Mendelova univerzita v Brně
Provozně ekonomická fakulta

Formy elektronického bankovníctva a ich využitie v Slovenskej republike

Bakalárska práca

Vedúci práce:
Ing. Jiří Třinácty

Petra Sojková

Brno 2016

Poďakovanie

Ďakujem môjmu vedúcemu práce Ing. Jiřímu Třináctému, za jeho odborné vedenie, metodickú pomoc a cenné rady, ktoré mi poskytol pri vypracovaní bakalárskej práce.

Čestné prehlásenie

Prehlasujem, že som tuto prácu: **Formy elektronického bankovníctva a ich využitie v Slovenskej republike**
vypracovala samostatne a všetky použité pramene a informácie sú uvedené v zozname použitej literatúry. Súhlasím, aby moja práca bola zverejnená v súlade s § 47b zákona č. 111/1998 Sb., o vysokých školách v znení neskorších predpisov, a v súlade s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Som si vedomá, že sa na moju prácu vzťahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brne má právo na uzatvorenie licenčnej zmluvy a užití tejto práce ako školského diela podľa § 60 odst. 1 Autorského zákona.

Ďalej sa zaväzujem, že pred spísaním licenčnej zmluvy o využití diela inou osobou (subjektom) si vyžiadam písomné stanovisko univerzity o tom, že predmetná licenčná zmluva nie je v rozporu s oprávnenými záujmami univerzity, a zaväzujem sa uhradiť prípadný príspevok na úhradu nákladov spojených so vznikom diela, a to až do ich skutočnej výšky.

V Brne dňa 9. mája 2016 _____

Abstract

Sojková, P. Forms of Electronic Banking and Their Use in the Slovak Republic. Bachelor thesis. Brno: Mendel University, 2016

Bachelor‘s thesis deals with the characteristics of selected forms of electronic banking, which are described in the theoretical part. Furthermore, the work aims the security and forms of attacks on electronic banking. The practical part contains an analysis of the presented forms and client satisfaction with their use and safeness. In the conclusion there are summarized the facts and there are suggested improvements.

Keywords

Electronic Banking, Internet Banking, Mobile Banking, Authentication, Security.

Abstrakt

Sojková, P. Formy elektronického bankovníctva a ich využitie v Slovenskej republike. Bakalárska práca. Brno: Mendelova univerzita v Brne, 2016.

Bakalárska práca sa zaoberá charakteristikou vybraných foriem elektronického bankovníctva, ktoré sú popísané v rámci teoretickej časti. Ďalej sa práca zameriava na zabezpečenie a formy útokov na elektronické bankovníctvo. Praktická časť obsahuje analýzu prezentovaných foriem a spokojnosť klientov s ich využívaním a bezpečnosťou. V závere práce sú zosumarizované zistené skutočnosti a návrh zlepšení.

Kľúčové slová

Elektronické bankovníctvo, Internet banking, mobile banking, autentizácia, bezpečnosť.

Obsah

Zoznam obrázkov

1 Úvod a cieľ práce

1.1 Úvod

Prudký technologický rozvoj v prvej polovici dvadsiateho storočia spôsobil zmenu aj v oblasti komunikácie. Tento rozvoj ovplyvnil všetky odvetvia a v bankovej sfére podnietil vznik nového fenoménu – elektronického bankovníctva.

Pre finančné inštitúcie je nevyhnutné zavádzať nové technológie kvôli veľkému konkurenčnému prostrediu. Bankový trh možno považovať za presýtený a získavanie nových zákazníkov je oveľa náročnejšie. Preto je rozhodujúce - poskytovať prvotriedne služby a tým si získať, ako aj udržať zákazníkov.

Rozširuje sa aj ponuka služieb, ktoré vďaka elektronickému bankovníctvu je možné vykonať bez návštevy pobočky. Ponúkané služby sa stali dôležitým nástrojom zvyšovania efektívnosti a konkurencieschopnosti bánk. V minulosti bolo možné komunikovať s bankou na diaľku prostredníctvom telefónov. V súčasnosti sa táto ponuka rozšírila aj o moderné technológie, ktorými sú počítač, mobilný telefón alebo tablet.

Elektronické bankovníctvo na Slovensku je pomerne využívaným nástrojom komunikácie klienta s bankou. Štatistiky Eurostatu (2016) ukazujú že v roku 2015 využívalo elektronické bankovníctvo 37 % klientov. Hlavný dôvod využívania elektronického bankovníctva je práve vyšší komfort komunikácie s bankou. Banky ponúkajú širokú škálu elektronických služieb za nízke alebo nulové poplatky.

S využívaním služieb elektronického bankovníctva úzko súvisí aj jeho bezpečnosť. Vhodné zabezpečovacie systémy využívané bankami vzbudzujú v klientovi dôveru.

1.2 Cieľ práce

Cieľom bakalárskej práce je analýza elektronického bankovníctva v Slovenskej republike a jeho konkrétne formy, ktoré sú využívané.

Charakteristika bankového systému Slovenskej republiky a jednotlivých služieb elektronického bankovníctva a ich trendov. Popísať bezpečnosť elektronického bankovníctva a hrozby s ním spojené.

Cieľom bakalárskej práce je aj dotazníkový prieskum, ktorý je zameraný na využívanie elektronického bankovníctva a služieb. Spokojnosť respondentov so službami a zabezpečením elektronického bankovníctva.

Zosumarizovanie odporúčaní pre efektívnejšie služby elektronického bankovníctva. Stanovenie návrhu optimálneho užívateľského rozhrania pre užívateľov.

2 Metodika

Pri písaní bakalárskej práce sme vychádzali z dostupnej domácej a zahraničnej literatúry a to monografickej, ako aj časopiseckej, z ktorej boli využité informácie pre spracovanie bakalárskej práce. Informácie boli taktiež čerpané z webových stránok bankových inštitúcií.

Využívali sme predovšetkým logické metódy skúmania, z ktorých dominovala analýza. Analýza predstavuje vedeckú metódu myšlienkového rozkladania skúmaného procesu alebo javu na menšie časti a prvky. Tieto menšie časti a prvky sú následne skúmané s cieľom zistiť ich podstatu. Hlavnou úlohou analýzy je identifikácia hlavných faktov a súvislostí, ktoré sú podstatné pri skúmaní určitých procesov (Molnář, 2012).

V predkladanej práci sme ďalej využili metódu komparácie. Komparácia spočíva v určení spoločných a rozličných znakov medzi jednotlivými javmi, procesmi a inštitúciami, ktoré sú východiskom pre kategorizáciu. Metóda komparácie bola využitá pri charakteristike služieb elektronického bankovníctva jednotlivých bánk.

Predovšetkým v praktickej časti, pri analýze využívania elektronického bankovníctva, bol využitý vlastný dotazníkový prieskum. Respondenti boli oslovovaní v časovom horizonte jedného mesiaca prostredníctvom on-line dotazníku. Otázky boli zostavené tak, aby ich formulácia bola jednoduchá, jednoznačná a neutrálna.

Analýza praktickej časti je doplnená o grafickú metódu, pomocou ktorej sme spracovali výsledky dotazníkového prieskumu. V práci boli využité koláčové grafy a stĺpcové grafy.

V rámci prvej kapitoly bakalárskej práce je popísaná stručná charakteristika bankového systému v Slovenskej republike. Kapitola následne nadväzuje na služby elektronického bankovníctva, ktoré sa využívajú v Slovenskej Republike. Ďalšiu časť predkladanej práce tvorí zabezpečenie elektronického bankovníctva, kde sú popísané základne metódy šifrovania a autentizačné metódy využívané na zabezpečenie. V poslednej časti prvej kapitoly sú charakterizované hrozby spojené s využívaním elektronického bankovníctva.

Druhú kapitolu tvorí analýza dotazníkového prieskumu, v rámci ktorej sme sa respondentov pýtali na základné otázky ohľadom využívania elektronického bankovníctva, jeho bezpečnosti a spokojnosti.

V rámci diskusie sú zhrnuté informácie ktoré sme získali dotazníkovým prieskumom, na základe ktorých sme vyvodili odporúčania pre zlepšenie služieb elektronického bankovníctva.

V závere sú stručne zhrnuté poznatky získané vypracovaním bakalárskej práce.

Ďalšiu kapitolu tvorí použitá literatúra. Práca doplnená prílohami, ktoré boli nevyhnutné k vypracovaniu bakalárskej práce.

3 Teoretická časť

V teoretickej časti bakalárskej práce je charakteristika bankového systému v Slovenskej republike, súčasne analýza elektronického bankovníctva a jeho bezpečnosť.

3.1 Bankový systém v Slovenskej republike

Bankový systém v rôznych krajinách sa líši. Rozlišujeme dva druhy bankového systému – jednostupňový bankový systém a dvojstupňový bankový systém. Slovenská republika využíva dvojstupňový bankový systém, ktorý tvorí Národná banka Slovenska a skupina komerčných bánk.

3.1.1 Národná banka Slovenska

Národná banka Slovenka bola založená ako nezávislá centrálna banka Slovenskej republiky podľa zákona o Národnej banke Slovenska. Súčasťou Eurosystému sa stala 1. januára 2009. Tvorí prvý stupeň bankového systému na Slovensku. Hlavným cieľom Európskej centrálnej banky spolu s ostatnými bankami eurozóny je udržiavanie cenovej stability. Ďalšími úlohami Slovenskej národnej banky v rámci Eurosystému je prispievať k zabezpečovaniu:

- menovej politiky
- devízových operácií a devízových rezerv
- vydávania eurových bankoviek a mincí
- platobného styku
- zberu a zostavovania štatistík
- medzinárodnej spolupráce
- vzájomnej spolupráce a podpore centrálnych bánk
- finančnej stability v eurozóne. (NBS, 2016)

Jednou z hlavných úloh centrálnej banky je taktiež vykonávanie regulácie a dohľadu nad finančným trhom. Cieľom je stabilizovanie bankového sektora a ďalšie funkcie ako napríklad vydávanie licenčných podmienok, pravidiel pre činnosť bankového sektora (NBS, 2016).

3.1.2 Komerčné banky

Komerčné banky tvoria druhý stupeň bankovej sústavy. Bankami v zmysle zákona sú *„právnické osoby so sídlom v SR, ktorá je úverovou inštitúciou podľa osobitného predpisu, a ktorá má bankové povolenie*“ (Zákon č. 483/2001 Zb., 2016).

Banku možno charakterizovať ako finančného sprostredkovateľa, ktorého hlavnou náplňou je prijímanie vkladov, poskytovanie úverov a vykonávanie platobného styku (Revenda, 2016).

Hlavnou funkciou komerčných bánk je finančné sprostredkovanie. Funkcia je vykonávaná na ziskovom princípe. Druhou hlavnou funkciou je vykonávanie bez-

hotovostného platobného styku. Banky vedú účty klientom, ktorý môžu uskutočňovať platby bezhotovostným prevodom (EuroEkonóm.sk, 2015).

Komerčné bankovníctvo na Slovensku tvorí 14 bánk so sídlom v Slovenskej republike a 13 bánk pôsobiacich na Slovensku ako pobočky zahraničných bánk (NBS, 2016).

Operácie bánk môžeme rozdeliť na aktívne a pasívne. Aktívne a pasívne služby bánk môžu byť poskytované aj elektronickou formou. Nasledujúca kapitola sa venuje elektronickému bankovníctvu.

3.2 Elektronické bankovníctvo

Elektronické bankovníctvo možno v súčasnosti považovať za fenomén doby. Využíva sa podstatne viac ako v minulosti. Elektronické bankovníctvo dnes expanduje. Nárast je spätý s rastom počtu klientov, ktorí elektronické bankovníctvo využívajú, ale aj s nárastom realizovaných transakcií. Tieto zmeny sú sprevádzané rozvojom siete, ktorá podmieňuje elektronické bankovníctvo (Polouček, 2013).

Využívané formy elektronického bankovníctva bývajú označované aj ako prostriedky vzdialeného prístupu. Umožňujú využívanie klasických bankových produktov elektronicky. Nejedná sa o nové produkty, ale zmenil sa len proces ich zjednania, využitia či ukončenia, ktorý bol prevedený do elektronickej podoby (Polouček, 2013).

Za výhody elektronického bankovníctva môžeme považovať zavádzanie nových komunikačných technológií, čo má prínos pre zákazníka ako aj pre banku. Výhodou je napríklad možnosť komunikácie odkiaľkoľvek a kedykoľvek, služby je možné objednávať a platiť cez Internet, zvyšuje sa produktivita a rastie ekonomické bohatstvo (Máče, 2006).

3.2.1 Platobné karty

Prvá podoba platobnej karty, ako ju poznáme dnes, bola vydaná v roku 1951 v Amerike, kedy boli karty používané americkými bankami na vymedzenom území. Bankám išlo o zárobkovú činnosť. Neskôr, v roku 1961, Bank of America spúšťa program Bank Americard, čo je prvá kartová asociácia niekoľkých bánk. Bank Americard boli predchodcami Visa Intrernational (Schlossberger, Hozák, 2005).

Platobné karty sú plastikové karty odpovedajúce medzinárodným normám, ktoré oprávnený držiteľ môže využívať na vykonávanie bezhotovostných platieb a výberov hotovostí z bežného účtu. Platobné karty sú vždy majetkom banky, ktorá kartu vydala (Polouček, 2013).

Platobná karta musí obsahovať označenie vydavateľa, meno držiteľa karty, platnosť karty a záznam dát, ktoré môžu mať formu magnetického krúžku alebo mikročipu. Platobné karty môžeme využívať na výber hotovosti v bankomate alebo v pobočkách bánk. Môžeme nimi priamo platiť za tovar v obchode alebo na internete. Bezhotovostne sa kartou v súčasnosti dá platiť takmer kdekoľvek (Schlossberger, Hozák, 2005)

Delenie platobných kariet podľa zúčtovania:

1 Debetné karty

Najčastejšie využívanie platobných kariet, kedy sú karty späté s bežným účtom v banke. Využívajú sa na platenie priamo u obchodníka, alebo na internete, alebo na výber z bankomatu. Čerpajú peniaze uložené na bežnom účte užívateľa (Přádka, 2000).

2 Kreditné karty

Karta nie je napojená na bežný účet, ale peniaze sú požičiavané od banky a tento úver je následné splácaný spolu s úrokmi. Pre kreditné karty nie je potrebné mať zriadený účet a sú často vydávané nebankovými subjektami. Držiteľ môže svoje záväzky voči banke uhradiť v tzv. bezúročnom období, v rozmedzí 30 -54 dní (Přádka, 2000; Schlossberger, Hozák, 2005).

3 Charge karty

Charge kary možno označiť ako „platenie na faktúru“, kedy vydavateľ po určitej dobe spočíta všetky čerpané položky a pošle faktúru na uhradenie. Na zaplatenie je určená doba, obyčajne 14 dní. Napr. American Express (Přádka, 2000).

3.2.1.1 Cash Back

Cash Back je služba, vďaka ktorej si môžeme vytiahnuť hotovosť aj v obchode. Cash Back funguje nasledovne: obchodník vystaví predajný doklad na vyššiu čiastku ako je cena nakúpeného tovaru a rozdiel je vyplatený v hotovosti z pokladne (Přádka, 2000).

Na Slovensku sa Cash Bank neteší priveľkej popularite, aj keď je poskytovaný niektorými bankami, ako napríklad Slovenskou sporiteľňou. Službu ponúkajú banky vo vybraných supermarketoch a obchodných domoch alebo aj v maloobchodnej predajnej sieti. Stačí nakúpiť minimálne za 5 euro, oznámiť predajcovi výšku požadovanej sumy, maximálne však 50 euro. Treba dbať na denný limit, do ktorého je zahrnutý aj výber prostredníctvom Cash Back. Ďalšou bankou, ktorá poskytuje Cash Back, je ČSOB. Podmienky pre výber hotovosti sú zhodné so SLSP. Avšak ČSOB účtuje klientovi 20 eurocentov za výber prostredníctvom Cash Back, pričom SLSP účtuje 10 eurocentov za výber. Službu Cash Back využíva aj Poštová banka. Poštová banka neúčtuje žiadne poplatky pre využívanie služby (ČSOB, 2016; SLSP, 2016; Poštová Banka, 2016).

3.2.1.2 Bankomaty

Bankomaty sú prístroje, ktoré slúžia na výber alebo vklad hotovosti z účtu klienta pomocou platobnej karty. Sú vybavené klientskou a operátorskou zónou. V rámci klientskej resp. obslužnej zóny, je prístroj vybavený monitorom a klávesnicou, čítačkou kariet, výplatným slotom a tlačiarňou účteniek. Operátorská časť je zložená z trezoru, výplatného a kódovacieho mobilu. Táto časť je určená pre obsluhu bankomatu. V dnešnej dobe sú bankomaty multifunkčnými zariade-

niami, ktoré majú aj iné funkcie ako len výber a vklad hotovosti. Vlastník platobnej karty môže prostredníctvom bankomatu po zadaní svojho PIN kódu zistiť zostatok na účte, dobyť kredit na mobile alebo svoju elektronickú peňaženku, vykonať vklad, vytlačiť darčekový kupón, požiadať o pôžičku, zmeniť PIN kód, získať informácie o platnosti karty alebo marketingové informácie a ponuky banky. Bankomaty sú vybavené možnosťou obsluhy pre nevidiacich. Zabezpečenie bankomatov je konštruované spôsobom zamedzenia ich poškodenia. Z bezpečnostných dôvodov sú ukotvené k zemi špeciálnymi úchytmi. Bankomaty sú taktiež vybavené aj bezpečnostnými kamerami monitorujúcimi nedovolenú manipuláciu (Klufa, 2013).

Bankomaty sú využívané všetkými bankami na Slovensku, avšak Tatra Banka ako prvá zaviedla výber hotovosti z bankomatu prostredníctvom mobilu. Výber z bankomatu je súčasťou mobilnej aplikácie Tatra Banky. Aplikácia skracuje čas s manipuláciou bankomatov Tatra Banky nasledovne: V aplikácii prostredníctvom záložky „Výber z bankomatu“ zvolíte jednu z najčastejšie vyberaných súm alebo zadáte vlastnú sumu. V prípade, že klient vlastní viaceré účty, je možné zvoliť si z ktorého účtu budú peniaze vybrané. Pri bankomate je potrebné stlačiť akékoľvek tlačidlo, zadať numerický kód, ktorý je vygenerovaný pre konkrétny výber aplikáciou a vybrať si bankovky. Kód je platný 20 minút od vytvorenia (TB, 2016).

3.2.2 Phonebanking

Phonebanking umožňuje klientovi komunikovať s bankou pomocou telefonického zariadenia. Telefonický rozhovor môže prebiehať dvoma formami, a to komunikáciou s automatickým telefónnym systémom alebo prostredníctvom komunikácie s telefónnym bankárom (MFSR,2014). Špecializované pracovisko býva označované ako call centrum, ktoré normálne funguje 24 hodín denne. Telefonát je zaistený heslami, ktoré pozná len klient a banka, pričom z dôvodu možného odpočúvania heslá nie sú použité v celku. Súčasťou služieb je aj poskytovanie automatizovaných hlasových informačných systémov, na ktorých prebieha jednoduchšia časť komunikácie medzi klientom a bankou. Výhodou phonebankingu je rýchlosť a úspora času. Ďalšou výhodou je, že nevyžaduje žiadne špeciálne technické vybavenie. Nevýhodou je malá ponuka služieb a riziko zneužitia disponovania s účtom prostredníctvom telefónu. (Polouček, 2013)

Operácie, ktoré je možné vykonávať prostredníctvom phonebankingu môžeme rozdeliť na aktívne a pasívne. Medzi aktívne operácie radíme príkaz k úhrade, vytvorenie trvalého príkazu k úhrade, zriadenie príkazu alebo trvalého príkazu k inkasu, možnosť zahraničného platobného styku a založenie, zmenu alebo zrušenie termínovaného vkladu. Za pasívne operácie považujeme zistenie zostatku na účte, informácie o pohyboch na účte, informácie o zadaných aj nevykonaných transakciách, informácie o produktoch a službách banky, výšku úrokových sadzieb a kurzový lístok (Přádka, 2000).

3.2.3 GSM Banking

Nasledujúca forma GSM banking je komunikácia s bankou, ktorá môže byť realizovaná:

a. prostredníctvom zašifrovaných **SMS správ –** klient banky môže prostredníctvom štruktúrovaných SMS správ odosielať požiadavky k získaniu informácií alebo príkazy na vykonanie. Banka odošle odpoveď SMS správou, ktorá obsahuje požadované informácie. Užívateľ môže byť o dianí na svojom účte informovaný automaticky alebo po vykonaní operácie je užívateľovi zaslaná správa. Klient si môže od banky vyžiadať pomocou naformátovanej správy potrebné informácie. Banka správu spracuje a klientovi odpovie (Přádka, 2000)
b. prostredníctvom technológie **SIMToolkit** – banka nahrá na simkartu mobilného telefónu vlastnú bankovú aplikáciu, ktorá bude dostupná v mobilnom telefóne. Pri nahrávaní je SIM karta zašifrovaná a nedajú sa z nej získať žiadne informácie. Zároveň je prístup chránený aj bankovým PIN nazývaným aj BPIN. V dnešnej dobe je technológia SIMToolkit postupne nahrádzaná smart aplikáciami. (Polouček, 2013)
c. s využitím technológie **WAP –** táto služba spočíva v komunikácii prostredníctvom internetu pomocou protokolu WAP (Wireless Application Protocol). Jedná sa o kombináciu telefónneho a internetového bankovníctva. Mobilné telefóny podporujúce službu WAP majú prístup na WAPové stránky banky, čo sú v podstate klasické stránky banky upravené na mobilnú verziu (Přádka, 2000).

3.2.4 Smartbanking

Smartbanking predstavuje mobilné aplikácie pre inteligentné telefóny a tablety založené na internetovom pripojení. Služba je možné si stiahnuť do mobilného telefónu alebo tabletu. Aplikácie slúžia na zisťovanie zostatkov a obratov na účtoch, zadávanie príkazov k úhrade alebo povolenie k inkasu, zadanie platby pre kreditnú kartu, objednávky výberov hotovosti na pobočke, dobíjanie kreditu, zjednanie cestovného poistenia alebo zisťovanie kurzov mien, nájdenie najbližšej pobočky a bankomatu a iné. Prostredníctvom aplikácie je možné vziať si úver. V súčasnosti príkazy na úhradu je možné vyplňovať aj pomocou QR kódu alebo odfotením IBANu. Pomocou aplikácie je možné si vytvoriť platobnú kartu s vlastným motívom. Mobilné aplikácie konkrétnych bánk sa líšia ponúkanými funkciami, dostupnosťou v cudzom jazyku alebo operačným systémom mobilu. Pre najbežnejšie operačné systémy (android, iOS) ponúkajú aplikácie všetky slovenské banky zadarmo (Klufa, 2013).

Výhodou mobilného bankovníctva je jeho všade prítomnosť, čo znamená, že jeho služby sú dostupné kdekoľvek, čím vytvárajú nové príležitosti pre spĺňanie potrieb zákazníkov. Ďalšou výhodou je jeho lokalizácia, kedy GPS technológia

umožňuje lokalizáciu užívateľa, ktorou je možné prispôsobiť ponuku služieb a komunikáciu užívateľovým potrebám (Ha, Canedoli, W. Baur, Bick, 2012).

Obr. 1 ČSOB Smartbanking (Chabada, 2011)

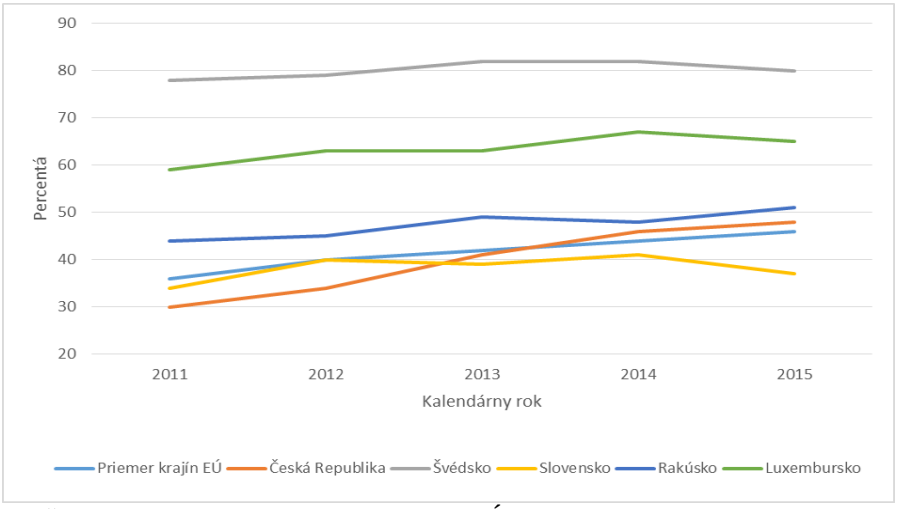
3.2.4.1 VIAMO

VIAMO je spôsob vykonávania platieb z mobilu na mobil. Platby sú obmedzené limitom do 200€. Osoby, ktorých banka podporuje túto službu, môžu vďaka svojmu mobilu posielať peniaze medzi sebou. Funkcia je označená ako *Platba osobe*. Stačí vybrať spomedzi kontaktov ten, ktorému chceme poslať peniaze, zadať sumu, ktorú je nutné potvrdiť PIN kódom a odoslať. Mobilné číslo musí mať klient prepojené so svojím účtom v banke. Obdobne je možné platiť aj v obchodoch, ktorých je ale obmedzené množstvo. V rámci Slovenskej republiky máme tri banky, ktoré využívajú službu VIAMO, sú to Tatra Banka, VÚB a ZUNO banka. VIAMO je poskytovaná zdarma (Viamo, 2016).

3.2.5 Internetbanking

Aplikácia nevyžaduje špeciálny hardware a platobný styk je vykonávaný prostredníctvom internetu. Pri splnení technických požiadaviek osobného počítača a uzatvorení zmluvy o poskytovaní tejto služby je užívateľ schopný sa hneď prihlásiť do systému. Klient sa prihlasuje do systému banky a po overení oprávnení má prístup k vykonávaniu požadovaných úkonov. Prístup do internetbankingu umožňuje prenos informácií o účtoch, zadávanie platobných príkazov, získavanie informácií z banky, zakladanie, zriaďovanie a rušenie termínových vkladov a pod. Internetbanking avšak vyžaduje vysoký stupeň ochrany prenosu dát. (Poloučeк,2013; Schlossberger, Hozák, 2005)

Na nasledujúcom grafe môžeme vidieť využívanie internetového bankovníctva vo vybraných krajinách Európy a európsky priemer vo veku 16 až 74 rokov. Slovenskú republiku možno považovať za priemernú vo využívaní elektronického bankovníctva.

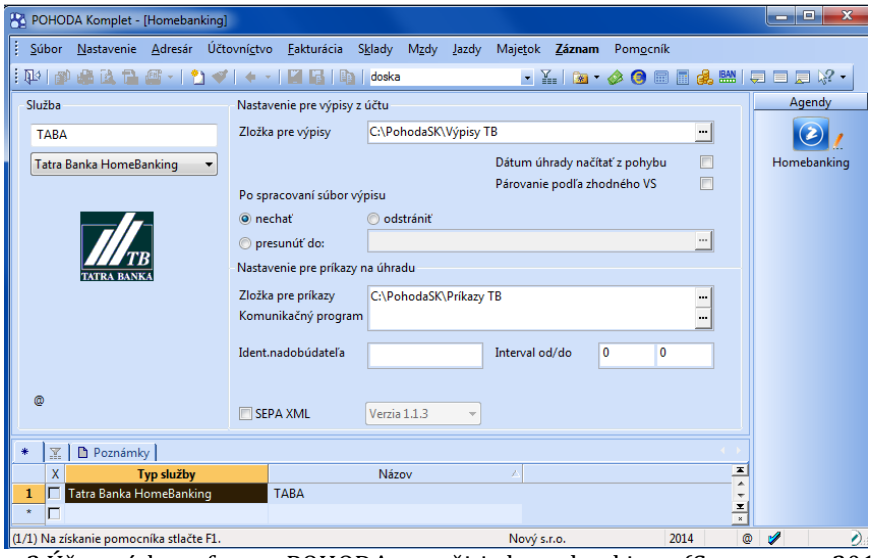


Obr. 2 Podiel používania internetového bankovnícva v EÚ v % vo veku od 16 do 74 (Eurostat, 2016)

3.2.6 Homebanking

Homebanking je založený na prepojení počítačového systému klienta s informačným systémom príslušnej banky po vyhradených dátových linkách. Homebanking môže mať podobu rôzne vyspelých elektronických služieb vylučujúcich akýkoľvek papierový kontakt medzi bankou a klientom. K prevádzke sa využíva pevné spojenie informačných aplikácií klienta a banky. Za výhodu homebankingu môžeme považovať, že je bezpečnejší ako iné aplikácie. Všetky nami vykonávané operácie sú off-line a po skončení dochádza ku spojeniu s bankou cez internet a prenosu dát. Nevýhodou homebankingu je jeho neprenosnosť. Možno ho využívať len z počítača, na ktorom je software nainštalovaný. Klient nemá k svojmu účtu pohodlný prístup z ľubovoľného miesta (MFSR, 2014). Prostredníctvom homebankingu môže klient využívať aj širokú škálu bankových služieb. Akými sú získavanie aktuálnych informácii o stave na účtoch, zadávanie domácich a zahraničných príkazov k úhrade, prepojenie informačného systému klienta a banky, prepojenie s účtovnými systémami a vyhľadávanie informácií o kurzoch na devízovom trhu, vývoj na akciových trhoch a pod (Polouček, 2013; Přádka, 2000).

V súčasnej dobe je homebanking u bežných používateľov nahrádzaný internetbankingom a homebanking je využívaný prevažne väčšími firmami, ktoré systém prepájajú so svojím účtovníckym softvérom.



Obr. 3 Účtovnícky software POHODA - využitie homebankingu (Stormware, 2014)

3.2.7 E-commerce

E-commerce, alebo inak aj online platby na internete sú aktuálnym a čoraz viac rozširujúcim sa trendom v elektronickom bankovníctve. Na platenie cez internet sa využívajú platobné brány. V minulosti boli platby platobnými bránami považované za nebezpečné, keby bolo možné zneužitie karty klienta. Obchodník mal prístup k osobným údajom klientovej platobnej karty. Práve z tohto dôvodu začali vznikať platobné brány. (Tučková, 2015). Komerčné e-shopy akceptujú online platby prostredníctvom platobných brán namiesto vlastných platobných systémov (Kumar, Thabrez, 2015). Nasledujúci text je venovaný platobným metódam, ktoré sú využívané na platenie na internete.

Platobná karta

Najpopulárnejšou platobnou metódou na internete **je platenie platobnou kartou.** Platobné brány podporujú platobné karty využívané na Slovensku (MasterCard, Visa, Maestro) a tiež podporujú sprievodné funkcie (opakované platby, pred autorizácia). Platobné karty sú radené medzi online platobné metódy (GOPAY, 2016).

Medzi ďalšie výhody patrí rýchlosť spracovávanej transakcie spolu s potvrdením platby, ľahká používateľnosť, bezpečnosť a využívanie funkcie 3D Secure. Platby vykonané na internete pomocou platobnej karty sú chránené prostredníctvom jednorazového kódu, ktorý banka bezplatne doručuje formou SMS správy majiteľovi karty (Securepay, 2016).

Online platobné tlačidlá - ePay

Ide o platbu na internete s vopred vyplneným platobným príkazom. Platba prebieha online v rámci jednej platobnej inštitúcie. Výhodou je okamžitá úhrada čiastky, eliminácia chybného zadania platobného príkazu. Platba je vykonávaná z vlastného internetového bankovníctva. Túto platobnú metódu využíva napríklad Slovenská

sporiteľňa, služba sa nazýva Sporopay. Služba je poskytovaná zdarma, podmienkou je využívanie internetbankingu. Pri platbe prostredníctvom Sporopay sme automaticky presmerovaný na e-platby Slovenskej sporiteľne, kde je vopred pripravený vyplnený formulár. Pre potvrdenie platby je potrebné zadať kód z GRID karty alebo SMS kľúča. Po vykonaní platby sme naspäť presmerovaný na stránky predajcu (GOPAY, 2016; SLSP, 2016).

E-platby poskytuje Tatra Banka (TatraPay), VÚB (E-platby VÚB), ČSOB (Platobné tlačidlo).

Bankové prevody

Bankový prevod je stále obľúbenou metódou platenia na internete. Platbu je možné vykonať kedykoľvek, ale spracovaná je v rámci úradných hodín konkrétnej banky (GOPAY, 2016).

Mobilné platby

Mobilné platby je možné realizovať prostredníctvom mobilného telefónu. Sú praktické pri úhradách menších čiastok. Túto službu poskytuje Tatra Banka v spolupráci s mobilnými operátorom O2 a Orange Slovensko. Mobilný telefón musí podporovať službu NFC[1]. Stačí požiadať operátora o NFC SIM kartu a mať aktivovanú službu *Bezkontaktné mobilné platby*. Službu je možné aktivovať si na pobočke Tatra Banky alebo cez kontaktné centrum. Platba prebieha jednoduchým priložením mobilu k terminálu (TB, 2016).

Mobilné platby taktiež poskytuje aj VÚB banka prostredníctvom aplikácie Wave2Pay, ktorá premieňa mobilný telefón na platobnú kartu. Platba je vykonaná rýchlo a bezpečne priložením telefónu k terminálu tam, kde sa dá platiť bezkontaktne. Služba Wave2Pay je poskytovaná aj formou nálepky. Nálepku je možné si objednať a vyzdvihnúť na vami zvolenej pobočke. K nálepke je možné stiahnuť si aplikáciu Wave2Pay, vďaka ktorej získame prehľad o platbách s nálepkou. Zobrazuje aj zostatok na účte s možnosťou nálepku aktivovať alebo deaktivovať (VÚB, 2016).

Elektronická peňaženka

Slúži predovšetkým na drobné platby. Klient si čipovú kartu nabije s možnosťou využitia karty aj na iné funkcie. V prípade, že karta slúži výhradne ako elektronická peňaženka, nie je zabezpečená PIN kódom a dokonca nie je vedená ani na určité meno, teda môže byť využívaná viacerými členmi rodiny alebo zamestnancami firmy. Výhodou je nevyhnutnosť nosiť pri sebe drobné mince a peniaze. Platenie sa stáva rýchlejším, čo je taktiež aj výhoda pre obchodníkov, ktorí sa vyhnú vysokým poplatkom za transakcie vykonávané kartami s magnetickým prúžkom. Najznámejšími elektronickými peňaženkami sú PayPall, Google Wallets, Amazon (Laha Roy, 2013).

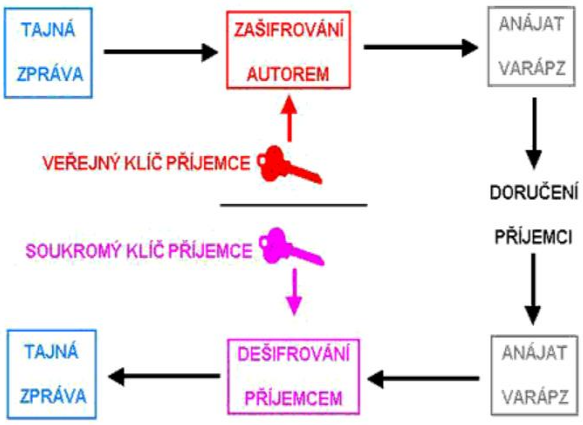
[1] NFC (z angl. Near Field Communication – „komunikácia na krátke vzdialenosti“) podobný technológii Bluetooth. (Faulkner, 2015)

Príkladom elektronickej peňaženky môže byť Skrill. Na Skrille je možné si založiť účet zadarmo. Ponúka aj zriadenie platobnej karty, ktorú možno využiť na bplatenie a výber z bankomatov. Skrill ponúka medzinárodné posielanie peňazí za nízke poplatky. Posielanie a prijímanie peňazí je možné vykonávať prostredníctvom e-mailovej adresy. Stačí, ak má užívateľ založený účet, môže posielať a prijímať peniaze uvedením konkrétnej čiastky a e-mailovej adresy. Platbu kartou od Skrillu je možné uplatniť na všetkých platobných miestach, kde sa využíva Mastercard. Platby vykonané prostredníctvom Skrillovej peňaženky je možné kontrolovať prostredníctvom aplikácie, ktorá je dostupná pre počítače, mobilné telefóny a tablety (Skrill, 2011).

3.3 Bezpečnosť elektronického bankovníctva

Princíp komunikačnej výmeny spočíva v zašifrovaní dát odosielaných odosielateľom a následne v odšifrovaní prijímateľom. Využíva sa veľké množstvo techník a metód podľa požiadavky na zaistenie. Pre elektronické bankovníctvo je nevyhnutné nájsť správne zabezpečenie systému, ktorému bude klient dôverovať.
Šifrovaním označujeme algoritmus, ktorým utajujeme dáta pomocou šifrovania. Využívame pritom šifrovací kľúč, ktorý býva zvyčajne tajný (Vondruška, 2006).

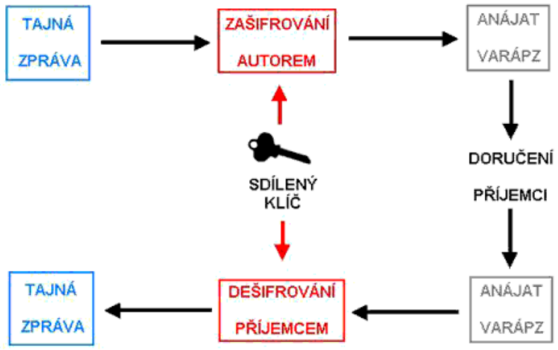
Asymetrické šifrovanie
Komunikačné strany majú vytvorenú dvojicu kľúčov. Jeden z nich je uchovaný v tajnosti (označovaný ako súkromný alebo privátny kľúč) a druhý je poskytnutý každému, kto má záujem o komunikáciu (verejný kľúč). V prípade odoslania správy osoba využije verejný kľúč a s jeho pomocou správu zašifruje. Správa je odoslaná príjemcovi, ktorý na rozšifrovanie využije svoj súkromný kľúč. Algoritmus nám zabezpečuje, že správa zašifrovaná verejným kľúčom sa s ním nedá rozšifrovať. Je potrebné použiť druhý kľúč (Doseděl, 2004).



Obr. 4 Asymetrické šifrovanie (Náderníček, 2003)

Symetrické šifrovanie

Symetrické šifrovanie inak označované aj ako konvenčné šifrovanie. Daný typ šifrovania je oveľa rýchlejší ako asymetrické šifrovanie. K šifrovaniu a dešifrovaniu správ sa využíva jeden a ten istý kľúč. Symetrické šifry môžeme rozdeliť na dve kategórie - prúdové a blokové. Pri prúdových šifrách šifrovanie prebieha bit po bite, pričom každý bit je zvlášť zašifrovaný aj dešifrovaný. Po kompletnom dešifrovaní je správa zlúčená do čitateľnej podoby. Blokové šifrovanie je rozšírenejšie, ktoré bitový sled rozdelí na bitové slová, ktoré sú vhodne doplnené bitovou šifrou tak, aby mali všetky slová zhodnú veľkosť (Baar, 2016).



Obr. 5 Symetrické šifrovanie (Náderníček, 2003)

Identifikácia užívateľa je proces určenia totožnosti užívateľa. Identifikácia môže byť zisťovaná zadaním údajov užívateľa alebo snahou systému určiť identitu z predom vybranej množiny užívateľov. Systém prechádza databázu všetkých užívateľov na základe biometrických informácií (napr. otlačky prstov), alebo tajných informácií ako napríklad identifikačný kód (Matyáš, Krhovják, 2008).

Autentizácia užívateľa je proces, kedy užívateľ udáva svoju identitu, napr. prihlasovacie meno, následne umožní jej overenie. Systém porovnáva udané charakteristiky s uloženými charakteristikami, ktoré zodpovedajú identite podľa záznamov v databáze (Matyáš, Krhovják, 2008).

Autorizácia užívateľa je proces priradenia oprávnenia pre prácu v systéme a špecifikuje právomoci užívateľa. Autorizácia nasleduje po autentizácii. Hlavnou úlohou autorizácie je overiť, či má užívateľ oprávnenie vykonať príslušnú akciu (Trisul, 2005-2016).

Autentizačné metódy

Heslá a jednorazové heslá

Heslo tvorí najjednoduchšiu autentizáciu spomedzi ostatných. Heslo je tvorené z reťazca dlhého 6 – 10 znakov, najlepšie netriviálneho a ľahko zapamätateľného užívateľom. Užívateľ predkladá heslo spolu s prihlasovacím menom – loginom systému, ktorý tieto údaje kontroluje s databázou (Matyáš, Krhovják, 2008).

Sú kladené rôzne aspekty na tvorbu hesla. Kvalita hesla je závislá na okolnostiach a použití. Bežné zásady na tvorbu hesla – najmenej 8 znakov, kde využijeme malé aj veľké písmená, číslice a špecifické znaky. Heslo by malo byť ľahko zapamätateľné, ľahko napísateľné ale ťažko uhádnuteľné, heslo nikdy nikomu neprezradíme, nikam si ho nezapisujeme a neukladáme. Vhodné je použitie rôznych hesiel pre rôzne systémy a taktiež je vhodné heslo raz za čas meniť (Vondruška, 2006).

Jednorazové heslo tvorí zreťazenie dvojice statického hesla zadaného užívateľom a náhodne vygenerované dostatočne veľké číslo. Dvojica je zašifrovaná, aby pri prenose neprišlo k zmene a tým získame informáciu, ktorá sa pri ďalšej autentizácii zmení (Doseděl, 2004).

Autentizačné tokeny

Token je zariadenie, ktoré je možné nosiť neustále so sebou a je nevyhnutné pre autentizáciu do systému. Tokeny majú špecifické fyzikálne vlastnosti, obsahujú tajné informácie, alebo sú schopné vykonávať výpočty.

Najčastejšími tokenmi sú karty. Môžeme ich deliť na niekoľko typov podľa obsahu a schopnosti. Najjednoduchšie sú karty s magnetickým pruhom, naopak zložitejšie a drahšie sú čipové karty (Matyáš, Krhovják, 2008).

Biometria

Biometrické technológie sú založené na meraní fyziologických vlastností ľudského tela (otlačok prsta, dúhovka alebo sietnica oka) alebo chovanie človeka (hlasová vzorka, dynamika podpisu). Systémy, využívajúce biometriu, sú spravidla spoľahlivejšie, presnejšie a uľahčujú komunikáciu s bankou. Využívajú sa dve základné operácie. Identifikácia klienta pre overenie klienta a druhá operácia, kedy identifikačná zložka slúži na potvrdenie právneho vzťahu. Výhodou pre klienta je rýchlosť, jednoduchosť a dostupnosť informácií bez použitia iných zariadení ako sú karty s certifikátmi. Pre obsluhu je výhodou ak ide o efektivitu, rýchlosť a celkovú produktivitu. Ak predchádzajúce parametre rastú, tým je obsluha spokojnejšia, pretože plní kritériá, podľa ktorých ich klienti hodnotia. Biometria znižuje riziká spojené s jednoznačnou identifikáciou osôb a je posilnená prevenciou proti falšovaniu identít a vykonávaniu neoprávnených operácií (Verecký, 2012).

Ako príklad môžeme uviesť Tatra Banku, ktorá využíva hlasovú biometriu ako spôsob identifikácie užívateľa. Prihlásenie sa do mobilnej aplikácie prostredníctvom otlačku prsta je možné v UniCredit banke. Avšak mobilný telefón musí danú funkciu podporovať (TB, 2016; Unicredit bank, 2013).

Trojfaktorová autentizácia

Jednofaktorovú autentizáciu tvorí napríklad meno a heslo. V prípade dvojfaktorovej autentizácie využívame predmet (token), kde je potrebná znalosť PIN kódu. Najvyšším stupňom bezpečnosti je trojfaktorová autentizácia, kedy ku dvojfaktorovej autentizácii pridávame špecifickú vlastnosť užívateľa. Napríklad môže ňou byť charakteristika očnej sietnice (Ludvík, 2016).

Postup trojfaktorovej autentizácie podľa Matyáša, Krhovjáka (2008) je uvedený v nasledujúcich krokoch:

1. Klient vloží token do zariadenia na autentizáciu.
2. Zadá PIN do autentizačného zariadenia, ktorý je priamo zaslaný do tokenu.
3. PIN je overený tokenom.
4. Klient vkladá svoju biometrickú informáciu (napr. otlačok prsta) do tokenu priamo, alebo prostredníctvom autentizačného zariadenia.
5. Token spracováva biometrickú informáciu a porovnáva ju s uloženým vzorom.
6. Token zahajuje komunikáciu protokolom výzva-odpoveď so systémom, do ktorého sa klient autentizuje a sú použité dôverné dáta, ktoré generuje a uchováva token.
7. Po úspešnom ukončení protokolu je klient autentizovaný.

Certifikáty

Certifikáty sú využívané z hľadiska vyššej bezpečnosti pri autentizácii užívateľov, pričom je využívaná asymetrická kryptografia (digitálny podpis). Certifikát je súbor dát, ktorý okrem verejného kľúča obsahuje aj identifikáciu vlastníka. Užívateľ vlastní kľúčový pár, tzv. súkromný a verejný kľúč, kde verejný kľúč je certifikovaný konkrétnou bankou a súkromný kľúč je uložený na kryptografickej čipovej karte a chráni prístup k PIN. Operácie, pre ktoré je digitálny podpis potrebný, prebiehajú vo vnútri karty, čo zabezpečuje bezpečné výpočtové prostredie (Doseděl, 2004).

Elektronický podpis

Pre vytvorenie elektronického podpisu sa využívajú asymetrické šifrové algoritmy. Je vytvorená dvojica kľúčov súkromný a verejný. Verejný kľúč je zaevidovaný u autority - predložený osobou a je k nemu vytvorené potvrdenie, tzv. certifikát. Súkromným kľúčom vlastník vykoná s otvoreným textom transformáciu nazývanú elektronický podpis. Ten, kto vlastní verejný kľúč môže s jeho pomocou overiť elektronický podpis, ktorý bol vytvorený za pomoci odpovedajúceho súkromného kľúča. Vlastník je zrejmý z evidencie verejného kľúča a držiteľ súkromného kľúča nemôže poprieť vlastníctvo elektronického podpisu pretože je jediným vlastníkom súkromného kľúča (Vondruška, 2006).

3.4 Riziká používania elektronického bankovníctva

S rastúcim trendom internetového bankovníctva vzrastajú aj nebezpečenstvá útokov na bankové účty klientov. Ich cieľom je vylákanie potrebných informácií na prihlásenie do systému alebo zneužitie PIN platobnej karty. Útoky sú čoraz bežnejšie. Banky sa snažia chrániť svojich klientov a informovať ich o nebezpečenstvách. V nasledujúcom texte sú uvedené najbežnejšie typy útokov.

Phishing

Phishingom sú označované podvodné e-maily, prostredníctvom ktorých sa útočník snaží vylákať dôverné informácie od užívateľa. Útočník sa snaží vyvolať dojem, že e-mail bol odoslaný organizáciou, ktorá sa snaží vylákať dôverné informácie. Text e-mailu môže vyzerať aj ako informácia o nevykonanej platbe, výzva k aktualizácií bezpečnostných údajov, oznámenie o dočasnom zablokovaní účtu, či platobnej karty, výskum klientskej spokojnosti alebo elektronický bulletin pre klientov. V texte správy sa nachádza link, ktorý na prvý pohľad vyzerá ako odkaz na stránku banky. V skutočnosti odkazuje na iné miesto, kde sú umiestnené podvodné stránky (Hoax.cz, 2000-2016).

Pharming

Pharming je sofistikovanejší útok. Cieľom útoku je automatické presmerovanie na stránky útočníka. Môže ísť o repliku stránok bankových inštitúcií a slúžiť napríklad ku získavaniu prihlasovacích údajov (Matyáš, Krhovják, 2008).

V prípade poskytnutia prihlasovacieho mena a hesla, ak nie je účet klienta ďalej zabezpečený, útočník môže nepozorovane prevádzať peniaze z účtu (Bezpecny-internet.cz, 2016).

Spyware

Spyware taktiež označovaný ako „nechcené technológie“ inštalované bez povolenia užívateľom alebo sú realizované tak, že nejakým spôsobom poškodzujú užívateľa – napríklad ovplyvňovaním súkromia užívateľa alebo bezpečnosti systému. Ich úlohou je používanie systémových zdrojov vrátane nainštalovaných programov alebo zbieranie a odosielanie ich osobných a inak citlivých informácií (Hlaváč, 2005).

Spyware sa dostáva do počítača v podobe trojského koňa alebo ako pribalený škodlivý kód k inému programu (Matyáš, Krhovják, 2008).

Libanonská slučka

Ide o útok na platobnú kartu klienta, kedy útočník vhodne umiestni videopásku do štrbiny pre vkladanie bankomatovej karty do bankomatu. Ak je karta vložená, páska ju zadrží tak, že nie je schopná ďalšieho pohybu. Útočník sa priblíži k obeti s pomocou, kedy obeti poradí opätovne zadať PIN kód. Po odchode obete, ktorá ide nahlásiť problém, vytiahne kartu z bankomatu a s pomocou PIN kódu vyberie z účtu peniaze ešte pred jej zablokovaním (Matyáš, Krhovják, 2008).

4 Praktická časť

V predchádzajúcej časti bakalárskej práce sú zhrnuté základné poznatky o elektronickom bankovníctve. Venovali sme sa využívaným formám ako je internet banking, phonebanking a mobile banking. Kapitola sa venovala aj formám zabezpečenia elektronického bankovníctva a spôsobom útokov. Nasledujúca časť sa zaoberá vyhodnotením dotazníkového prieskumu, ktorého otázky korešpondujú s teoretickými poznatkami.

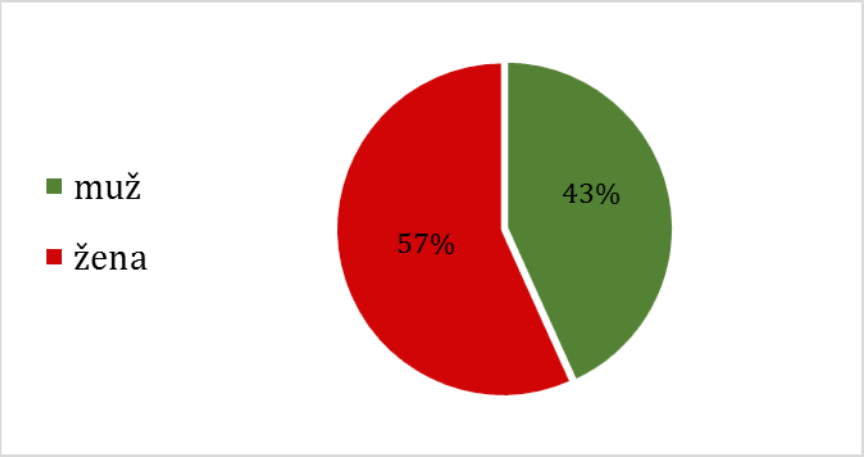
4.1 Elektronické bankovníctvo v Slovenskej republike

V nasledujúcej časti bakalárskej práce budeme analyzovať využívanie elektronického bankovníctva na Slovensku prieskumom, ktorý pozostával z anonymného dotazníka. Dotazníkový prieskum je súčasťou cieľa predkladanej bakalárskej práce. Dotazníkový prieskum sa realizoval v marci 2016 a počet respondentov bol 110. Dotazník pozostával z 19 otázok. Prvé dve otázky sa týkali základných údajov o respondentovi ako je pohlavie a vek. Ďalšiu sériu otázok tvorili informácie o využívanej banke a o využívaní elektronického bankovníctva, bezpečnosť služieb elektronického bankovníctva, služieb spojených s platobnými kartami a spokojnosť užívateľov.

4.1.1 Charakteristika respondentov

Prvé dve otázky dotazníkového prieskumu sa týkajú pohlavia a veku respondentov.

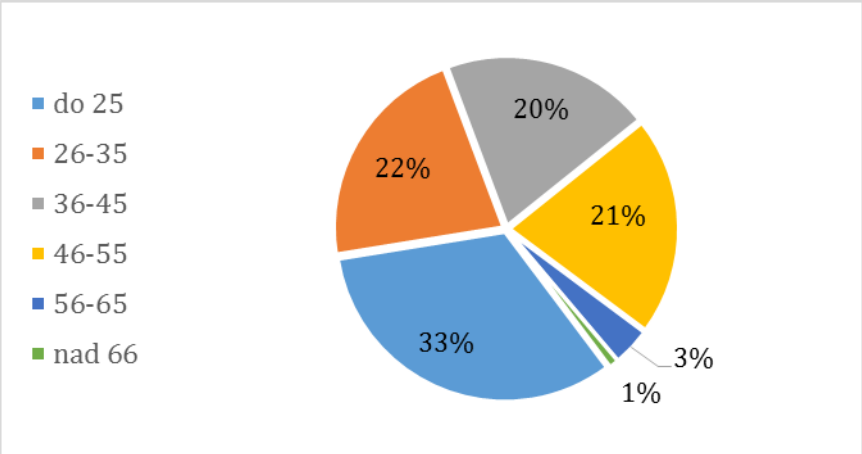
Pohlavie



Obr. 6 Pohlavie respondentov

Skupinu opýtaných respondentov tvorí 63 žien, čo predstavuje 57% a 48 mužov, t. j. 43% zo všetkých opýtaných.

Vek



Obr. 7 Vek respondentov

Prieskumu sa zúčastnilo viacero vekových kategórií. Najviac respondentov bolo vo veku do 25 rokov, čo je 33%. Druhú najpočetnejšiu skupinu, t. j. 22%, tvorili respondenti vo veku 26 až 35 rokov. Respondenti vo veku 36 – 45 rokov predstavujú 20%. Ďalšiu vekovú kategóriu 45 – 55 rokov tvorilo 21%. Najmenšie skupiny sú vekové kategórie 55 – 65 rokov t.j. 3% a veková kategória nad 66 rokov tvorí 1%.

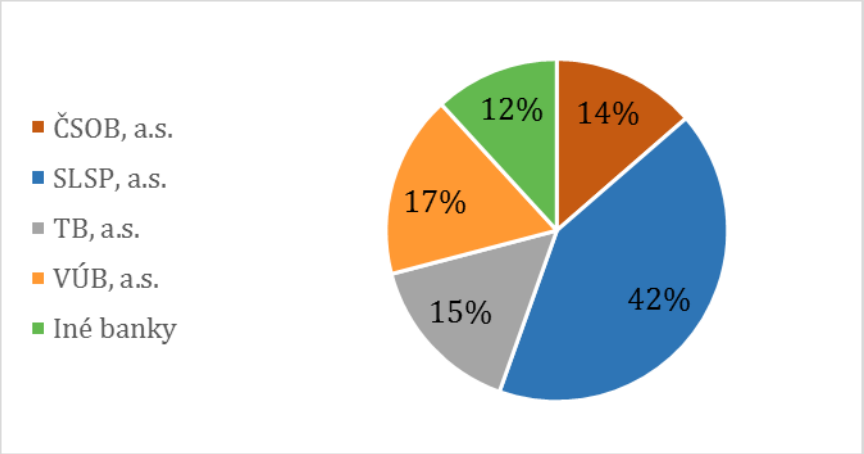
4.1.2 Analýza využívania služieb elektronického bankovníctva

Nasledujúca skupina otázok je formulovaná za účelom zistiť respondentove preferencie vo využívaní elektronického bankovníctva. Obsahom otázok sú preferencie ohľadom banky, dôvody využívania/nevyužívania elektronického bankovníctva, spokojnosť s elektronickým bankovníctvom, spôsob zabezpečenia elektronického bankovníctva. Otázky boli formulované jednoducho, formou označovania vybranej odpovede.

Otázka: Ktorú z nasledujúcich bánk využívate?
Nasledujúci graf zobrazuje využívané banky na Slovensku. Banky boli vybrané na základe štatistiky o počte rozmiestnených pobočiek na Slovensku. Štatistika je dostupná na webovej stránke Národnej banky Slovenska. Odpovede respondentov korešpondujú so štatistikou o rozmiestnených pobočkách. Podľa štatistiky najviac organizačných jednotiek, t. j. 298 pobočiek, na Slovensku má Slovenská sporiteľňa. Počet respondentov využívajúcich Slovenskú sporiteľňu je 42 % (46 respondentov). Druhú najvyužívanejšiu banku, Všeobecnú úverovú banku, využíva 17% z opýtaných. Všeobecná úverová banka má na Slovensku 234 pobočiek. 15% (t. j. 17 respondentov) využíva Tatra Banku. Počet pobočiek Tatra banky je 191. 14% opýtaných využíva Československú obchodnú banku. Československá obchodná banka má 135 organizačných pobočiek na Slovensku. 12% respondentov využíva inú ako z vyššie uvedených bánk. Medzi ostatné banky, ktoré boli vybrané respon-

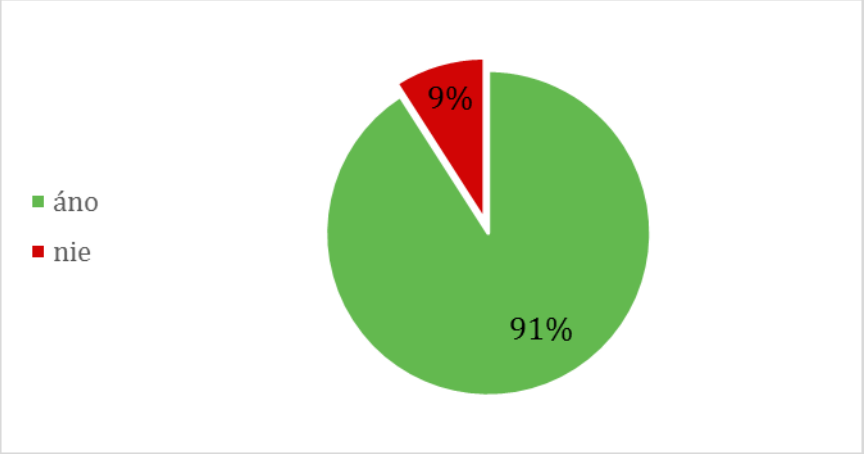
dentmi, patrí Poštová banka, Zuno, MBank, Unicredit bank, Prima Banka a Otp banka. Počty pobočiek ostatných bánk sú malé čísla (NBS, 2016).

Môžeme predpokladať, že počet organizačných jednotiek bánk má istú spojitosť s využívaním služieb jednotlivých bánk. Banky s väčším počtom organizačných jednotiek sú dostupnejšie pre klientov. Klient nájde pobočku vo svojom meste, prípadne aj v dedine. Služby poskytovaných bánk sú efektívnejšie.



Obr. 8 Využívané banky na Slovensku

Otázky: „Využívate niektorú z foriem elektronického bankovníctva?“ a „Ak NEVYUŽÍVATE služby elektronického bankovníctva, aké sú vaše dôvody?“



Obr. 9 Využívanie foriem elektronického bankovníctva

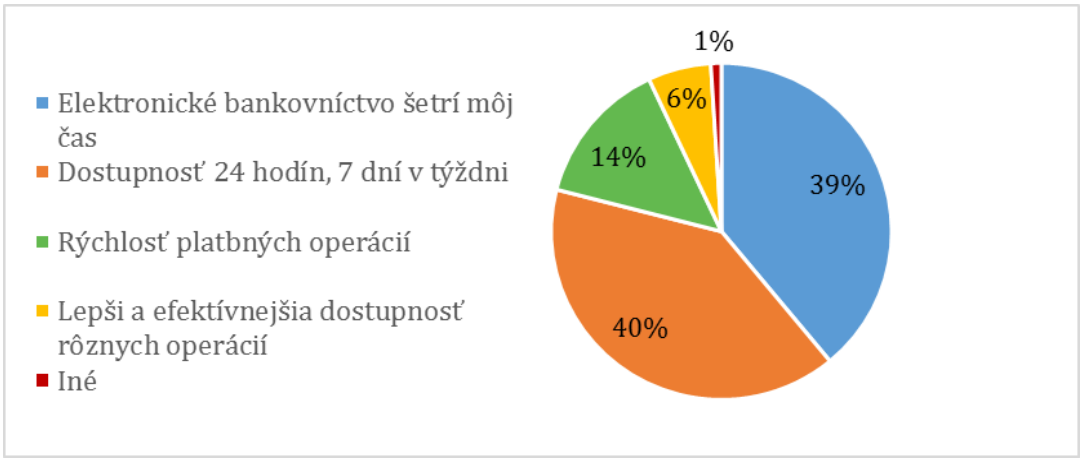
Elektronické bankovníctvo je trend. Avšak nie všetci ho využívajú. Ako ukazuje graf, 91% predstavuje 100 respondentov dotazníka, ktorí využívajú elektronické bankovníctvo. 9% respondentov elektronické bankovníctvo nevyužíva. Dôvody, ktoré respondenti uviedli, sú obava zo zneužitia osobných údajov. Dôvod uviedlo 6 respondentov. Ďalšie zvolené dôvody boli nedostatok informácií o elektronickom bankovníctve (odpoveď zvolili 2 respondenti). Klient si vystačí aj s inými službami

banky a to, že klient nevlastní účet v banke. Dané dôvody uviedli dvaja respondenti.

Otázka: „Aký je Váš hlavný dôvod využívania služieb elektronického bankovníctva?“

Ďalším bodom dotazníku bola otázka na hlavný dôvod využívania elektronického bankovníctva. Za najviac preferovaný dôvod, ktorý si respondenti volili je dostupnosť elektronického bankovníctva. Daný dôvod označilo 40 respondentov (40%). Druhý dôvod pre využívanie elektronického bankovníctva respondenti považujú šetrenie svojho času vďaka elektronickému bankovníctvu. Tento dôvod označilo 39%. 14% respondentov považuje za hlavný dôvod rýchlosť platobných operácií, 6% lepšiu a efektívnejšiu dostupnosť rôznych operácií a 1% považuje za hlavný dôvod iný, ktorý avšak neuviedol.

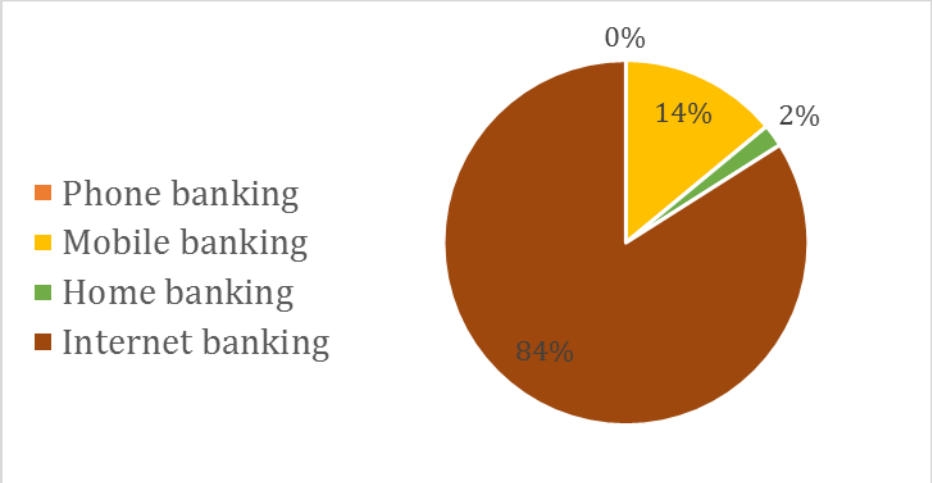
Elektronické bankovníctvo je skutočnosť, ktorú ľudia využívajú z rôznych dôvodov. Ako hlavné dôvody možno uviesť úsporu času, efektívnejšie využívanie ponúkaných služieb a dostupnosť.



Obr. 10 Hlavný dôvod využívania elektronického bankovníctva

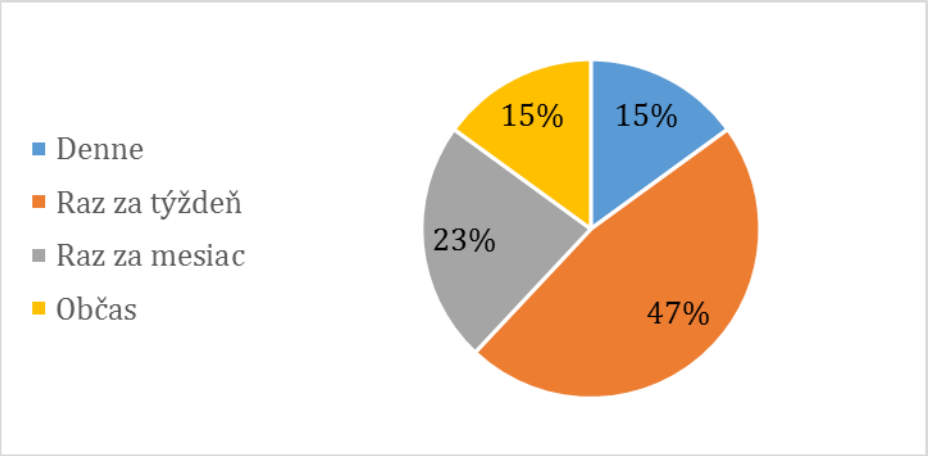
Otázka: „Ktorú z nasledujúcich foriem elektronického bankovníctva využívate najviac?“

Za najpreferovanejšiu formu elektronického bankovníctva respondenti považujú internet banking. Danú možnosť si zvolilo 84% respondentov. 14% respondentov využíva mobile banking a 2% využívajú homebanking. V rámci prieskumu môžeme predpokladať, že služby homebankingu sú postupne nahrádzané internetbankingom. Ako bolo uvedené vyššie, internetbanking ma tú výhodu, že je možné sa pripojiť odkiaľkoľvek, zatiaľ čo pri homebankingu je potrebné mať nainštalovaný softvér. Služby mobile bankingu možno označovať aj ako smartbanking. Smartbanking je prevažne nová podoba služieb elektronického bankovníctva, ktorej využívanie nie je ešte dostatočne zaužívané. Banky podnikajúce v Slovenskej republike ponúkajú aplikácie do mobilných telefónov zdarma.



Obr. 11 Formy elektronického bankovníctva

Otázka: „Ako často využívate elektronické bankovníctvo?“



Obr. 12 Pravidelnosť využívania elektronického bankovníctva

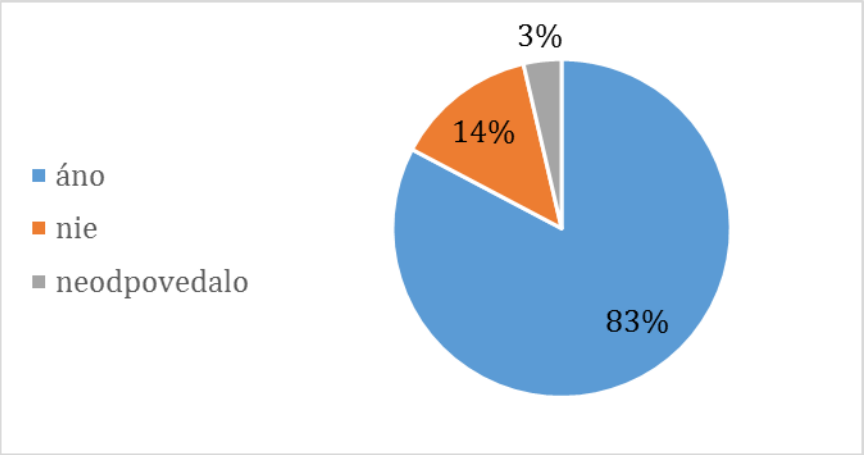
Elektronické bankovníctvo sa stáva súčasťou našich životov stále viac. 15% respondentov uviedlo, že využíva elektronické bankovníctvo každý deň. 47% respondentov využíva elektronické bankovníctvo aspoň raz za týždeň. 23% respondentov využíva elektronické bankovníctvo raz za mesiac a 15% ho využíva občas.

Otázka: „Využívate samoobslužnú zónu (bankomaty, informačné terminály atď..)?“

Samoobslužné zóny sú neoddeliteľnou súčasťou elektronického bankovníctva, prostredníctvom ktorých si môžeme vytiahnuť alebo vložiť peniaze na účet (bankomaty), zistiť informácie o zostatkoch na účtoch. 83% respondentov využíva samoobslužnú zónu, 14% respondentov samoobslužnú zónu nevyužíva, 3% respondentov na otázku neodpovedalo.

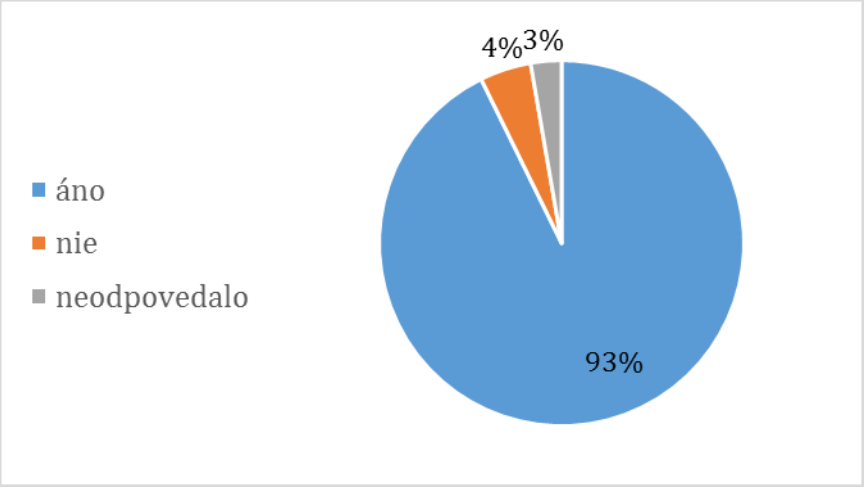
Môžeme predpokladať, že respondenti, ktorí nevyužívajú samoobslužné zóny, uprednostňujú napríklad platbu kartou. Ďalším príkladom môže byť, že klienti zís-

kavajú informácie o svojich účtoch a ponukách bánk inými spôsobmi, napríklad prostredníctvom internetbankingu.



Obr. 13 Využívanie samoobslužnej zóny

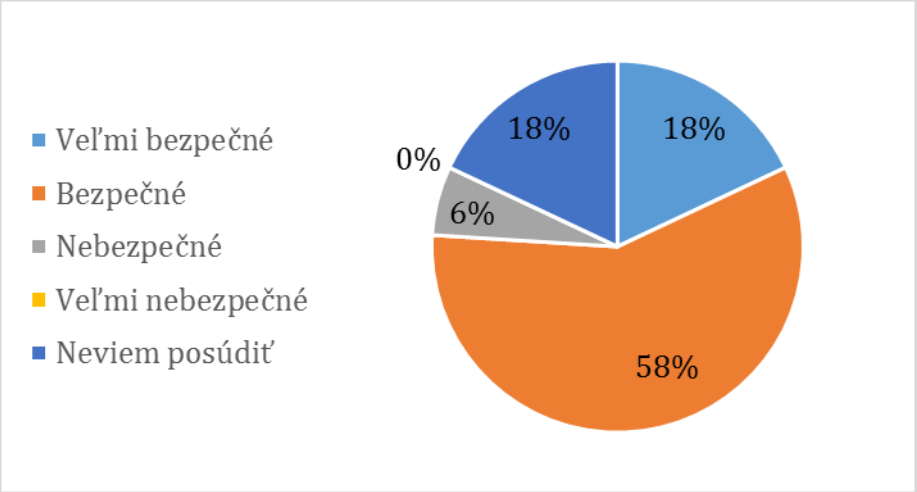
Otázka: „Využívate platobnú kartu aj ako platobný prostriedok (v obchode, na internete)?“



Obr. 14 Platobná karta ako platobný prostriedok

Rozmach platenia platobnými kartami neustále rastie, čo reprezentuje aj predchádzajúci graf. Až 93% respondentov uviedlo, že využíva platobnú kartu ako platobný prostriedok. Platbu kartou môžeme realizovať v kamennom obchode alebo aj v internetovom obchode. V súčasnosti, sú platobné terminály pre platbu kartou nevyhnutnou súčasťou každého kamenného obchodu. 4% respondentov nevyužíva platobnú kartu na platenie, 3% neodpovedali na otázku.

Otázka: „Aké je podľa Vášho názoru elektronické bankovníctvo z hľadiska bezpečnosti ?“



Obr. 15 Bezpečnosť elektronického bankovníctva

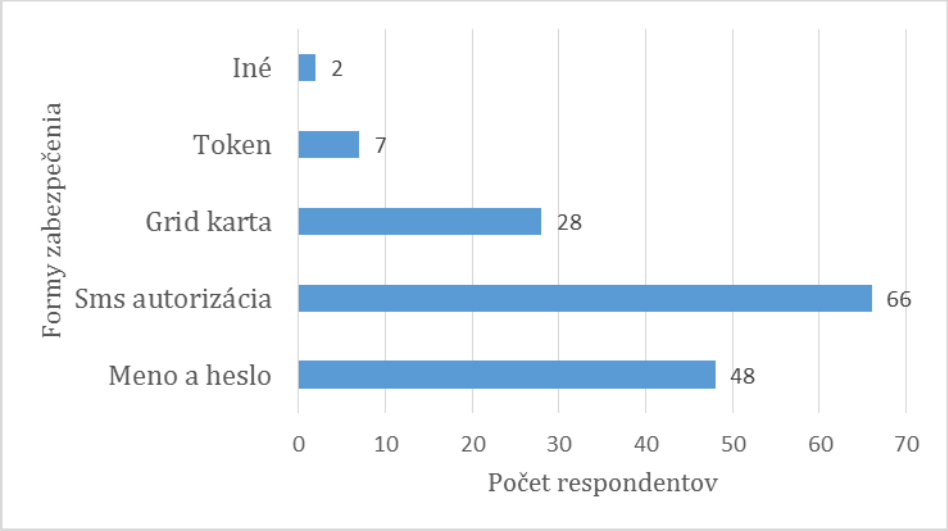
Otázka sa týka bezpečnosti elektronického bankovníctva a ako ho vnímajú respondenti. 18% respondentov označilo elektronické bankovníctvo za veľmi bezpečné. 58% respondentov považuje využívanie elektronického bankovníctva za bezpečné. Elektronické bankovníctvo ako nebezpečné označilo 6% respondentov. 18% respondentov nevie posúdiť bezpečnosť využívaného elektronického bankovníctva. Dôvodom môže byť napríklad neznalosť zabezpečovacích systémov, čo môže viesť aj k nedôvere zákazníkov voči jednotlivým bankovým subjektom.

Bezpečnosť je nevyhnutný prvok elektronického bankovníctva a znalosť základných vlastností bezpečnosti, resp. fungovania, by mal poznať každý klient.

Otázka: „Ktorú z uvedených foriem zabezpečenia využívate?“

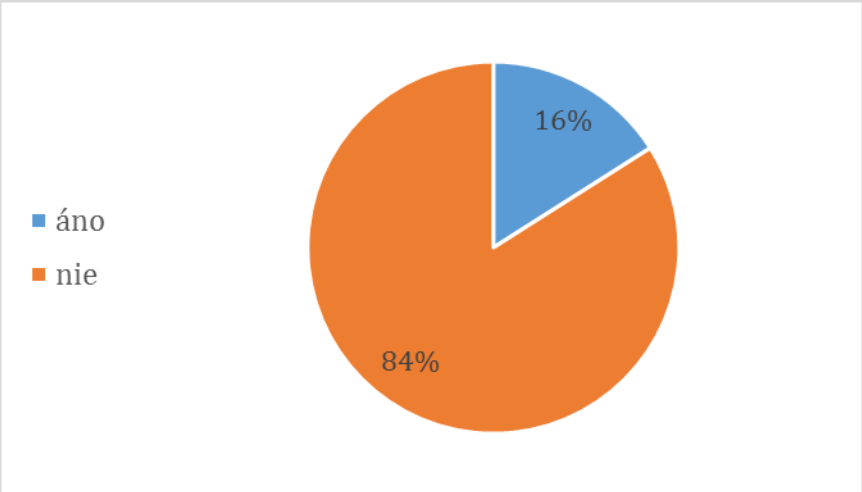
Banky poskytujúce svoje služby, ponúkajú rôzne formy zabezpečenia. Otázka sa týka zabezpečovacích prvkov, ktoré respondenti využívajú. Najviac využívanou formou zabezpečenia je *SMS autorizačný kód*, ktorý využíva 66 respondentov. 48 respondentov využíva ako formu zabezpečenia *Meno a heslo*. 28 respondentov využíva *Grid kartu*, 7 respondentov využíva *Token* a jeden respondent uviedol, že ako formu zabezpečenia využíva *Čítačku karty*.

Vo veľa prípadov v dotazníkovom prieskume si respondenti vyberali kombinácie dvoch, resp. troch foriem zabezpečenia. Najčastejšiu dvojicu tvorili *Meno a heslo a SMS zabezpečovací kód*. Danú kombináciu si zvolilo 22 respondentov. Trojicu využívaných foriem tvorili zabezpečovacie prvky: *Meno a heslo, SMS autorizačný kód a Grid karta*. Kombináciu troch foriem využíva 9 respondentov. Môžeme predpokladať, že kombinácie rôznych foriem zabezpečenia považujú respondenti za bezpečnejšie a ťažšie môže prísť k zneužitiu údajov alebo okradnutiu klienta.



Obr. 16 Formy zabezpečenia elektronického bankovníctva

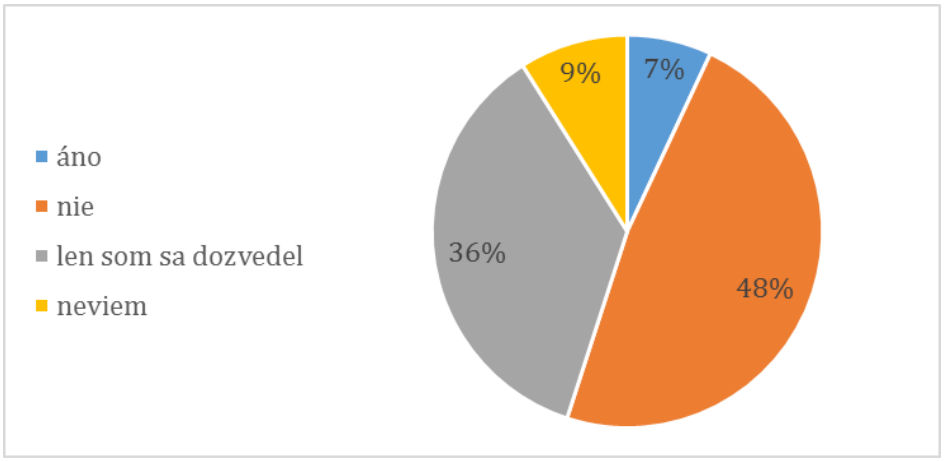
Otázka: „Vyskytujú sa vo Vami používanom elektronickom bankovníctve nejaké obťažujúce (zbytočné) úkony ?“



Obr. 17 Výskyt obťažujúcich, zbytočných úkonov

Otázka sa týka výskytu obťažujúcich alebo zbytočných úkonov v elektronickom bankovníctve. 84% respondentov uvádza, že v používanom elektronickom bankovníctve sa nenachádzajú žiadne obťažujúce úkony. 16% respondentov pokladá niektoré úkony za zbytočné. Predpokladáme, že môže ísť napríklad o vysoké poplatky spojené s niektorými službami elektronického bankovníctva, alebo neprehľadnosť internet bankingu.

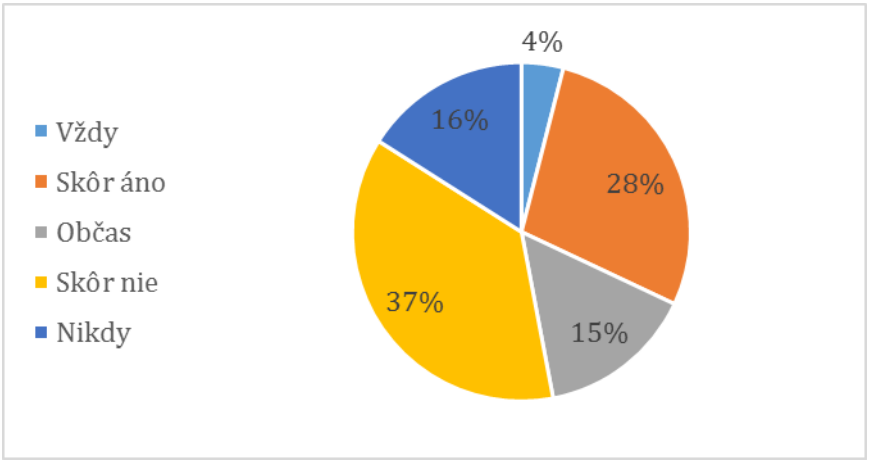
Otázka: „Stretli ste sa s nejakou podvodnou operáciou spojenou s elektronickým bankovníctvom ?“



Obr. 18 Stretnutie sa s podvodnými operáciami v elektronickom bankovníctve

Podvodné operácie spojené s elektronickým bankovníctvom sú popísané vyššie v texte. Na danú otázku odpovedalo 48% respondentov, ktorí sa s podvodnou operáciou nestretli. 7% opýtaných sa stretlo s podvodnou operáciou, 36% respondentov uviedlo, že sa o podvodných operáciách dozvedeli a 9% respondentov nevedelo určiť, či sa stretlo s podvodnou operáciou spojenou s elektronickým bankovníctvom. Banky zvyknú posielať e-maily, kedy je zvýšený výskyt podvodných operácií a upozorňujú klientov, aby si dávali pozor.

Otázka: „Uprednostňujete pri prevode vyššej sume osobnú návštevu pobočky ?“



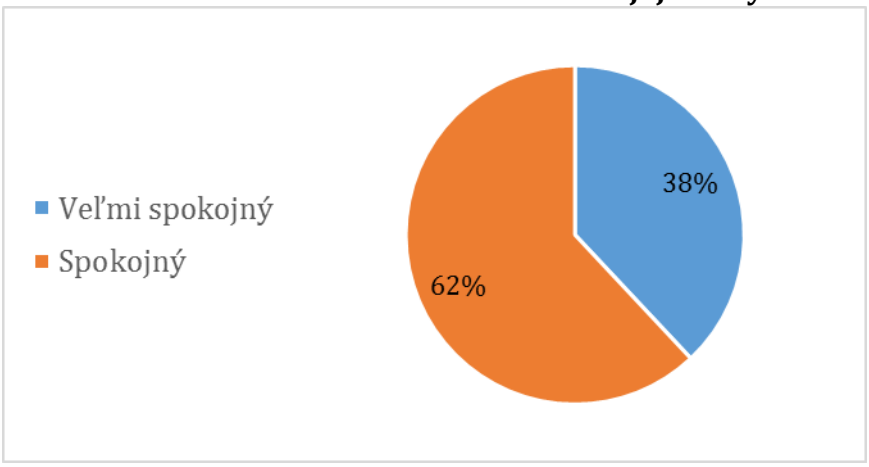
Obr. 19 Preferovanie prevodu vyššej sumy cez pobočku banky

Ako je vnímaná bezpečnosť elektronického bankovníctva nám odkazuje aj ďalšia otázka, v ktorej sme sa respondentov pýtali, či uprednostňujú platbu vyššej položky prostredníctvom internetu alebo radšej osobnú návštevu pobočky. Osobnú náv-

števu pobočky pri prevode vyššej sumy vždy uprednostňuje 4% respondentov. 28% skôr uprednostňuje prevod vyššej sumy návštevou pobočky a občas to uprednostňuje 15% respondentov. 37% respondentov označilo, že nemajú problém s prevodom vyššej sumy prostredníctvom internet bankingu a 16% respondentov uhrádza vždy aj vyššie sumy prostredníctvom internet bankingu.

Môžeme predpokladať, že väčšia časť respondentov, pokladá internetové bankovníctvo za bezpečné a dôveruje elektronickým službám bánk.

Otázka: „So službami elektronické bankovníctva mojej banky som:“



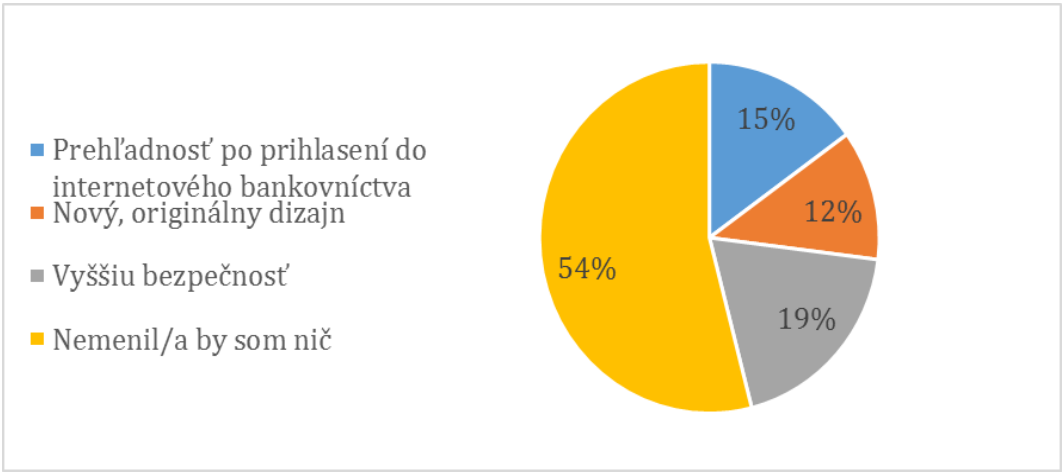
Obr. 20 Spokojnosť respondentov so službami elektronického bankovníctva

38% respondentov uviedlo, že sú veľmi spokojní so službami elektronického bankovníctva a 62% spokojní. Nespokojnosť s elektronickým bankovníctvom neuviedol ani jeden respondent.

Otázka: „Ktoré z nasledujúcich možností by ste zvolili ako zmenu pre služby elektronického bankovníctva Vašej banky ?“

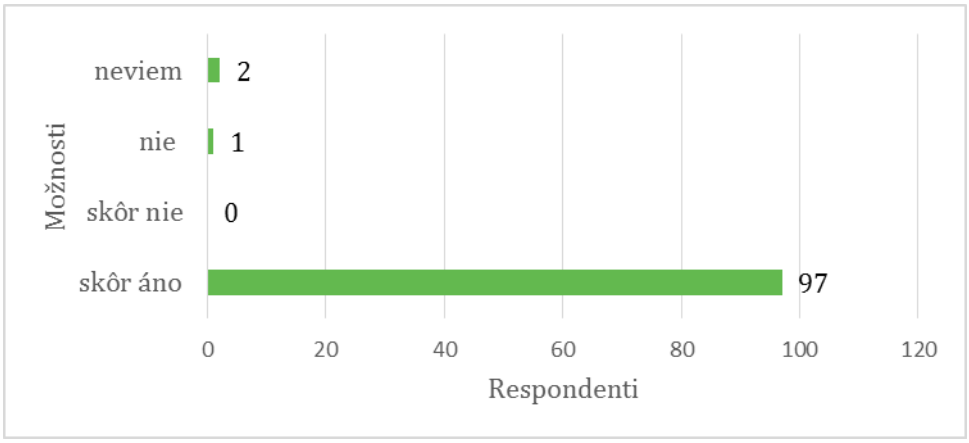
Cieľom otázky bolo zistiť, ktoré z uvedených dôvodov by si zvolili ako zmenu pre svoje elektronické bankovníctvo alebo by nemenili nič. 54% respondentov by na elektronickom bankovníctve nemenilo nič. 19% respondentov by zvýšilo bezpečnosť elektronického bankovníctva. 15% respondentov označilo za zmenu vyššiu prehľadnosť po prihlásení do internetového bankovníctva a 12% respondentov zvolilo možnosť nového, originálneho dizajnu.

Otázka potvrdzuje, že elektronické bankovníctvo, je neustále inovované a klienti na ňom nenachádzajú žiadne problémy a zmeny. Zvyšok respondentov by zvýšilo bezpečnosť, môže sa stať, že banka ponúka aj iné formy zabezpečenia avšak klient nie je nimi oboznámený.



Obr. 21 Zmeny v elektronickom bankovníctve

Otázka: „Plánujete využívať elektronické bankovníctvo aj v budúcnosti?“
Z grafu nasledujúceho môžeme vyčítať, že 97 respondentov dotazníkového prieskumu plánuje využívať elektronické bankovníctvo aj v budúcnosti. 1 respondent uviedol, že neplánuje využívať elektronické bankovníctvo v budúcnosti. 2 respondenti nevedia, či plánujú využívať elektronické bankovníctvo v budúcnosti.



Obr. 22 Využívanie elektronického bankovníctva v budúcnosti

5 Diskusia a záver

Nasledujúca kapitola bakalárskej práce obsahuje diskusiu a záver. V rámci diskusie sú vyhodnotené získané poznatky z dotazníkového prieskumu. Zároveň diskusia obsahuje návrh užívateľského rozhrania elektronického bankovníctva.

V závere sú zosumarizované ciele bakalárskej práce a vytýčili sme najvyužívanejšie formy elektronického bankovníctva.

5.1 Diskusia

Na základe dotazníkového prieskumu hodnotíme nasledujúce skutočnosti. Medzi najvyužívanejšie banky patrí Slovenská sporiteľňa, Všeobecná úverová banka, Československá obchodná banka a Tatra banka. Elektronické bankovníctvo využíva 91% respondentov uskutočneného prieskumu, čo považujeme za vysoké percento. Dôvody, pre ktoré respondenti nevyužívajú elektronické bankovníctvo sú nedostatok informácií, obava zo zneužitia údajov a zabezpečovacích kódov alebo si respondenti vystačia s ostatnými službami banky.

Respondenti za najväčší prínos elektronického bankovníctva považujú – elektronické bankovníctvo šetrí čas, dostupnosť 24 hodín, 7 dní v týždni, rýchlosť platobných operácií, lepšia a efektívnejšia dostupnosť ponúkaných služieb.

Medzi najvyužívanejšie formy elektronického bankovníctva patrí internetbanking a mobile banking. Iné formy elektronického bankovníctva ako napríklad homebanking a phonebanking, môžeme považovať za ustupujúce pred modernými a efektívnejšími službami. Taktiež sme sledovali pravidelnosť využívania služieb elektronického bankovníctva. Priemerné využívanie služieb elektronického bankovníctva raz za týždeň uviedlo 47% respondentov.

Z pohľadu bezpečnosti a spokojnosti so službami elektronického bankovníctva sú respondenti viac ako spokojní. Až 76% respondentov považuje elektronické bankovníctvo za bezpečné. Spokojnosť so službami elektronického bankovníctva označuje 100% respondentov. Na základe výsledkov prieskumu tvrdíme, že ponuka služieb elektronického bankovníctva je pre klientov uspokojivá.

Na druhej strane nie všetci respondenti považujú služby elektronického bankovníctva za bezpečné, respektíve nevedia posúdiť bezpečnosť elektronického bankovníctva. Danú skutočnosť považujeme za negatívum pri poskytovaní služieb elektronického bankovníctva. Banky by mohli venovať priestor aj pre vysvetlenie základného fungovania zabezpečovacích systémov a tak zvyšovať svoju popularitu a konkurenčnú výhodu.

Na základe zistených skutočností sme schopní zostaviť návrh optimálneho užívateľského rozhrania, vhodného pre bežného užívateľa elektronického bankovníctva. Rozhranie by malo spĺňať požiadavky jednoduchej dostupnosti služieb, ktoré sú prostredníctvom elektronického bankovníctva poskytované. Ako príklad uvádzame, že klient vie ľahko nájsť základné nástroje na vykonanie jednoduchých úkonov – informácie o účtoch, vykonanie platby, vytvorenie inkasa alebo trvalého

príkazu. Grafika užívateľského rozhrania by mala byť nenáročná a prívetivá pre potreby klienta.

Pri návrhu užívateľského rozhrania je vhodné vykonávať analýzy, prostredníctvom ktorých sa rozhranie testuje samotnými užívateľmi. To môže tvorcom pomôcť pri zdokonaľovaní rozhrania a neskôr poskytovať efektívnejšie služby. Neoddeliteľnou súčasťou užívateľského rozhrania je jeho optimálna bezpečnosť, napríklad využívanie biometrických prvkov alebo rôznych elektronických kľúčov, ktoré by boli cenovo dostupnejšie.

Do úvahy pri tvorbe užívateľského rozhrania a neskôr jeho využívania navrhujeme zohľadniť aby bol priestor pre spätnú väzbu. V rámci spätnej väzby vie klient upozorniť na chyby, prípadne odporučiť zlepšenie systému. Je vhodné, aby užívateľské rozhranie obsahovalo aj informácie o poskytovaných službách, ktoré sú v rámci rozhrania dostupné. Tým sa klient vie lepšie orientovať v užívateľskom rozhraní a využívanie služieb bude považovať za efektívnejšie.

5.2 Záver

Využívanie elektronického bankovníctva je na vzostupe. Banky, podnikajúce na území Slovenskej republiky, vedia, že poskytovanie služieb elektronického bankovníctva je významným prvkom v konkurenčnom boji. Banky musia neustále zveľaďovať poskytované služby aby bol tento boj efektívnejší. Klienti využívajú služby elektronického bankovníctva stále viac, pretože služby sú dostupnejšie a šetria čas, čím vzrastá aj efektivita ponúkaných služieb.

Práca obsahuje charakteristiku bankového systému, elektronického bankovníctva a formy, ktoré sa využívajú v Slovenskej republike. Medzi najvyužívanejšie formy patrí internetbanking, ktorý je poskytovaný všetkými vyššie spomenutými bankami. Ďalšou využívanou službou je mobile banking. Do mobile bankingu zaraďujeme smartbanking - mobilnú aplikáciu, prostredníctvom ktorej môže klient získavať aktuálne informácie ale taktiež aj vykonávať platby a prevody peňazí.

Platobné karty majú neoddeliteľné miesto medzi využívanými formami elektronického bankovníctva. Platobné karty už dávno neslúžia len na výber hotovosti z bankomatu ale aj na samotné platenie v kamenných obchodoch a na internete. S tým je spojený rozmach platenia na internete, kde banky poskytujú platenie prostredníctvom platobných kariet alebo vopred vyplnenými príkazmi na úhradu.

S rastúcim využívaním elektronického bankovníctva vzrastá aj požiadavka bezpečnosti. Banky sa snažia predchádzať útokom varovaním klientov, ale napriek tomu útoky vyvolávajú v klientoch nedôveru voči bankám. Preto je vhodné aby banka vedela informovať klientov o bezpečnosti účtov.

Praktická časť bakalárskej práce sa zaoberá vyhodnotením dotazníkového prieskumu, ktorý bol zameraný na využívanie foriem elektronického bankovníctva.

V praktickej časti bakalárskej práce sme vykonali analýzu využívaných foriem elektronického bankovníctva, ktorej zosumarizovanie a odporúčania sú uvedené v diskusii bakalárskej práce.

6 Literatúra

BAAR, ONDŘEJ. Šifrování, Symetrické šifrování. *Bloger.cz* [online]. 2007 [cit. 2016-05-05]. Dostupné z: http://owebu.bloger.cz/Bezpecnost/Sifrovani-Symetricke-sifrovani

BEZPECNYINTERNET.CZ. Phishing and pharming. *bezpečnýinternet.cz* [online]. [cit. 2016-03-02]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

ČSOB. Individuálni klienti. *ČSOB* [online]. 2015 [cit. 2016-05-04]. Dostupné z: https://www.csob.sk/individualni-klienti

DOSEDĚL, TOMÁŠ. *Počítačová bezpečnost a ochrana dat.* Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

EUROEKONÓM.SK. Bankovníctvo a banky: Bankový systém. EuroEkonóm.sk [online]. 2015 [cit. 2016-04-18]. Dostupné z: http://www.euroekonom.sk/financie/bankovnictvo-a-banky/

EUROSTAT. Individuals using the internet for internet banking. *Eurostat* [online]. 2015 [cit. 2016-04-18]. Dostupné z: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00099

FAULKNER, Cameron. What is NFC? Everything you need to know. *TechRadar* [online]. 2015 [cit. 2016-04-18]. Dostupné z: http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410

GOPAY. Platenie s nami bude poriadna jazda. *Platebnabrana.sk* [online]. GOPAY s.r.o, 2016 [cit. 2016-03-10]. Dostupné z: https://www.platobnabrana.sk/

HA, Kyung-Hun, CANEDOLI, Andrea, W. BAUR, Aaron a BICK, Markus. Mobile banking — insights on its increasing relevance and most common drivers of adoption. *Electronic Markets* [online]. 2012. [cit. 2016-04-17]. DOI: 10.1007/s12525-012-0107-1. ISSN 1019-6781. Dostupné z: http://link.springer.com/10.1007/s12525-012-0107-1

HOAX.CZ. *Co je to phishing ?* [online]. 2000-2016 [cit. 2016-03-02]. Dostupné z: http://www.hoax.cz/phishing/

CHABADA, Michal. ČSOB predstavila vlastnú Android aplikáciu. *MôjAndroid.sk* [online]. 2011 [cit. 2016-04-18]. Dostupné z: https://www.mojandroid.sk/csob-predstavila-vlastnu-android-aplikaciu/

KLUFA, František. *Elektronické platební prostředky: jak se vyhnout rizikům*. 1. vyd. Praha: Sdružení českých spotřebitelů, 2013. Průvodce spotřebitele. ISBN 978-80-87719-07-7.

KUMAR, Sangeeth S. a THABREZ, Shams. *Payment Gateway Interface* [online]. San Jose: Cisco Technology, Inc., 2015 [cit. 2016-03-10]. Dostupné z: http://www.freepatentsonline.com/y2015/0347989.html

LAHA ROY, Tasmayee. What you must know about an E-wallet? *The Economic Times* [online]. 2013 [cit. 2016-04-18]. Dostupné z: http://articles.economictimes.indiatimes.com/2013-06-14/news/39976342_1_e-wallet-facility-airtel-money-flipkart

LUDVÍK, Miroslav. *Autentizační prvky a metody pod drobnohledem* [online]. 2004 [cit. 2016-03-02]. Dostupné z: http://www.penize.cz/investice/16777-autentizacni-prvky-a-metody-pod-drobnohledem

MATYÁŠ, Vašek a KRHOVJÁK, Jan. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. 1. vyd. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

MÁČE, Miroslav. *Platební styk: klasický a elektronický*. 1. vyd. Praha: Grada, 2006. Osobní a rodinné finance. ISBN 80-247-1725-5.

MFSR. Ako rozumieť peniazom. *FINinfo.sk* [online]. 2013 [cit. 2016-03-10]. Dostupné z: http://www.fininfo.sk/sk/titulka

MOLNÁŘ, Zdeněk. Pokročilé metody vědecké práce. 1. vyd. Zeleneč: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.

NÁDERNÍČEK, PETR. Pravdy o elektronickém podpisu a šifrování (1) - základní pojmy. *SvětSítí* [online]. 2003 [cit. 2016-04-18]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Pravdy-o-elektronickem-podpisu-a-sifrovani-1-zakladni-pojmy-1252003

NBS. Úvodná stránka. *Národná banka Slovenska* [online]. 2016 [cit. 2016-05-04]. Dostupné z: http://www.nbs.sk/sk/titulna-stranka

POLOUČEK, Stanislav. *Bankovnictví*. 2. vyd. V Praze: C.H. Beck, 2013. Beckovy ekonomické učebnice. ISBN 978-80-7400-491-9.

POŠTOVÁ BANKA. Služba CashBack. *Poštová banka, a. s.* [online]. 2016 [cit. 2016-05-07]. Dostupné z: https://www.postovabanka.sk/ucty/platby-a-sluzby/cashback/

PŘÁDKA, Michal. *Elektronické bankovnictví: rady a tipy*. Vyd. 1. Praha: Computer Press, 2000. Praxe manažera (Computer Press). ISBN 80-7226-328-5.

REVENDA, Zbyněk. *Peněžní ekonomie a bankovnictví*. 5., aktualiz. vyd. Praha: Management Press, 2012. ISBN 978-80-7261-240-6.

SECUREPAY. 3D Secure [online]. 2016 [cit. 2016-03-10]. Dostupné z: https://www.securepay.com.au/developers/products-and-services/3d-secure/

SCHLOSSBERGER, Otakar a HOZÁK, Ladislav. *Elektronické platební prostředky*. 1. vyd. Praha: Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.

SKRILL, Control all your online payments through one easy-to-use account. *Skrill* [online]. 2015 [cit. 2016-04-17]. Dostupné z: https://www.skrill.com/en/

SLSP, a. s. *Slovenská sporiteľňa, a. s.* [online]. Bratislava, 2016 [cit. 2016-05-04]. Dostupné z: https://www.slsp.sk/sk/ludia

STORMWARE. Homebanking - internetové bankovníctvo. *Stormware* [online]. 2014 [cit. 2016-04-18]. Dostupné z: https://www.stormware.sk/pohoda/homebanking.aspx

TRISUL. Autentizace a autorizace. *Trisul, s.r.o* [online]. 2005-2016 [cit. 2016-04-18]. Dostupné z: http://www.trisul.cz/bezpecnost-autentizace-autorizace/

TB, a. s. *Inovácie Tatra banky* [online]. Bratislava, 2016 [cit. 2016-05-04]. Dostupné z: https://www.inovacietb.sk/

TUČKOVÁ, Táňa. PORADNA: Jak platit na internetu? Nejlépe kartou. *Novinky.cz* [online]. 2015 [cit. 2016-03-10]. Dostupné z: http://www.novinky.cz/finance/financni-radce/372467-poradna-jak-platit-na-internetu-nejlepe-kartou.html

UNICREDIT BANK. Mobilná aplikácia Smartbanking. Unicredit bank [online]. 2013 [cit. 2016-05-07]. Dostupné z: http://www.unicreditbank.sk/sk/Obcania/Ucty-a-baliky/Elektronicke-bankovnictvo/Mobilna-aplikacia-Smart-Banking

VERECKÝ, Štepán. Biometria a elektronické podpisy. *Unicorns systems* [online]. 2012 [cit. 2016-04-17]. Dostupné z: http://www.unicornsystems.eu/sk/novinky-sk/clanok/biometria-a-elektronicke-podpisy.html

VIAMO, a. s.: Poslať peniaze nebolo nikdy ľahšie. *VIAMO, a. s.* [online]. 2016 [cit. 2016-05-04]. Dostupné z: http://viamo.sk/sk/osoba/

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vyd. Ilustrace Bára Buchalová. Praha: Albatros, 2006. Oko (Albatros). ISBN 80-00-01888-8.

VÚB Banka. *VÚB Banka: Osobné financie* [online]. 2016 [cit. 2016-05-05]. Dostupné z: https://www.vub.sk/sk/osobne-financie/

Zákon č. 483/2001 Zb. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podľa stavu k 1. 1. 2016

Prílohy

A Dotazník

Vážený respondent/vážená respondentka.

Predkladám Vám dotazník, ktorý sa týka prieskumu pre bakalársku prácu s názvom Formy elektronického bankovníctva a jeho využitie v Slovenskej republike. Vyplnenie dotazníka je anonymné.

Pohlavie:

a) muž
b) žena

Vek:

a) do 25 rokov
b) 26 – 35 rokov
c) 36 – 45 rokov
d) 46 – 55 rokov
e) 56 – 65 rokov
f) 66 a viac

Ktorú z nasledujúcich bánk využívate ?

a) Československá obchodná banka, a.s. (ČSOB)
b) Slovenská sporiteľňa, a.s. (SLSP)
c) Tatra Banka, a.s.
d) Všeobecná úverová banka, a.s. (VÚB)
e) iná, uveďte

Využívate niektorú z foriem elektronického bankovníctva?

a) áno
b) nie

Ak nevyužívate služby elektronického bankovníctva, aké sú vaše dôvody?

a) vystačím si s ostatnými službami banky
b) nemám dostatok informácií o elektronickom bankovníctve
c) nemám vlastný účet
d) obava z neužitia osobných údajov a zabezpečovacích kódov
e) iný dôvod

Aký je Váš hlavný dôvod využívania služieb elektronického bankovníctva?

a) elektronické bankovníctvo šetrí môj čas
b) dostupnosť 24 hodín 7 dní v týždni
c) rýchlosť platobných operácií
d) lepšia a efektívnejšia dostupnosť rôznych informácií
e) iné dôvody

Ktorú z nasledujúcich foriem elektronického bankovníctva využívate najviac?

a) phone banking (call centrum)
b) mobile banking (SMS banking, GSM SIM Toolkit banking, SMARTbanking)
c) home banking
d) mail banking
e) internet banking

Ako často využívate elektronické bankovníctvo?

a) Denne
b) raz za týždeň
c) raz za mesiac
d) Občas

Využívate samoobslužnú zónu (bankomaty, informačné terminály atď..)?

a) áno
b) nie

Využívate platobnú kartu aj ako platobný prostriedok (v obchode, na internete) ?

a) áno
b) nie

Aké je podľa Vášho názoru elektronické bankovníctvo z hľadiska bezpečnosti ?

a) veľmi bezpečné
b) bezpečné
c) nebezpečné
d) veľmi nebezpečné

Ktorú z uvedených foriem zabezpečenia využívate?

a) Meno a Heslo
c) SMS autorizačný kód
b) GRID karta
d) Token (EOK)
e) iné

Vyskytujú sa vo Vami používanom elektronickom bankovníctve nejaké obťažujúce (zbytočné) úkony ?

a) áno
b) nie

Stretli ste sa s nejakou podvodnou operáciou spojenou s elektronickým bankovníctvom ?

a) áno
b) nie
c) len som dozvedel/a
d) neviem

Uprednostňujete pri prevode vyššej sume osobnú návštevu pobočky ?

a) vždy
b) skôr áno
c) občas
d) skôr nie
e) nikdy

So službami elektronické bankovníctva mojej banky som :

a) veľmi spokojný
b) spokojný
c) nespokojný
d) veľmi nespokojný

Ktoré z nasledujúcich možností by ste zvolili ako zmenu pre služby elektronického bankovníctva Vašej banky ?

a) prehľadnosť po prihlásení do internetového bankovníctva
b) nový, originálnejší image
c) vyššiu bezpečnosť
d) nemenil by som nič

Plánujete využívať elektronické bankovníctvo aj v budúcnosti?

a) skôr áno
b) skôr nie
c) nie
d) neviem
e) nikdy