často zaměňována s rozpoznáváním hlasu. Přitom se jedná o dvě odlišné technologie, jejichž jediným pojítkem je právě hlas. Zatímco rozpoznávání řeči funguje na principu převodu zvukového záznamu na text s cílem zjistit význam slov, hlasová verifikace pracuje s porovnáváním vzorků hlasu, tzv. hlasového otisku. Cílem je zjistit shodu s otiskem, uloženým v databázi, na významu slov nezáleží.

Dalším rozšířeným omylem je přílišná náročnost na vybavení. Zde je však třeba rozlišit dvě různé oblasti, ve kterých hlasová biometrie nachází využití – hlasovou identifikaci a hlasovou verifikaci. Hlasová identifikace se využívá k rozpoznání neznámého řečníka, tzn. nevíme, kdo mluví a je potřeba prohledat databázi a najít shodný vzorek. Verifikace naopak slouží k ověření předpokládaného řečníka, tzn. víme, kdo mluví a porovnáváme tak pouze otisk jeho hlasu s otiskem z databáze. Veškeré aplikace pro hlasovou verifikaci tak mohou fungovat na běžných standardních počítačích.

V neposlední řadě pak stojí domněnka, že autentizace hlasem není bezpečná. Ale jsou klasické metody bezpečnější? Současná praxe zabezpečení pomocí PIN kódů nebo jiných hesel se ukazuje být nedostatečnou. Běžný člověk totiž používá maximálně osm

hesel. Hlas má jednu obrovskou výhodu – máte ho vždy u sebe. Pokud k zadávání hesla používáte hlas, můžete ho mít bez obav napsané a nalepené třeba na monitoru.

Navzdory těmto rozšířeným omylům odborníci očekávají v následujících pěti letech rapidní nárůst trhu. Dnes je hlasová verifikace nejčastěji využívána v telefonních aplikacích kontaktních center k ochraně přístupu k citlivým datům. Další široce využívanou oblastí použití je zabezpečení přístupu do objektů. Růst se však kromě těchto dvou oblastí dotkne zejména finančního sektoru, kde hlasová verifikace může přinést značnou úsporu nákladů na zabezpečení a nárůst uživatelského komfortu a bezpečí.

Přínosy pro zákazníka

Vlastní přínosy implementace řešení hlasové biometrie je možné rozdělit na dvě oblasti, a to přínosy dané samotnou technologií a jejími vlastnostmi a dále přínosy díky možnosti poskytování nových služeb v rámci hlasových aplikací.

- **Bezpečný přístup k privátním informacím**
- **Vysoká úroveň zabezpečení**
- **Přístup k informacím pro nevidomé**
- **Zkrácení doby nutné k ověření volajícího**
- **Flexibilní architektura**
  Řešení webové služby. Možnost implementace prakticky do jakéhokoliv stávajícího prostředí.
- **Otevřená platforma**
  Otevřenost pro budoucí růst jak z pohledu kapacitního, tak z pohledu nových funkcí a služeb.
- **Jazyková nezávislost**
  Heslem může být cokoliv.
- **Vysoká dostupnost řešení**

Využití hlasové biometrie u slovenské Tatra Banky

Pro příklad implementace této technologie využijeme případovou studii slovenské Tatra Banky, která hlasovou biometrii zavedla v roce 2013.

DŮVOD:

- nepohodlný a zdlouhavý proces ověření totožnosti
- 90 % hovorů vyžaduje autentizaci s průměrnou délkou 40 vteřin

ŘEŠENÍ

- Tatra banka nemá IVR takže bylo nasazeno řešení FreeSpeech Voice Biometrics
- Interní návratnost (ROI) byla stanovena na 11 měsíců
- Nejdříve realizována placená studie proveditelnosti

OBCHODNÍ VÝSLEDKY

- v průměru o 36 vteřin kratší AHT
- 75 000 registrací nových klientů během 6 týdnů, nyní se zaregistrovalo 100 000+
- Podstatné snížení podvodných transakcí
- 97 % ověření totožnosti volajícího jsou automatizované
- zabezpečení banky (Net Promoter Score) se zvýšilo z 31 to 69

Z výše uvedené studie vidíme velký přínos pro banku při využití této hlasové biometrie, jako dalšího bezpečnostního prvku.

Závěr:

Z hlediska bezpečnosti je hlasová biometrie výrazným krokem kupředu. Stejně jako otisk prstu nebo DNA je hlas jedinečným pro každého člověka. Dokonce ani ten nejlepší imitátor nedokáže hlasovou identifikaci obelstít. Dalším bezpečnostním prvkem je identifikace dřívějších podvodníků nebo potenciálních bezpečnostních hrozeb. Pokud se někdo pokusí nějakým způsobem banku nebo klienta ohrozit, jeho hlas se uloží do databáze řekněme podvodníků a při dalším pokusu bude hned odhalen po promluvení. Samozřejmě i tato technologie má své úskalí.

Zde můžeme přirovnat slovenskou Tatra banku k české Air bank. Mají srovnatelný počet klientů a poboček. Jedná se taky o novou inovativní banku, oblíbenou u klientů. Z toho důvodu můžeme počítat podobný dopad, při zavedení hlasové biometrie u Air bank. Pro Českou spořitelnu je toto srovnání velice obtížné, už jen

z toho důvodu, že náklady na pořízení tohoto zařízení jsou pro každou banku velice odlišné.

Z dotazníku vyplynulo, že pouze 9% oslovených by využilo možnost ověření hlasem. Může to být i z toho důvodu, že je to nová forma zabezpečení a lidé k tomu nemají ještě takovou důvěru.

6 Závěr

V této práci jsem zanalyzoval současnou situaci bezpečnosti elektronického bankovnictví, vyhodnotil jednotlivé formy, vyzdvihl jejich výhody a nevýhody, upozornil na některá rizika spojená s jejich používáním a přitom nastínil možné směry jeho vývoje do budoucnosti.

Dnes je velmi důležité mít přehled nejen o současném stavu, ale sledovat i nové trendy. Za prioritu přímého bankovnictví lze považovat neomezený přístup klienta ke svému účtu. Platební transakci je možné vyřídit odkudkoliv a kdykoliv. To přináší v porovnání s návštěvami poboček značnou úsporu času. Za hlavní přednost přímého bankovnictví je možné považovat časově neomezený přístup klienta ke svému účtu. I z finančního hlediska je pro klienty internetové bankovnictví výhodou, mnoho bank, a to zejména nových, nabízí svým zákazníkům internetové bankovnictví zcela zdarma. Pro tuto formu existují i konkrétní rizika, která klient nebo banka při využití služeb přímého bankovnictví podstupují.

V teoretické části práce jsem se zabýval vymezením internetového bankovnictví: jeho definicí, historií, nastíněním výhod a nevýhod při využívání internetového bankovnictví jak pro klienta, tak i pro banku. Také jsem se zmínil o nejrůznějších formách napadení internetového bankovnictví a jeho bezpečnostních opatřeních. Zmapoval jsem největší útoky na internetové bankovnictví a na české servery. Nejvíce české banky ohrožují útoky hackerů. Především tzv. DDoS útoky, kdy se jedná o neúnosně velký počet malých útoků na jedno konkrétní místo. Poslední takovýto útok vyřadil servery českých bank na několik hodin.

Díky analýze současného stavu zabezpečení u jednotlivých bank bylo zjištěno, že nejčastější formou zabezpečení je uživatelské jméno a heslo pro vstup do elektronického bankovnictví. Další formy jsou sms verifikace pro vstup nebo certifikáty a tokeny. Každá banka má zároveň i zabezpečenou přihlašovací stránku do

elektronického bankovnictví. Pro potvrzování plateb je skoro všemi bankami využíváno potvrzení pomocí sms kódu.

Byl vytvořen dotazník spokojenosti s bezpečností elektronického bankovnictví. Tento dotazník obdržela skupina respondentů pracující v bankovním sektoru, aby byly zajištěny převážně odborné názory. Ukázalo se, že např. pouze necelá polovina odpověděla, že jejich banka využívá protokol https k zabezpečení přístupové stránky do elektronického bankovnictví. Tento protokol ovšem využívají všechny banky, jak prokázala analýza zabezpečení elektronického bankovnictví. V dotazníku byly položeny otázky, zda by klienti využili nové formy zabezpečení, jako jsou: otisk prstu, sken čipu na občanském průkazu nebo ověření pomocí hlasové biometrie. Nejvíce dotazovaných by využilo metodu otisku prstu 57 %, dále čip na občanském průkazu 37 % a v poslední řadě hlasovou verifikaci pouze 9 %.

Obecným mezinárodním trendem v oblasti zabezpečení jsou biometrické technologie. Pro oblast bankovnictví byly navrženy technologie jako signpad, čtečka otisku prstů, čtečka čipu na občanských průkazech a hlasová biometrie.

Pro srovnání byly zvoleny 2 banky a to Air bank a Česká spořitelna. Tyto banky byly vybrány na základě odlišnosti v počtu klientů, poboček a délky působení na českém trhu.

Z propočtu čtečky otisků prstů je patrné, že je počáteční investice vyšší než u čtečky čipů občanských průkazů. Je tedy i delší návratnost investice. Na základě dotazníkového šetření by tuto formu zabezpečení využilo 56 %. Při zvýšení počtu klientů o tuto hodnotu je návratnost u Air bank 19 dnů a u České spořitelny 7 dnů. Ze srovnání bank vychází, že Česká spořitelna má 17 krát více klientů než Air bank, ale pouze 4 krát větší zisk na jednoho klienta. Doba návratnosti i rentabilita investice vychází lépe pro Českou spořitelnu. V případě zvýšení zisku při ovlivnění 56 % celého trhu, by procentuální zvýšení vyšlo ovšem 10 krát lépe pro Air bank.

Z dotazníku vyplynulo, že počet klientů, kteří by metodu ověření pomocí čipu na občanském průkazu využili, by byl 37 %. Srovnal jsem české občanské průkazy s německými průkazy s čipem, kde je tato forma běžně používaná. Protože čipy na občanských průkazech nejsou u nás téměř využívané, doporučil bych tuto formu řešit, až s podporou státních institucí. Návratnost případné investice do čteček čipů na občanských průkazech je od zvýšení počtu klientů o 5 % téměř okamžitá, pro obě sledované banky. Návratnost investice i rentabilita vychází výhodněji pro Českou spořitelnu. I v tomto případě vychází procentuální zvýšení zisku lépe pro Air bank, při ovlivnění 37 % celého trhu klientů.

Cena softwaru na hlasovou biometrii není veřejně dostupný údaj, proto pro zjištění výhodnosti je použito srovnání Air bank a slovenské Tatra banky, kde byla tato technologie zavedena. U Tatra banky hlasová biometrie přinesla nejen zvýšení bezpečnosti, ale i úsporu nákladů.

Závěrem tedy vyplývá, že zmiňované formy formy zabezpečení, jako jsou čtečka otisku prstu, čtečka čipu na občanském průkazu nebo hlasová verifikace, mají své přínosy nejen ve zvýšení zisku a úspoře nákladů, ale hlavně ve zvýšení bezpečnosti.

7 Seznam použitých zdrojů

Bezpečnost IB. In: *Bezpečnost IB* [online]. 2011 [cit. 2014-04-16]. Dostupné z: http://genmedia.cz/blog/bezpecnost-internetoveho-bankovnictvi.html

Bezpečnost internetového bankovnictví obecně. In: *Bezpečnost internetového bankovnictví obecně* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx

Bezpečnost v bankovnictví: Klienti si nemění hesla a neumí zabezpečit chytrý telefon. In: *Bezpečnost v bankovnictví: Klienti si nemění hesla a neumí zabezpečit chytrý telefon* [online]. [cit. 2014-04-16]. Dostupné z: http://www.finance.cz/zpravy/finance/412996-bezpecnost-v-bankovnictvi-klienti-si-nemeni-hesla-a-neumi-zabezpecit-chytry-telefon/

Ceed, Elektronické bankovnictví [on-line]. [2006-9-11]. Dostupné z:http://www.ceed.cz/bankovnictvi/778elektronicke-bankovnictvi.htm

ČERMÁK, Miloš. Nepříjemné: Přichází nová generace bankovního malwaru. In: *Nepříjemné: Přichází nová generace bankovního malwaru* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.bankovnipoplatky.com/zaujalo-nas-prichazi-nova-generace-bankovniho-malwaru-20455

Další útok hackerů v ČR: Terčem internetové bankovnictví velkých bank, ČNB i web burzy. In: *Další útok hackerů v ČR: Terčem internetové bankovnictví velkých bank,* [online]. [cit. 2014-04-16]. Dostupné z: http://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci

ČNB i web burzy [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.patria.cz/zpravodajstvi/2282801/dalsi-utok-hackeru-v-cr-tercem-internetove-bankovnictvi-velkych-bank-cnb-i-web-burzy.html

Čtečka kontaktních karet Gemalto IDBridge CT30. [online]. 2013 [cit. 2015-01-19]. Dostupné z: http://www.eshop-sovte.cz/produkt/ctecka-kontaktnich-karet-gemalto-idbridge-ct30/

FRANCOVÁ, Pavla. Největší banky v Česku napadli hackeři. Vyřadili jim z provozu internetové bankovnictví. In: *Největší banky v Česku napadli hackeři. Vyřadili jim z provozu internetové bankovnictví* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://byznys.ihned.cz/c1-59450640-nejvetsi-banky-v-cesku-napadli-hackeri-vyradili-jim-z-provozu-internetove-bankovnictvi

HOVORKA, Jiří. Bezpečnost IB. In: *Bezpečnost iB* [online]. 2012 [cit. 2014-04-16]. Dostupné z: http://aktualne.centrum.cz/finance/penize/clanek.phtml?id=731692

Internetové bankovnictví. In: BOUŠOVÁ, Kateřina. *Internetové bankovnictví* [online]. 2006 [cit. 2014-04-16]. Dostupné z: http://m.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci

Jak bezpečné je vaše internetové bankovnictví?. In: BITTO, Ondřej. *Jak bezpečné je vaše internetové bankovnictví?* [online]. 2005 [cit. 2014-04-16]. Dostupné z: http://www.lupa.cz/clanky/jak-bezpecne-je-vase-internetove-bankovnictvi/

JELÍNEK, Martin. Autentizační tokeny v praxi. In: *Autentizační tokeny v praxi* [online]. 2008 [cit. 2014-04-16]. Dostupné z: http://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm

KLÍMA, Vlastimil. Bezpečnost internetového bankovnictví. In: *Bezpečnost internetového bankovnictví* [online]. 2009 [cit. 2014-04-16]. Dostupné z: http://cryptography.hyperlink.cz/2009/ST_2009_06_11_11.pdf

KRČMA, Pavel. Jak (ne)bezpečné může být elektronické bankovnictví?. In: *Jak (ne)bezpečné může být elektronické bankovnictví?* [online]. 2012 [cit. 2014-04-16].

Dostupné z: http://computerworld.cz/securityworld/jak-ne-bezpecne-muze-byt-elektronicke-bankovnictvi-48497

KRČMÁŘ, Petr. *Televizní bankovnictví na dosah ruky*. ROOT.CZ [online]. 1. 4. 2005 [cit. 2012-03-26]. Dostupné z: http://www.root.cz/clanky/televizni-bankovnictvi/

KUČERA, Petr. Téměř polovina Čechů nepoužívá internetové bankovnictví. In: *Téměř polovina Čechů nepoužívá internetové bankovnictví* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://zpravy.aktualne.cz/finance/temer-polovina-cechu-nepouziva-internetove-bankovnictvi/r~i:article:780458/

LAZAREVIČ. Lidé stále podceňují přístup k zabezpečení internetového bankovnictví. In: *Lidé stále podceňují přístup k zabezpečení internetového bankovnictví* [online]. 2014 [cit. 2014-04-16]. Dostupné z: http://www.mesec.cz/clanky/lide-stale-podcenuji-zabezpeceni-internetoveho-bankovnictvi-podcenuj/

MÁČE, Miroslav. *Elektronický platební styk*, Grada Publishing, a.s., 2006, ISBN 8024717255.

MAREK, Vlastimil. Něco v síti: fejetony, které vycházely od roku 1997 na internetu na adrese http://svet.namodro.cz. DOI: http://zpravy.aktualne.cz/finance/banky-zvysuji-za.

MARTÍNEK, Lukáš. Magistrát už vydává nové elektronické občanky. In: *Magistrát už vydává nové elektronické občanky* [online]. 2012 [cit. 2014-04-18]. Dostupné z: http://www.hradeckralove.org/noviny-a-novinky/magistrat-uz-vydava-nove-elektronicke-obcanky

MARVANOVÁ, M., SCHLOSSBERGER, O. et al. *Platební styk*, 2. dopl. vyd. Praha : Bankovní institute, 1998. 376 s.

MATĚJŮ, David. Bezpečnost elektronického bankovnictví. In: *Bezpečnost elektronického bankovnictví* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnost-elektronickeho-bankovnictvi.htm

Může být biometrický podpis skutečně bezpečný?. In: *Může být biometrický podpis skutečně bezpečný?* [online]. 2011 [cit. 2014-04-16]. Dostupné z: http://www.viditelnypodpis.cz/blog/

Počátky internetového bankovnictví. In: *Počátky internetového bankovnictví* [online]. 2014 [cit. 2014-04-16]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

Pozor při práci s elektronickým bankovnictvím, pokusů o zneužití přibývá. In: *Pozor při práci s elektronickým bankovnictvím, pokusů o zneužití přibývá* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.bankovnipoplatky.com/pozor-pri-praci-s-elektronickym-bankovnictvim-pokusu-o-zneuziti-pribyva-20912

PŘÁDKA, Michal, KALA, Jan: *Elektronické bankovnictví*, Computer press, 2000, ISBN 8072263285.

Přímé bankovnictví. In*: Přímé bankovnictví* [online]. 2012 [cit. 2014-04-16]. Dostupné z: http://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

Registrační biometrická čtečka otisku prstů. [online]. 2012 [cit. 2015-01-19]. Dostupné z: http://www.tzk-sro.cz/snimace-otisku-prstu/703-registracni-biometricka-ctecka-otisku-prstu.html

SALMON, Michal. Kulhající bezpečnost internetového bankovnictví. In: *Kulhající bezpečnost internetového bankovnictví* [online]. 2008 [cit. 2014-04-16]. Dostupné z: http://www.mesec.cz/clanky/kulhajici-bezpecnost-internetoveho-bankovnictvi/

Srovnání antivirových programů, srovnání antivirů. In: *Srovnání antivirových programů, srovnání antivirů.* [online]. 2014 [cit. 2014-04-16]. Dostupné z: http://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx

ŠENKÝŘOVÁ, Bohuslava, et al. Bankovnictví I. 2. aktualizované vyd. Praha : Grada, 1999. 263 s. ISBN 80-7169-859-8.

TOMEK, Lukáš. USB token: pamatuje si hesla a šifruje. Útok zabere dvě a půl minuty. In: *USB token: pamatuje si hesla a šifruje. Útok zabere dvě a půl minuty* [online]. 2010 [cit. 2014-04-16]. Dostupné z: http://www.lupa.cz/clanky/usb-token-pamatuje-si-hesla-sifruje-neni-bezpecny/

Vývoj elektronického bankovnictví. In: *Vývoj elektronického bankovnictví* [online]. 2013 [cit. 2014-04-16]. Dostupné z: http://www.ceed.cz/bankovnictvi/779vyvoj_elektornickeho_bankovnictvi.htm

8 Slovník pojmů a zkratek

- e-business - elektronické podnikání;
- e-commerce – elektronické obchodování;
- e-banking – elektronické bankovnictví;
- e-government – elektronizace veřejné správy, elektronické vládnutí;
- e-learning – vzdělávací proces využívající informační a komunikační technologie k tvorbě kurzů, k distribuci studijního obsahu;
- intranet – označení pro část počítačové sítě, která používá stejné technologie jako Internet (rodinu protokolů TCP/IP, přenosový protokol HTTP atp.). Na rozdíl od Internetu je však Intranet privátní („soukromý“), tj. jeho využívání je omezeno na malou skupinu uživatelů (například pracovníci firmy, školy);
- extranet – specifický případ aplikace mechanismů, přístupů a protokolů uplatňovaných v Internetu (a Intranetu) na množinu spolupracujících ekonomických subjektů. Za typické uživatele považujeme partnery ekonomického subjektu. Přístup ke zdrojům Extranetu je řízen a kontrolován. Zdroje Extranetu jsou využívány k zefektivnění procesů, které mezi ekonomickým subjektem a partnery probíhají;
- e-shop – internetové obchody;
- sprinter – je mechanické zařízení, které snímá z embosované platební karty vytlačené (tedy embosované) údaje, což jsou číslo karty, doba její platnosti a jméno majitele. Tyto údaje se následně objeví na účtence, kterou vytiskne a zákazník podepíše;
- homebanking – klient je přes modem napojen svým firemním nebo domácím počítačem na počítač banky a může si sám kontrolovat stav účtu a zadávat příkazy, aniž by musel jít osobně do pobočky banky;
- telebanking – telefonní bankovnictví – je jedna z metod spojení klienta s bankou. Dříve používané ve spojení s pevnou linkou, dnes v drtivé většině případů využívané prostřednictvím komunikace skrze mobilní telefon;
- phishing – je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci;

- pharming – (někdy překládáno do češtiny jako *farmaření*) je podvodná technika používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu po napsání URL banky do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky. Ani zkušení uživatelé nemusejí poznat rozdíl (na rozdíl od příbuzné techniky phishingu);
- hacking – jsou počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb. V masmédiích se tento termín používá pro počítačové zločince a narušitele počítačových sítí;
- smishing – podvodná technika fungující na principu zasílání lživých sms zpráv, kdy se v síti operátora objevily zprávy, které budily zdání, že jsou od finanční instituce, a upozorňovaly klienty na zablokování účtu;
- attack vector – vektor attaku;
- black hat – černý klobouk;
- botnet – robot síť;
- malware – je počítačový program určený ke vniknutí nebo poškození počítačového systémuDDos – odepření služby;
- keylogging – je software, který snímá stisky jednotlivých kláves. Antivirem bývá považován za virus. V případě software se jedná o určitou formu spyware;
- shareware – je označení pro software chráněný autorským právem, který je možné volně distribuovat (typicky na internetu nebo na CD, DVD, jež jsou přílohami časopisů). Uživatel má možnost software po určitou dobu zkoušet, zda mu vyhovuje nebo ne. Pokud ho ale nadále používá, je povinen se řídit podle autorovy licence a zpravidla zaplatit cenu programu nebo se třeba jen registrovat;
- token – je převážně fyzické zařízení, které usnadňuje uživatelům zabezpečených služeb ověření pro přístup a užívání;
- Tv banking – komunikace klienta s bankou přes tv;
- password – heslo;
- SignPad – tzv. podpisový tablet;
- matching – srovnání;

9 Seznam grafů, tabulek a obrázků

Grafy:

Obrázky:

Tabulky:

10 Přílohy

Příloha č. 1. Dotazník „Bezpečnost elektronického bankovnictví“

1. **Oblast základních dat**

- **Jste?**
  - Muž
  - Žena
- **Vaše věková kategorie je:**
  - 18–24
  - 25–29
  - 30–39
  - 40–49
  - 50–59
  - 60 a více
- **Do jaké skupiny se řadíte?**
  - Student
  - Zaměstnaný
  - Podnikatel
  - Nezaměstnaný
  - Jiné …
- **Jaké máte nejvyšší dosažené vzdělání?**
  - základní
  - středoškolské
  - vyučen/a
  - vysokoškolské
  - žádné

2. **Využívání el. bankovnictví**

- **Využíváte elektronické bankovnictví? (pokud odpovíte ne, tak nemusíte pokračovat v dotazníku)**

- Ano
- Ne
- Moje banka nenabízí tuto službu

- **Jak využíváte internetové bankovnictví?**
  - Aktivně – denně
  - Aktivně – občas (jednou týdně)
  - Pasivně – nejsem přesvědčený o bezpečnosti (jednou měsíčně)
  - Pasivně – mám, ale nepoužívám

3. Zabezpečení

- **Jaký typ zabezpečení Vaše banka využívá pro vstup do el. bankovnictví?**
  - Protokol http (zabezpečení přihlašovací stránky do el. bankovnictví bankou)
  - Uživatelské jméno pro vstup do el. bankovnictví
  - Uživatelské heslo pro vstup do el. bankovnictví
  - Autentizační sms (pro vstup do el. bankovnictví)
  - Certifikát (soubor dat vytvořený bankou a uložený v PC, na USB nebo čipové kartě)
  - Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)
  - Čipové karty (nutné pro vstup a ovládání el. bankovnictví)
  - Jiné …
- **Je pro Vás toto zabezpečení dostačující?**
  - Ano
  - Ne
- **Jaký typ zabezpečení Vaše banka využívá pro potvrzení plateb?**
  - Autorizační sms (pro ověření transakce)
  - Uživatelské heslo pro potvrzení platby
  - Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)
  - Jiné (prosím uveďte)

- **Je pro Vás toto zabezpečení dostačující?**
    - Ano
    - Ne
- **Jaký typ zabezpečení je pro Vás důležitý?**
    - Protokol http (zabezpečení přihlašovací stránky do el. bankovnictví bankou)
    - Uživatelské jméno pro vstup do el. bankovnictví
    - Uživatelské heslo pro vstup do el. bankovnictví nebo pro potvrzení platby
    - Autorizační sms (pro ověření transakce)
    - Autentizační sms (pro vstup do el. bankovnictví)
    - Certifikát (soubor dat vytvořený bankou a uložený v PC, na USB nebo čipové kartě)
    - Token (generátor kódu pro vstup, nejčastěji ve formě klíčenky)
    - Čipové karty (nutné pro vstup a ovládání el. bankovnictví)
    - Jiné …
- **Jak je pro Vás zabezpečení důležité při výběru banky?**
    - Velmi důležité
    - Důležité
    - Není to pro mě rozhodující
    - Změnil bych kvůli tomu banku
- **Vybral(a) byste si banku, která by Vám nabídla metodu otisku prstu jako formu zabezpečení? (při každé návštěvě pobočky své banky, byste se identifikoval(a) otiskem prstu, bez nutnosti předložení dalšího identifikačního dokladu)**
    - ano, tuto formu zabezpečení bych využil(a)
    - ne, nevyužil(a) bych tuto formu zabezpečení
    - ne, nemám důvěru k tomuto typu zabezpečení

- **Vybral(a) byste si banku, která by Vám nabídla metodu identifikace pomocí čipu na občanském průkazu nebo pasu jako formu zabezpečení? (při každé návštěvě pobočky své banky, by pracovník použil čtečku,do které by vložil Váš doklad, všechny údaje by se automaticky načetly, zároveň by došlo k ověření totožnosti)**
    - ano, tuto formu zabezpečení bych využil(a)
    - ne, nevyužil(a) bych tuto formu zabezpečení
    - ne, obávám se zneužití těchto dat
- **Vybral(a) byste si banku, která by Vám nabídla metodu ověření pomocí rozpoznávání hlasu jako formu zabezpečení? (při prvním použití nahrajete svůj hlas, při dalším použití stačí jen promluvit a rovnou dojde k ověření vaší identity. Nemusíte zdlouhavě zodpovídat na otázky operátora, ani si pamatovat žádná hesla)**
    - ano, tuto formu zabezpečení bych využil(a)
    - ne, nevyužil(a) bych tuto formu zabezpečení
    - ne, obávám se zneužití těchto dat

- **Jakou banku nyní využíváte?**
    - Air Bank a.s.
    - BRE Bank S.A. (mBank)
    - Citibank Europe plc, organizační složka
    - Česká spořitelna, a.s.
    - Českomoravská stavební spořitelna, a.s.
    - Československá obchodní banka, a.s.
    - Equa bank, a.s.
    - Evropsko-ruská banka, a.s.
    - Fio banka, a.s.
    - GE Money Bank, a.s.
    - Hypoteční banka, a.s.
    - Komerční banka, a.s.
    - LBBW Bank CZ, a.s.
    - Modrá pyramida stavební spořitelna, a.s.

- Oberbank AG – pobočka Česká republika
- Raiffeisen stavební spořitelna, a.s.
- Raiffeisenbank, a.s.
- Raiffeisenbank im Stiftland eG pobočka Cheb, odštěpný závod
- Sberbank CZ, a.s.
- Stavební spořitelna České spořitelny, a.s.
- UniCredit Bank Czech Republic, a.s.
- Waldviertler Sparkasse Bank AG
- Wüstenrot hypoteční banka, a.s.
- Wüstenrot stavební spořitelna, a.s.
- ZUNO BANK AG, organizační složka
- Jiná