# Analýza produktů elektronického bankovnictví ve vybraných bankách České republiky

Pavel Gruna

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav financí a účetnictví
akademický rok: 2011/2012

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Pavel GRUNA** |
| Osobní číslo: | **M08057** |
| Studijní program: | **B 6208 Ekonomika a management** |
| Studijní obor: | **Management a ekonomika** |
| Téma práce: | **Analýza produktů elektronického bankovnictví ve vybraných bankách České republiky** |

Zásady pro vypracování:

**Úvod**

**I. Teoretická část**

- **Zpracujte literární řešerši na téma elektronické bankovnictví.**

**II. Praktická část**

- **Proveďte marketingový výzkum spokojenosti klientů mezi retailovými uživateli elektronického bankovnictví.**
- **Navrhněte doporučení pro výběr produktů elektronického bankovnictví pro vybrané typy retailového klienta.**

**Závěr**

Rozsah bakalářské práce: **cca 40 stran**

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

**DVOŘÁK, Petr. Bankovnictví pro bankéře a klienty. 3. přepracované a rozšířené vydání. Praha: Linde Praha, 2005. 681 s. ISBN 80-7201-515-X.**
**KONDABAGIL, Jayaram. Risk management in electronic banking: Concepts and best practices. 1st edition. Singapore: Wiley, 2007. 288 s. ISBN 978-0-470-82243-2.**
**MÁČE, Miroslav. Platební styk: klasický a elektronický. První vydání. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.**
**MATYÁŠ, Václav a KRHOVJÁK, Jan. Autorizace elektronických transakcí a autentizace dat i uživatelů. Vyd. 1. Brno: Masarykova univerzita, 2008. 128 s. 1. ISBN 978-80-210-4556-9.**
**POLOUČEK, Stanislav a kol. Bankovnictví. 1. vydání. Praha: C. H. Beck, 2006. 716 s. ISBN 80-7179-462-7.**

Vedoucí bakalářské práce: **Ing. Eva Cipovová**
Ústav financí a účetnictví

Datum zadání bakalářské práce: **2. dubna 2012**

Termín odevzdání bakalářské práce: **18. května 2012**

Ve Zlíně dne 2. dubna 2012

prof. Dr. Ing. Drahomíra Pavelková
*děkanka*

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta managementu a ekonomiky

prof. Dr. Ing. Drahomíra Pavelková
*ředitel ústavu*

# PROHLÁŠENÍ AUTORA
# BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému,
- na mou bakalářskou/diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2];
- podle § 60[3] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;

---

[1] *zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:*

*(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.*

*(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.*

*(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.*

[2] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:*

*(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).*

[3] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

*(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.*

- podle § 60[4] odst. 2 a 3 mohu užít své dílo – bakalářskou/diplomovou práci - nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);

- pokud bylo k vypracování bakalářské/diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské/diplomové práce využít ke komerčním účelům.

Prohlašuji, že:

- jsem bakalářskou/diplomovou práci zpracoval/a samostatně a použité informační zdroje jsem citoval/a;

- odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 18.5.2012 .....

.....

---

[4] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

*(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.*

*(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.*

## ABSTRAKT

Předmětem této bakalářské práce je analýza vybraných produktů elektronického bankovnictví pro retailové klienty v České republice. Teoretická část popisuje problematiku platebních karet a forem vzdáleného přístupu k elektronickému bankovnictví. Praktická část je zaměřena na srovnání jednotlivých produktů elektronického bankovnictví a doporučení vhodné nabídky banky pro využívání elektronického bankovnictví. Součástí praktické práce je dotazníkové šetření zjišťující spokojenost klientů s využíváním elektronického bankovnictví.



Klíčová slova: elektronické bankovnictví, přímé bankovnictví, platební karta, telefonní bankovnictví, mobilní bankovnictví, internetové bankovnictví, autentizace, autorizace.



## ABSTRACT

The subject of this thesis is an analysis of selected products of electronic banking for retail clients in the Czech Republic. The theoretical part describes the issue of payment cards and forms of remote access to electronic banking. The practical part is focused on the comparison of products of electronic banking and recommendations to choose appropriate bank offers of electronic banking. The practical work also contains survey of client satisfaction with the use of electronic banking.



Keywords: electronic banking, direct banking, paymend card, phonebanking, mobile banking, internet banking, authentication, authorization.

Tímto bych rád poděkoval vedoucí mé bakalářské práce Ing. Evě Cipovové za odborné vedení, vstřícný přístup a za poskytnutí cenných rad v průběhu jejího zpracování.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

# ÚVOD

Za posledních deset let je patrný rozvoj elektronického bankovnictví natolik, že je považováno za dominantní trend bankovnictví. Dochází k rozsáhlejšímu využívání stávajících produktů, mění se způsob a možnosti jejich využití a vznikají také naprosto nové produkty. To má za následek nárůst počtu klientů, kteří elektronické bankovnictví využívají, zvýšený objem transakcí a postupné zdokonalování sítě zařízení, bez kterých by nebylo možné elektronické bankovnictví využívat.

Produkty elektronického bankovnictví zavádějí nejen nový způsob v komunikace mezi bankou a klientem, ale tím pádem vyvstávají nová rizika, která dopadají jak na banku, tak i na klienta. Význam těchto rizik roste s rozvojem produktů elektronického bankovnictví a týká se stále většího počtu klientů. Podceňování a nedostatečná ochrana proti rizikům totiž ústí ve velké potencionální ztráty.

Téma jsem si vybral z důvodu, že považuji elektronické bankovnictví za důležitý obor bankovnictví, se kterým se každý z nás denně setkáváme.

V první části teoretické práce se zaměřím na elektronické bankovnictví jako pojem a jeho právní úpravu z hlediska zákonů Evropské Unie i zákonů České republiky.

Druhá kapitola bude zaměřena na platební karty, jejich druhy, náležitosti a využití. Popsán bude také proces autorizace platby platební kartou, zabezpečení a možná rizika spojená s používáním platební karty.

Třetí kapitola se bude týkat forem vzdáleného přístupu k elektronickému bankovnictví. Menší část zde bude věnován telefonnímu bankovnictví a mobilnímu bankovnictví, větší část pak internetovému bankovnictví. Přiblížím metody autentizace a autorizace transakcí v internetovém bankovnictví, zmíním rizika a nastíním budoucnost internetového bankovnictví i jeho autorizace, která by se mohla v brzké době začít využívat.

Praktická část začne marketingovým výzkumem spokojenosti klientů prostřednictvím dotazníkového šetření. Na základě jeho výsledků také budu analyzovat nabídky vybraných bank.

Cílem mé práce je analyzovat nabídky produktů elektronického bankovnictví od České spořitelny, Komerční banky, ČSOB, GE Money bank, mBank a na základě analýzy doporučit retailovému klientovi nabídku banky, která bude optimální.

# I. TEORETICKÁ ČÁST

# 1 TERMÍN ELEKTRONICKÉ BANKOVNICTVÍ

„Elektronické bankovnictví lze definovat jako poskytování standardizovaných bankovních produktů a služeb klientele prostřednictvím elektronických cest“ (Polouček et al, 2006, s. 176)

## 1.1 Právní úprava vztahů mezi bankou a klientem u produktů elektronického bankovnictví

Vzhledem k velkému významu elektronického bankovnictví je daná oblast z hlediska práva ošetřena předmětem úpravy na úrovni Evropské Unie. Za základní normu se považuje Směrnice 2000/46/ES o přístupu k činnosti institucí elektronických peněz, jejím výkonu a obezřetnostním dohledu nad touto činností. (Dvořák, 2005, s. 387)

Cílem této směrnice je zamezení „praní špinavých peněz“ tj. nekontrolované emise elektronických peněz, zajistit právní jistotu klienta a zlepšit důvěru veřejnosti k elektronickým peněžním prostředkům. Dále je to Směrnice 2002/65/ES o uvádění finančních služeb pro spotřebitele na trh na dálku a Směrnice 97/7/ES o ochraně spotřebitele v případě smluv uzavřených na dálku, které obsahují postup při zneužití platební karty. Komise také vydala doporučení 97/489/ES o operacích prováděných elektronickými platebními prostředky a vztahu mezi vydavateli a držiteli platebních karet s důrazem na ochranu práv držitele. (Dvořák, 2005, s. 387)

V České republice jsou základní vztahy upraveny Zákonem o platebním styku, který zahrnuje do právního řádu ČR výše uvedené směrnice Evropské Unie a odráží do jisté míry i doporučení Evropské Unie. Zákon o platebním styku určuje práva a povinnosti subjektů, kteří se zúčastní převodu peněžních prostředků. Tyto pravidla se týkají i produktů elektronického bankovnictví.

Česká národní banka za účelem ochrany držitelů vydává vzorové obchodní podmínky, které navazují na zákon o platebním styku. Tyto vzorové podmínky na rozdíl od zákona nejsou závazné. Banky mají povinnost vydávat a zveřejňovat své obchodní podmínky, nicméně se mohou od vzorových obchodních podmínek lišit. V úvodních ustanoveních svých obchodních podmínek banky musí poskytovat informace, do jaké míry se tyto obchodní podmínky odchylují od původních vzorových podmínek.

## 1.2 Definice pojmů platebních produktů elektronického bankovnictví

Za platební produkty elektronického bankovnictví lze v podstatě označit všechny produkty banky, při kterých komunikace klienta s bankou probíhá zčásti, nebo plně elektronickou formou.

Pro praktické účely vymezení pojmů lze vycházet ze zákona o platebním styku. Zákon č. 124/2002 Sb. § 15, říká, že:

„Elektronickým platebním prostředkem je

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

b) elektronický peněžní prostředek.

Elektronickým peněžním prostředkem je platební prostředek, který uchovává peněžní hodnotu v elektronické podobě.

Elektronickými penězi je peněžní hodnota, která:

a) představuje pohledávku za vydavatelem,

b) je uchovávaná na elektronickém peněžním prostředku,

c) je vydávaná proti přijetí peněžních prostředků v hodnotě ne nižší, než je hodnota vydávaných elektronických peněz, a

d) je přijímána jako platební prostředek jinými osobami než jejich vydavatelem.“

Zatímco prostředek vzdáleného přístupu k peněžní hodnotě je možno označit za nový způsob využívání klasických platebních produktů, jako je ovládání běžného účtu skrze různé formy vzdáleného přístupu, tak elektronické peníze jsou nová forma peněz.

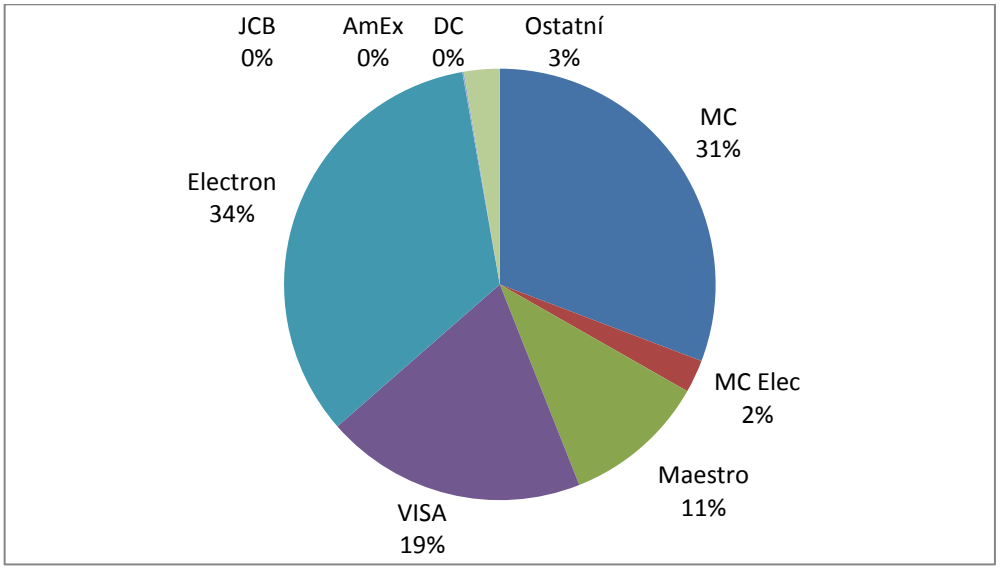
# 2 PLATEBNÍ KARTY

Platební karta je moderním prostředkem bezhotovostního platebního styku. V současné době je jeden z nejčastěji používaných platebních prostředků, v mnoha zemích nahradila používání dříve velmi oblíbených šeků. Platební kartu využívají zejména fyzické osoby, protože jejich relativně nízké denní limity je zamezují používat v platebním styku u podnikatelských subjektů. Platební karta je vyrobena z plastu a odpovídá mezinárodní normě ISO 3554 z hlediska konstrukce, velikosti a použitých materiálů při výrobě. Její rozměry jsou 85,6 x 54 x 0,76 mm. Pomocí platební karty je její majitel oprávněn vykonávat peněžní transakce (Dvořák, 2005, s. 370)

## 2.1 Náležitosti platebních karet

Emitované platební karty musí obsahovat následující náležitosti:

1) označení vydavatele karty – nejvýznamnější vydavatele platebních karet lze rozdělit do následujících 3 skupin:
   - banky a bankovní asociace (VISA, MasterCard, JCB)
   - finanční společnosti (American Express, Diners Club)
   - obchodní domy, telekomunikační, letecké společnosti atd.




*Obr. 1 Podíl nejvýznamnějších vydavatelů karet na celkovém počtu vydaných karet v ČR v roce 2011 (vlastní zpracování z dat SBK)*

2) jméno držitele platební karty a jeho identifikaci (nejčastěji se používá podpis nebo rodné číslo) – držitel karty je obvykle majitel účtu, ke kterému je karta vystavena.

Karta může být vystavena i pro další osoby, které jsou oprávněny disponovat s prostředky na účtu. Jméno držitele může být dlouhé maximálně 27 znaků. Jestliže se jedná o firemní platební kartu, tak se pod jménem držitele karty uvádí také název firmy, k jejímuž účtu je karta vystavena. Tak jako jméno držitele karty, tak i název firmy se musí vejít do 27 znaků.

3) číslo platební karty – číslo platební karty obsahuje 16 až 19 znaků a má následující strukturu. První dva znaky určují druh platební karty, dalších zpravidla pět znaků určuje vydavatele karty a zbývajících 8 až 13 znaků slouží k identifikaci držitele karty.
4) doba platnosti karty – doba platnosti bývá uvedena na kartě většinou jako měsíc a rok uvádějící konec platnosti karty, v některých případech i začátek platnosti karty. Doba platnosti karet se liší, od jednoho roku po několik let. Karty s prošlou dobou splatnosti jsou automaticky zablokovávány, po prošlé lhůtě je již nelze použít.
5) záznam dat (Máče, 2005, s. 371)

## 2.2 Druhy platebních karet

### 2.2.1 Druhy platebních karet podle techniky záznamu dat

Data na platební kartě mají formu tištěných znaků písmen a číslic a dále pak ve formě elektronického záznamu. Data v podobě alfanumerických znaků mohou být na kartě zaznamenána dvojím způsobem:

1) reliéfní písmo (embossing) – údaje o identifikaci je vyražena na kartě pomocí metody plastického písma. Embossing je nejrozšířenější způsob personifikace plastových karet. Po vyražení písma je možno toto reliéfní písmo obarvit. Tyto vyražené údaje na kartě lze snímat prostřednictvím mechanických imprinterů a přenášet je tak na pokladní stvrzenku.
2) hladký tisk (indent printing) – tato metoda se používá u karet, které se používají pouze v bankomatech nebo elektronických platebních terminálech. Nelze s nimi tedy platit v obchodech vybavených mechanickým imprinterem.

Elektronickým záznamem dat jsou na kartě uložena data potřebná k operaci s platební kartou. Tato forma do určité míry určuje úroveň zabezpečení karty. Rozlišujeme základní tři způsoby elektronického záznamu dat:

1) magnetický proužek. Jde o klasický způsob záznamu uložení dat, který je v současné době nejvíce rozšířen. Avšak tato rozšířenost má za následek překonání této technologie zabezpečení, následné prolomení ochrany a zneužití karty. Tento způsob umožňuje manipulaci bez zadání PIN kódu a jediný prvek ochrany tak zůstává podpis majitele.
2) použití čipu – na těchto kartách je magnetický proužek nahrazen čipem, popřípadě jsou karty s magnetickým proužkem kombinované s čipem. Na tuto kartu lze uložit podstatně více informací než na karty s magnetickým proužkem, což má za následek zvýšení bezpečnosti při operaci s kartou. Tyto karty vyžadují při manipulaci zadání PIN kódu. Skutečnost, že data nelze tak jednoduše kopírovat jako u karet s magnetickým proužkem, také přispívá k jejich větší bezpečnosti.
3) laserové karty – záznam na těchto kartách je na stejném principu jako u kompaktních disků. Kapacita záznamu u těchto karet velmi vysoká. Avšak nevýhodou jsou velké náklady na výrobu karet i zařízení potřebné k jejich čtení. Tyto náklady a poněkud nižší ochrana dat, než v případě karet čipových, brání většímu rozšíření a uplatnění laserových karet do budoucna.

### 2.2.2 Druhy platebních karet podle způsobu zaúčtování transakce

**Debetní karty**

Debetní karta je přímo vázána na běžný účet klienta. Slouží pro bezhotovostní placení u kamenných i internetových prodejců. U kamenných prodejců platba probíhá přes terminál, který je on-line napojený na systém banky a platbu okamžitě zaúčtuje. Pokud klient nemá sjednaný kontokorentní úvěr, nelze jít u těchto karet do záporného zůstatku, tedy do mínusu. Nemá-li držitel debetní karty dostatek peněžních prostředků na běžném účtu, platba u obchodníka neproběhne. Debetní karty jsou nejčastěji používaný typem platebních karet u retailových klientů.

**Kreditní karty**

Na rozdíl od debetních karet není kreditní karta spojena s běžným účtem klienta, nýbrž s tzv. revolvingovým úvěrem poskytnutým bankou. Tento typ úvěru se vyznačuje tím, že se opakuje za stejných podmínek každý měsíc a také stanoveným limitem, do jehož výše je možno úvěr čerpat. Klient nemusí částku splácet ihned, avšak bývá stanovena minimální měsíční splátka. Úvěr čerpaný kreditní kartou je úročen poměrně vysokými úroky. Existuje

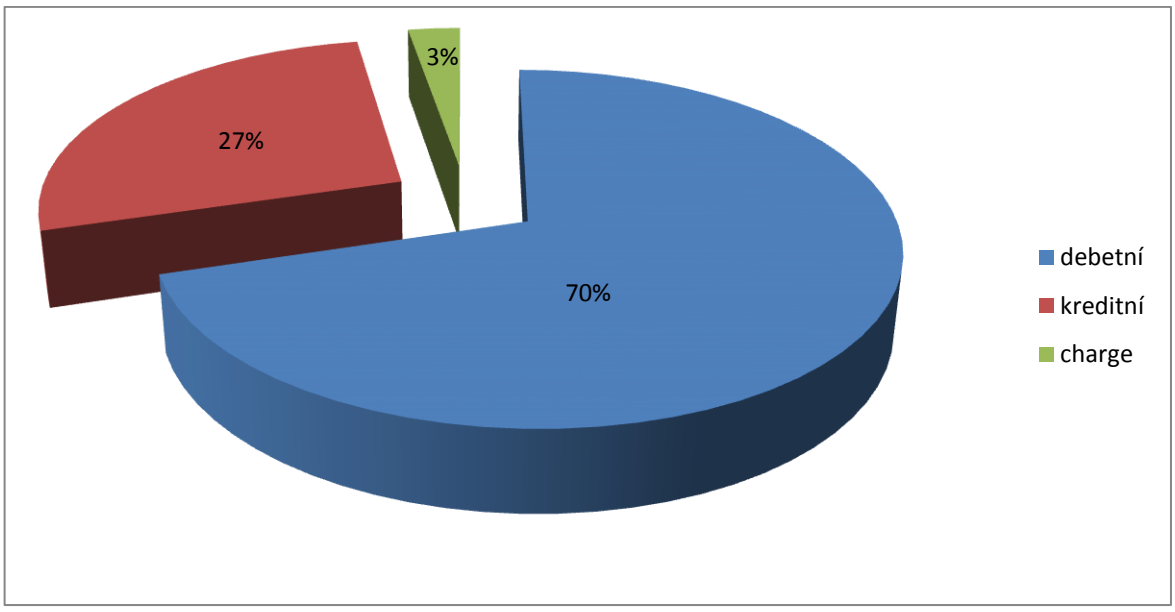
však i bezúročné období. Pokud klient během bezúročného období splatní dlužnou částku, tak neplatí žádné úroky. Toto období se pohybuje od 40 do 55 dnů. (Peníze.cz, ©2000 - 2012)

### Charge karty

Některé banky mají v nabídce produktů charge karty, které jsou nejstarším typem platební karty. Od kreditních karet se liší povinností klienta uhradit celou dlužnou částku vůči bance ke stanovenému datu v následujícím měsíci po období, kdy se úvěr čerpal. O dlužné částce držitele informuje měsíční výpis z účtu, kde jsou zaznamenány veškeré transakce, které byly s kartou prováděny. Tyto karty banky zpravidla vydávají jen svým ověřeným bonitním klientům.

### Elektronická peněženka

Jedná se o tzv. předplatní kartu (pre-paydcard). Hlavním účelem elektronické peněženky je omezení používání drobných bankovek a mincí. Jsou médiem nové generace umožňující platit pomocí předplacených částek. Transakce probíhá pomocí kontaktu čipové karty a platebního terminálu. Tuto kartu lze nabíjet u provozovatele systému za hotovost. (Polouček et al, 2006, s. 183)




*Obr. 2 Podíl druhů vydaných karet podle způsobu zaúčtování transakce na celkovém počtu vydaných karet v ČR v roce 2011 (vlastní zpracování dle dat SBK)*

## 2.3 Využití platebních karet

Platební karty umožňují držitelům různé způsoby využití. Mezi základní funkce platebních karet lze zmínit následující.

### 2.3.1 Výběr hotovosti pomocí bankomatu

Bankomat je zařízení, prostřednictvím kterého může klient získat hotovost bez asistence cizí osoby. Jednotlivé úkony jako například výše vybrané hotovosti si klient volí sám. Výhodou bankomatu je jednoduché ovládání a nepřetržitá dostupnost po celý den. Jediným požadavkem na klienta je znalost svého osobního identifikačního čísla, tj. PIN kódu, kterým prokazuje oprávněnost kartu používat. Banky si za použití bankomatu obvykle účtuje poplatek, který je pro jejich vlastní klienty zpravidla vyšší než pro klienty cizích bank. (Peníze.cz, ©2012)

### 2.3.2 Výběr hotovosti na pobočce banky

Při nemožnosti použít bankomat má klient možnost vybrat hotovost na pobočce banky. Na rozdíl od výběru z bankomatu je na pobočce banky po klientovi vyžadována identifikace pomocí dokladu totožnosti.

### 2.3.3 Bezhotovostní platby

Platba pomocí platební karty patří mezi nejvýhodnější způsoby využití platební karet, jelikož klient za použití platební karty nic neplatí. Banka své vlastní náklady spojené z realizace transakce kryje z poplatků, které vznikají obchodníkům za zprostředkování provedené transakce. Přímé bezhotovostní placení lze provádět v obchodech, restauracích, letištích, benzinových pumpách a dalších místech. (Dvořák, 2005, s. 378)

### 2.3.4 Cash back

Cash back je způsob vybírání hotovosti prostřednictvím platebních karet při platbě obchodníkovi. Klient si tak při placení může vybrat hotovost přímo u obchodníka do stanoveného limitu a nemusí tak ztrácet čas hledáním bankomatu. Odpadají tak poplatky za výběr hotovosti z bankomatu. Celkový součet platby a výběru se pak držiteli karty zaúčtuje společně. Tuto službu mají klienti bank aktivovanou automaticky s vydáním platební karty.

## 2.4 Autorizace platby platební kartou

Autorizace nebo-li proces získávání souhlasu s provedením platební operace, je základní formou zajištění platby platební kartou. Zabezpečuje totéž, co podpis platebního příkazu v běžném platebním styku. Je zajišťována v celosvětové elektronické síti několika způsoby. Rozlišujeme tedy autorizaci negativní, při které se ověřuje platnost karty a zda není překročen limit platby a autorizaci pozitivní, kdy se provádí předchozí operace a následně kontroluje zůstatek na účtu. (Polouček et al, 2006, s. 187)

Podle technického způsobu kontroly se autorizace dělí na:

1) elektronickou autorizaci s využitím PIN kódu. Tento způsob kontroly má využití při používání bankomatů, v obchodech při užití čipových karet a na místech, kde se využívají platební terminály
2) elektronickou autorizaci s využitím podpisu klienta. Na místech, kde se používají starší platební terminály a využívají se klasické platební karty s magnetickým proužkem, má využití tento proces kontroly.
3) ověření autorizačního limitu s využitím podpisu. V obchodech, které nejsou vybaveny elektronickými terminály, mají zastoupení mechanické imprintery při použití embosovaných karet.

## 2.5 Zabezpečení a rizika platebních karet

### 2.5.1 Ochranné prvky platebních karet

Ochrana platebních karet je záležitostí nejen výrobce, ale i jejich držitelů. Podle způsobu ohrožení se ochrana dělí na ochranu proti padělání a ochranu proti zneužití. Následující ochranné prvky jsou záležitosti výrobce karty, který tak kartu chrání proti padělání:

- Hologram - trojrozměrný obraz – znak na hologramu se mění při pohybu karty charakteristickým způsobem
- Podpisové proužky – slouží k záznamu vzorového podpisu držitele karty
- Ochranné prvky viditelné pouze v UV světle
- Speciální tisk karty
- Tisk čísla karty na podpisový proužek
- Kód za číslem karty na magnetickém proužku (Polouček et al, 2006, s. 187)


1 logo banky
2 EMV čip
3 číslo karty
4 jméno držitele karty
5 platnost karty
6 logo vydavatele karty
7 magnetický proužek
8 podpisový vzor
9 hologram
10 kód CVC

*Obr. 3 Rozmístění bezpečnostní prvků na platební kartě (vlastní zpracování)*

Ochrana proti zneužití karty přenáší zodpovědnost na držitele platební karty. Držitel karty by neměl nikomu cizímu sdělovat svůj PIN kód a musí chránit kartu proti krádeži. Dále kartu používat pouze na důvěryhodných obchodních místech a důvěryhodných zařízeních. Nemá-li držitel k obchodníkovi důvěru, měl by k platbě použít raději hotovost.

Při ztrátě nebo odcizení platební karty by měl držitel jednat rychle a kartu ihned zablokovat u vydavatele, poté v případě krádeže kontaktovat policii.

### 2.5.2 Skimming

Skimming je podvodné jednání, při kterém pachatelé elektronicky zkopírují údaje z magnetického proužku karty bez vědomí držitele karty. Tyto údaje následně nahrají na novou padělanou platební kartu. Skimmingová zařízení jsou nainstalovaná na bankomat v důmyslném systému, při kterém zařízení kopíruje magnetický proužek platební karty a minikamera snímá obraz, na kterém jde rozeznat zadávání jednotlivých číslic PIN kódu.

Banky proto instalují antiskimmingová zařízení zabraňující skenování karet, neoprávněné stahování jejich dat a dále zkvalitňují bezpečnost bankomatů.

Zneužít kartu kopírováním mohou prodavači v obchodech, kde držitel kartou platí, nebo číšníci v restauracích. V restauracích se může stát, že číšník si od klienta kartu vezme a odnese s sebou pryč z klientova dohledu. Pomocí kopírovacího zařízení zkopíruje magnetický pásek karty a opíše její číslo. Tato data pak může dále prodat třetím osobám na černém trhu k následné výrobě padělané karty.

V zahraničí je rozšířené falšování stvrzenek z již uskutečněných plateb. Tato činnost se děje v restauracích, v kterých mají platební terminály funkci, která umožňuje přidávat k účtu přirážku spropitného. Pokud klient tuto kolonku spropitného nevyplní, zůstává tato možnost na číšníkovi, který ji může zneužít ve svůj prospěch. (Matyáš a Krhovják, 2008, s. 86)

### 2.5.3 Libanonská smyčka

Útok pomocí libanonské smyčky spočívá v umístění pásky do otvoru pro vkládání platební karty do bankomatu. Pokud je platební karta vložena do bankomatu, páska ji zadrží a karta nejde zasunout dovnitř bankomatu, ani vytáhnout z bankomatu ven. K oběti tohoto podvodu se mezitím nachomýtne zdánlivě náhodný kolemjdoucí, který oběti poradí zadání PIN kódu, který podvodník odpozoruje. Jakmile oběť odejde reklamovat problém na pobočku banky, podvodník platební kartu vytáhne a s odpozorovaným PIN kódem vybere hotovost z bankomatu ještě předtím, než karta bude zablokována. (Matyáš a Krhovják, 2008, s. 86)

### 2.5.4 Podvody bez fyzické přítomnosti platební karty

Podvody bez přítomnosti karty jsou takové podvody, při kterých nejsou na místě uskutečňovaného prodeje přítomny buď držitel karty, nebo platební karta. Data o platební kartě jsou podvodně získávána při provedeném nákupu prostřednictvím písemné, telefonní, faxové nebo internetové objednávky.

Autentizačním prvkem při písemné nebo faxové objednávce je obvykle podpis klienta. Po rozšíření internetu se k těmto objednávkám začal používat internetový způsob objednávky, avšak bez autentizace podpisem. Bezhotovostní platby tohoto typu se staly u zákazníků velmi oblíbené.

Míra rizika zneužití je vyšší než u běžných transakcí z toho důvodu, že obchodník nemá možnost fyzicky zkontrolovat kartu, ani identitu držitele karty, který by se mohl prokázat, že je právoplatný držitel dané karty. U transakcí bez fyzické přítomnosti karty tak dochází ke zvýšenému počtu neoprávněných transakcí. Podvodníci data o kartách získávají ze zahozených nebo zkopírovaných potvrzení o transakcích, jejich podvodným vyžádáním např. e-mailem, z fiktivních internetových obchodů, hackováním databáze s údaji o provedených transakcích apod. Obdobně jako u podvodu padělanou kartou se právoplatný držitel karty o podvodu nedozví, dokud neobdrží výpis s pohybem transakcí na účtu.

Z pohledu bank je řada možností, jak se bránit podvodům bez fyzické přítomnosti karty. Jedna z možností je tisk třímístného kontrolního kódu do podpisového proužku na zadní straně karty. Klient je obchodníkem vyzván k jeho zadání při platbě jako autentizace skutečnosti, že klient má kartu ve svém držení.

Další z možností je zavedení prvku autentizace pro bezpečné platby, technologii 3D Secure. Tato technologie umožní autentizaci držitele karty anebo obchodní společnosti, která vlastní dotyčný internetový obchod. Pro využívání technologie 3D Secure je nutná registrace obchodníka u kartové asociace. Společnost VISA označuje tuto technologii jako "Verified by VISA", MasterCard jako "MasterCardSecuricode".

Princip této technologie 3D Secure je v tom, že nakupující neposkytuje obchodníkovi údaje o své platební kartě, ale přímo bance a tím je zajištěna větší bezpečnost. Informace o kartě jsou přenášena pomocí HTTPS protokolu, který údaje klienta zakóduje tak, aby údaje byly dostupné pouze bance. Držitel karty navíc může rozšířit proces autentizace při placení o další kontrolní údaje, které zná pouze on. I kdyby byla jeho karta odcizena a zneužita, nikdo jiný jeho kartou nezaplatí, i když bude mít zkopírované běžné údaje karty jako je číslo karty, datum expirace a kontrolní číslo. Zákazník je pak při platební transakci vyzván k zadání těchto dodatečných údajů, které si předem nastavil. Tyto dodatečné údaje mohou být z nejrůznějších oblastí zákazníkova života jako například oblíbený sportovní klub, jméno domácího mazlíčka nebo oblíbené jídlo. Až po zadání těchto správných dodatečných údajů je transakce provedena. Celý proces ověřování platby je následně rozšířen o jednorázové heslo zaslané přímo na mobilní telefon klienta, který tak transakci definitivně potvrdí. (ShopCentrik, ©2012)

Úroveň zabezpečení těchto plateb je na srovnatelné úrovni s transakcemi v internetovém bankovnictví. Klient si navíc může nastavit speciální limit pro placení kartou na internetu, nebo povolit platby bez přítomnosti karty jen na vyžádání, v tomto případě se jedná o dočasné odblokování na základě žádosti držitele karty a následné zablokování. Pokud nechce kartu k platbám na internetu používat vůbec, má zároveň možnost tyto platby zakázat.

Obecně banky technologii 3D Secure podporují a motivují zákazníky i obchodníky k jejímu využívání prostřednictvím různorodých akcí, například zdarma doprava zboží z konkrétního obchodu nebo přiložením dárku k nákupu. I díky této technologií podíl plateb na internetu na celkových platbách provedený prostřednictvím platebních karet meziročně roste.

### 2.5.5 Pojištění proti riziku zneužití karty

U některých bank má klient možnost se nechat pojistit proti riziku zneužití karty. Toto pojištění kryje ztráty ze zneužití karty v době od 24 hodin před nahlášením ztráty až do okamžiku převzetí odpovědnosti ze strany banky. Pojištění se nevztahuje na transakce, u kterých byl zadán PIN kód jako výběry z bankomatu a platbou u obchodníků. Pojišťovna hradí poplatky spojené s blokací či stoplistací a vydání karty nové.

Stoplist je listina odcizených embosovaných či ztracených embosovaných karet. Banka ji rozešle jednotlivým obchodníkům a svým partnerským bankám. Tento proces trvá delší časové období. Může trvat i několik dnů, během kterých lze kartu zneužít.

Povinností pojištěného je okamžitě po zjištění, že karta byla zneužita, ztrátu telefonicky ohlásit a následně ji v bance písemně potvrdit, a to nejpozději následující pracovní den po ohlášení, případně návratu ze zahraničí.

Placené pojistné závisí na požadovaném limitu pojištění. Čím vyšší placené pojistné je, tak tím je vyšší limit ochrany. Například za 150 korun klient získá ochranu do limitu 15 tisíc Kč, za 1300 korun ručí pojišťovna do výše 100 tisíc Kč. Avšak klient se podílí na pojistném případu desetiprocentní spoluúčasti, minimálně tři sta korun. Pojistka je sjednána jako jednorázová ke konkrétní kartě. Zaniká tedy dnem ukončení platnosti karty anebo nastáním pojistné události. (Peníze.cz, ©2000 – 2012)

Pojištění ztráty karty se vyplatí u karet embosovaných, které mají vysoké limity pro platby a výše poplatků za jejich stoplistaci dosahuje tisíců korun. Naproti tomu u karet elektronických přijde jejich blokace na méně peněz, než činí minimální výše spoluúčasti a pojištění tak kryje jen případné ztráty ze zneužití. Nemá smysl uzavírat pojistku pro karty Maestro, u kterých je ve většině zemí včetně České republiky pro všechny transakce vyžadován PIN a pojištění se na ně nevztahuje.

# 3 FORMY VZDÁLENÉHO PŘÍSTUPU K ELEKTRONICKÉMU BANKOVNICTVÍ

Za prostředky vzdáleného přístupu je možno označit produkty, které umožňují používat klasické bankovní produkty elektronickou cestou. Většinou se nejedná o nové produkty, nýbrž jejich proces podstaty využití se převedl do elektronické podoby. U některých produktů se využití produktu téměř nezměnilo, u jiných lze hovořit o vzniku nového produktu.

## 3.1 Telebanking

Telebanking nebo-li phonebanking je telefonní platební styk, který umožňuje ovládat svůj účet prostřednictvím hlasové komunikace. Tato komunikace probíhá buď s živým zaměstnancem call centra banky nebo s hlasovým informačním systémem. Identifikace klienta probíhá pomocí systému hesel, která zná pouze klient a banka. V rámci bezpečné komunikace z důvodu možného odposlouchání hovoru banka nevyžaduje po klientovi celé přístupové heslo, ale například pouze 4. či 6. znak hesla. Pomocí phonebankingu lze zjišťovat aktuální zůstatek na běžném účtu, provádět jednorázový i trvalý příkaz k úhradě a realizovat doplňkové služby jako například zablokování platební karty z důvodu ztráty či krádeže. Tento způsob je vhodný pro klienty, kteří z nějakého důvodu nechtějí nebo nemají možnost využívat internetové bankovnictví (Máče, 2006, s. 171)

## 3.2 GSM banking

GSM banking je platební styk realizovaný přes mobilní telefon. Komunikace může být založena na:

1) šifrovaných SMS zprávách – komunikace probíhá podle předem přesně strukturovaných příkazů prostřednictvím SMS zpráv. Klient zadá požadavek na konkrétní úkon a banka mu pošle zpět na mobilní telefon požadovanou informaci.
2) technologii SIM toolkitu – tento způsob vyžaduje SIM kartu s nainstalovanou bankovní aplikací, která umožňuje jednoduchou správu účtů. Pro spuštění aplikace je vyžadováno zadání hesla v podobě BPINu. (Máče, 2006, s. 171)

## 3.3 WAP banking

Služba WAP spočívá v komunikaci po Internetu pomocí protokolu WAP. Jedná se o kombinaci telefonní a internetového bankovnictví, kdy mobilní telefon přistupuje na WAPové

stránky banky, což jsou zjednodušené a zmenšené webové stránky pro menší displeje mobilních telefonů. (Máče, 2006, s. 171)

V současné době je tento způsob komunikace klienta s bankou na ústupu především díky rozšíření smartphonů s mobilním internetem, který umožnuje přístup na plnohodnotnou aplikaci internetového bankovnictví. Proto klienti nemají potřebu používat tento celkem zastaralý systém.

## 3.4 Homebanking

Homebanking je založen na propojení osobního počítače klienta s počítačem banky pomocí speciálního programu, který je nainstalován na klientův počítač. Poskytuje nepřetržitý přístup k službám jako například příkazy k úhradě, trvalé příkazy, zůstatky na účtu, konverze měn. Tento způsob vylučuje veškerý papírový kontakt mezi bankou a klientem. Vyžaduje určitou technickou způsobilost klienta. Bezpečnost je založena ochraně k přístupu k datům pomocí hesel, kódovaných zasílaných zpráv a digitálního podpisu. Výhodou zde je, že tato služba bývá kompatibilní s účetními a ekonomickými programy, ale nevýhodou je, že lze používat pouze počítač, kde je program nainstalován. Alternativou k homebankingu je internetové bankovnictví (Finance.cz, ©2012)

## 3.5 Internetové bankovnictví

„Internetové bankovnictví jsou služby pro manipulaci s účtem prostřednictvím počítače a sítě Internet“. (Matyáš a Krhovják, 2008, s. 79)

Na rozdíl od služby homebanking, pro provoz internetového bankovnictví stačí připojení k Internetu a webový prohlížeč. Uživatel internetového bankovnictví může pomocí této služby provádět obdobné úkony jako v telefonním bankovnictví, například zadávání jednorázových a trvalých příkazů, založení termínovaného vkladu, zjišťování stavu na účtech. Klientovi přináší velkou výhodu v podobě online informace, protože zrakový vjem je jednodušší a lépe přijímán než sluchový. (Máče, 2006, s. 172)

Komunikace v rámci internetového bankovnictví probíhá pomocí standardního protokolu SSL. Protokol SSL je v současné době jednou z nejpoužívanějších metod zajištění bezpečného přenosu dat přes počítačové sítě. Pomocí digitálních certifikátů je tak zašifrována veškerá komunikace mezi klientem a serverem. Při použití SSL může mít uživatel jistotu,

že server, kterému odesílá data, je skutečně server, který zamýšlel navštívit, a hlavně, že předávaná data nemohou být odposlechnuta a zneužita třetí stranou. (ACTIVE 24, ©2011)

### 3.5.1 Metody autentizace internetového bankovnictví

Je vhodné zmínit následující termíny, které se používají v procesu zabezpečení bezpečného přihlášení klienta do internetového bankovnictví a následné bezpečné platební transakce.

- Identifikace*: Identifikace uživatele je proces, ve kterém se uživatel představí systému jako platný uživatel.*

- Autentizace*: Proces, který určuje skutečnou, pravou identitu uživatele, který se snaží o přístup do systému.*

- Autorizace*: Tento proces určuje, které aktivity budou povoleny. Běžně je autorizace v kontextu s autentizací. Jakmile se uživatel autentizuje, jsou mu přiděleny určitá oprávnění.* (CAMO, ©1997-2012)

U internetového bankovnictví se můžeme setkat s rozličnými způsoby autentizace, které využívají:

- uživatelského jména a hesla
- certifikátu
- elektronického podpisu
- SMS kódu
- autentizačního PIN kalkulátoru
- souřadnicovou autentizaci

Uživatelské jméno a heslo je považováno za základní způsob ověření identity uživatele. Je vhodné ho kombinovat s dalšími způsoby autentizace. Z hlediska bezpečnosti je kladen požadavek na nově vytvářená hesla ohledně minimální délky, složení číslic, písmen a speciálních znaků. Bývá pravidlem, že po několika chybných pokusech dochází k dočasnému zablokování účtu. Pro odblokování je vyžadována návštěva pobočky banky, někdy stačí hovor na infolinku banky.

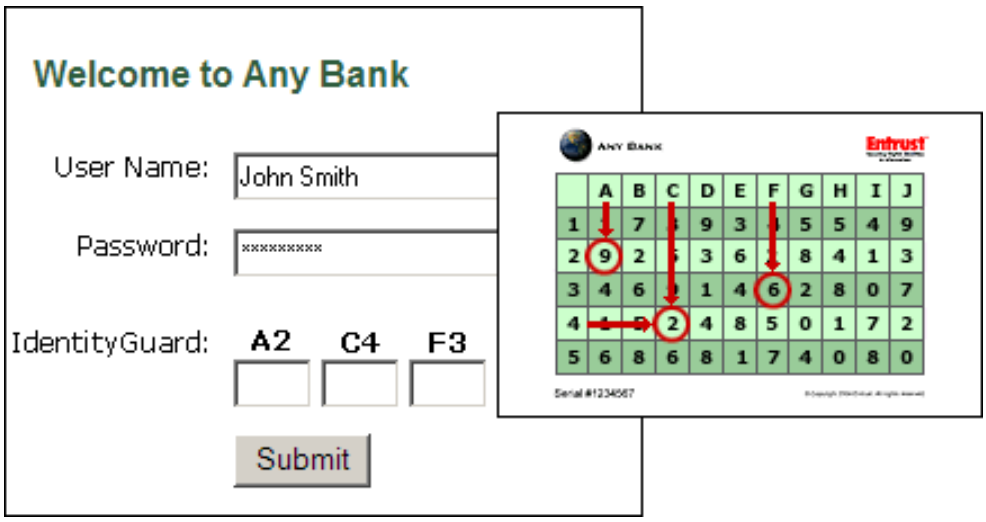
Banky mohou na přání klienta vydávat časově omezený certifikát, jenž je ověřen při žádosti o autentizaci. Součástí certifikátu je také příslušný soukromý klíč. Tento soukromý klíč spolu s certifikátem jsou uloženy na externím paměťovém médiu typu flash disk, disketa, paměťová karta a jsou nahrávány z média jenom tehdy, jsou-li potřeba. Banky nabí-

zejí možnost nahrání certifikátu a citlivých dat na tzv. kryptografickou čipovou kartu, které má tu výhodu, že uživatel citlivá data z karty, byť třeba jenom omylem, nesmaže. Kryptografická karta provádí totiž veškerá operace automaticky sama.

Elektronický podpis se využívá při komunikaci se speciálními programy. Je to v podstatě program, který je postaven bázi dvou klíčů, tajného a veřejného. Veřejný klíč musí být aktivován pro danou komunikaci odpovědnou autoritou. Klient i banka mají vytvořeny dva klíče. Proces zabezpečení a komunikace této technologie spočívá v tom, že odesílatel zašifruje svá data pomocí svého tajného klíče a veřejného klíče druhé strany čili příjemce. Ta obsah komunikace rozšifruje pomocí svého tajného klíče a veřejného klíče odesílatele a tím je zajištěna identifikace a autentizace.

Doplněním elektronického podpisu je využití hashovací funkce, prostřednictvím které lze vytvořit otisk zprávy, takzvaný hash. Vstupem hashovací funkce může být libovolně dlouhá zpráva, výstupem je pak otisk, který má pevně stanovenou délku. Jestliže je ve zprávě změněno jedno písmeno, pak otisk na výstupu je úplně jiný. Nejvyužívanější hashovací funkce jsou MD5 (Message digest) a SHA-1 (SecurehashAlgoritm). Hash se používá k elektronickému podpisu tak, že se k připravenému dokumentu, například příkazu k úhradě, vypočte hash pomocí hashovací funkce. Dále se hash šifruje s tajným klíčem odesílatele a veřejným klíčem příjemce a zašifrovaný výstup se pošle příjemci. Příjemce pomocí svého tajného a veřejného klíče odesílatele rozšifruje dokument, ve kterém pak stejná hashovací funkce vypočítá hash a porovná ho s přiloženým rozšifrovaným otiskem. Pokud se oba hashe neliší, nebylo s dokumentem manipulováno a transakce je tak bezpečná. (Máče, 2006, s. 166)

Zajímavým a méně nákladným je řešení firmy Entrust zvané Identity Guard. Toto řešení umožňuje oboustrannou souřadnicovou autentizaci. Uživatel dostane kartu, kterou používá po stanovenou dobu, po expiraci dostane kartu novou. Na kartě je tabulka s předtištěnými znaky viz obrázek Uživatel je při autentizaci, kromě uživatelského jména a hesla, vyzván k zadání písmen na dané souřadnici, například A2, C4 a F3.




*Obr. 4 Souřadnicová autentizace společnosti Entrust (Entrust, ©2012)*

Tato dodatečná autentizace poskytuje ochranu proti phishingu a malwaru. Pokud by tyto útoky na klientovu bezpečnost odhalily uživatelské jméno a heslo, pak v případě použití souřadnicové autentizace by odhalily jenom málo znaků z celé tabulky znaků. (Matyáš a Krhovják, 2008)

### 3.5.2 Metody autorizace transakcí

Pro autorizaci transakcí se používají prakticky stejné způsoby jako v případě autentizaci uživatele. Lze použít soukromý klíč a příslušný podpisový certifikát umístěný buď v počítači, přenosném médiu nebo čipové kartě. Banka může také využít metodu TAN, při které se klientovi zasílají na mobilní telefon vygenerované jednorázové autorizační kódy s časově omezenou platností.

Klient si také může vyžádat od banky sadu velkého množství jednorázových autorizačních kódů, které postupně zadává při požadavku na autorizaci nebo autentizaci. Tuto sadu například sto kódů lze získat přímo na pobočce banky, poštou, nebo prostřednictvím šifrovaných SMS zpráv.

Pro šifrování dat v GSM sítích se používá symetrický algoritmus A5. Tímto algoritmem jsou šifrována však pouze data mezi mobilním telefonem a základnovou BTS stanicí. Z toho vyplývá, že organizace spravující infrastrukturu GSM má přístup k dešifrovaným datům a operátor u SMS uchovává minimálně informace o odesílateli a příjemci zprávy a datum. Šifrování přenášených dat není povinná vlastnost sítě a není obtížné ji také obejít. Proto jsou zprávy odesílané v rámci GSM bankingu navíc šifrované SIM toolkitem se sdí-

leným symetrickým klíčem uloženým v bance a na SIM kartě. (Matyáš a Krhovják, 2008, s 81)

Některé banky nabízejí klientům formu autorizace operací s platební kartou v podobě jejího uzamčení. Dokud je karta "uzamčena", nelze s ní provádět žádné finanční transakce. Jakmile dá klient pokyn (např. SMS zprávou), karta se pro finanční operace odemkne. Toto odemknutí může být trvalé, ale i časově omezené.

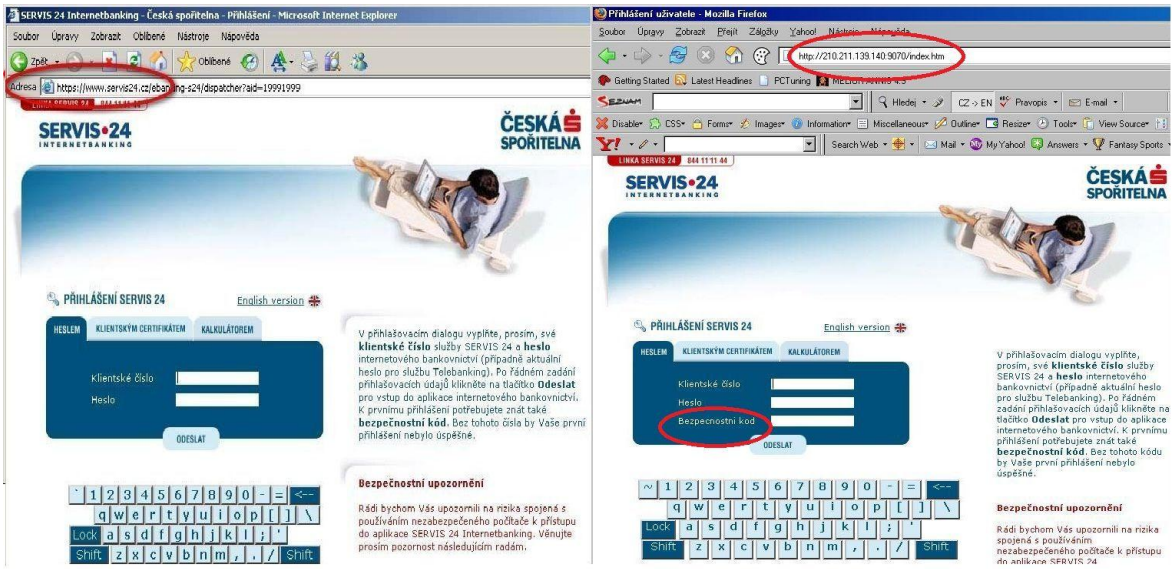
Kromě již popsaných způsobů autorizace je pro elektronické transakce nastaven časový limit, během kterého lze provést transakce v určité maximální výši. Časový limit obvykle bývá denní a výše transakce se v různých bankách liší, v českých maximálně až 300 tisíc Kč. Pro rychlé zjištění neoprávněné operace je také vhodné povolit notifikaci klienta o transakci formou SMS zprávy.

### 3.5.3 Rizika internetového bankovnictví

**Phishing**

Jako phishing je označena technika podvodu, při které útočník zasílá hromadně podvodné e-mailové zprávy, které mají za cíl vyvolat zdání, že byly odeslány z e-mailové adresy klientovy banky. Tento mail je zpravidla psán lámanou češtinou nebo angličtinou a obsahuje kromě zprávy také odkaz. Pokud uživatel klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky banky. Na podvodných stránkách je připraven formulář, kde jsou požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě. Kromě toho se podvodníci snaží z klientů vylákat přihlašovací údaje k elektronickým peněženkám, se kterými se obchoduje a platí na internetu. (PayPal, eBay, Paysec). Cílem phishingového e-mailu je tedy získání přihlašovacích údajů a jejich následné zneužití. (Hoax, ©2000-2012)

Phishingový e-mail může tedy vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, či jako výzkum klientské spokojenosti. Slovo phishing vzniklo jako zkratka výrazů „***p**assword**h**arvesting**f**ishing***“, což v doslovném překladu znamená „sběr hesel rybařením“. Postup podvodníků totiž připomíná techniku rybaření. Rozesílají hromadně e-maily na mnoho náhodných adres, tak jako rybáři, kteří rozhazují sítě do vody a rovněž čekají, jaký úlovek se chytí na návnadu. V České republice jsou nejčastější obětí phishingu klienti České Spořitelny. (Bezpečný internet, ©2012)




*Obr. 5 Srovnání zabezpečeného přístupu se stránkou napadenou pomoci phishingu (Pooh, ©2006)*

### Pharming

Metoda pharming využívá speciální počítačové programy založené na manipulaci s DNS servery, které klienty při přihlášení do internetového bankovnictví automaticky přesměrují na stránky, které jsou věrnou replikou stránek klientovy banky, ale ve skutečnosti jsou pouze jejich napodobeninou. Zde tyto stránky poté klienta požádají o zadání všech přihlašovacích jmen a příslušných hesel k nim. Pokud je klient zadá, tak se mohou neoprávnění uživatelé přihlásit do internetového bankovnictví pod jeho jménem provádět tak neoprávněné transakce. Jestliže nemá klient nastavenu autorizaci transakce pomocí dalšího zabezpečení např. pomocí autorizační SMS nebo certifikátu, může útočník klientovi bez zábran převádět peníze z jeho účtu. (Bezpečný internet, ©2012)

### 3.5.4 Budoucnost internetového bankovnictví

S nárůstem uživatelů mobilního internetu ve smartphonech (chytrých telefonech) bude růst počet klientů bank, kteří budou chtít využívat internetové bankovnictví skutečně kdykoli a kdekoli. U těchto zařízení lze k internetovému bankovnictví přistupovat prostřednictvím standardního webového rozhraní nebo prostřednictvím aplikace určený pro daný operační systém uživatele. Již v současné době mají banky v nabídce aplikace pro operační systém Android nebo pro uživatele produktů Apple iPhone nebo iPad s operačním systémem iOS.

Použití je jednoduché. Uživatel si zdarma stáhne z interaktivního obchodu (Google Play nebo AppStore, záleží na uživatelovu operačním systému) aplikaci, prostřednictvím které může přistupovat ke svému účtu kdykoliv, kdy má fungující internetové připojení. Tato aplikace klientovi umožní vykonávat běžné úkony jako provádět platební příkazy, vypsat historii transakcí nebo kurzovní lístek.

Některé banky v této aplikaci implementovali funkci, která obsahuje mapu bankomatů a poboček. Prostřednictvím GPS navigace v telefonu se na mapě zobrazí uživatelova poloha a jednotlivé bankomaty a pobočky v okolí. Klepnutím na ulici nebo město, kde se pobočka nebo bankomat nachází, se zobrazí náhled s otevírací dobou a pokud uživatel bude chtít, navigace ho dovede k zadanému cíli. (iWOZ, ©2012)

### 3.5.5 Budoucnost autentizace internetového bankovnictví

Uživatelé internetového bankovnictví budou i nadále při autentizaci používat klasické uživatelské číslo a heslo, nicméně se stále častěji bude objevovat tzv. vícefaktorová autentizace. Vícefaktorová autentizace je založena na vlastnictví nějakého předmětu, kterým se uživatel prokazuje, že je oprávněn disponovat s daným účtem. Tento předmět může být hardware token.

Nejznámějším hardware tokenem je token typu společnosti RSA, který generuje jednorázové kódy na displeji. Jeho výhodou je, že je velice obtížně ho zkopírovat. Potíž nastává tehdy, když jej jeho majitel ztratí nebo se mu token rozbije. Do doby, než klient obdrží token nový, nemůže se přihlásit ke svému účtu. Tyto tokeny mohou být v budoucnosti nahrazeny smartphony, které by umožnily přijímat jednorázové kódy pomocí SMS zpráv nebo pomocí softwarových aplikací tyto hesla jednorázově generovat.


*Obr. 6 Hardware token společnosti RSA (PokerStars, ©2012)*

Další z metod autentizace, která se bude v budoucnosti prosazovat, je autentizace na základě biometrických informací. Biometrické informace jsou jedinečnými identifikačními znaky každého člověka, nelze jej proto zaměnit s jinými, je tak zaručena vysoká spolehlivost a přesnost této metody. „Biometrické informace pracují s různými charakteristickými znaky člověka, jako jsou otisk prstu, geometrie tváře, duhovka oka, sítnice oka, geometrie ruky, geometrie prstů, struktura žil na zápěstí, tvar ucha, složky lidského hlasu, lidský pach, DNA, dynamika podpisu a dynamika psaní na klávesnici.*"* (Ščurek, 2008)

Při volání do banky se tak budeme setkávat s technologií rozpoznávání hlasu, při přihlašování do internetového bankovnictví s funkcí rozpoznávání obličeje uživatele a také způsobu psaní hesla na klávesnici. Tyto technologie na rozdíl od například snímače otisku prstů nevyžadují instalaci žádného speciálního hardware zařízení. (CleverAndSmart, ©2012)

# II. PRAKTICKÁ ČÁST

# 4 MARKETINGOVÝ VÝZKUM SPOKOJENOSTI KLIENTŮ

Tato kapitola je zaměřena na proběhlý marketingový výzkum spokojenosti klientů mezi retailovými uživateli elektronického bankovnictví prostřednictvím dotazníkového šetření. Dotazník byl vytvořen elektronickou formou pomocí služby Google Docs a distribuován respondentům prostřednictvím e-mailu a Facebooku. Cílem dotazníku bylo zjistit spokojenost retailových klientů s používanými produkty elektronického bankovnictví, jejich přednosti a nedostatky. Taktéž byly zjišťovány názory respondentů na zabezpečení služeb i jejich stanoviska ohledně možného způsobu zabezpečení do budoucna. Tento dotazník obsahuje celkem 25 otázek a vyplnilo jej 296 respondentů.

## 4.1 Stanovení hypotéz

Na úvod jsou stanoveny tyto hypotézy, které po vyhodnocení dotazníku potvrdíme nebo vyvrátíme.

**H1** – Více než 90% respondentů starších 18 let, ale zároveň mladších než 29 let využívá nějaký produkt elektronického bankovnictví

**H2** – Alespoň 50% respondentů s nižším než vysokoškolským vzděláním by nevyužilo při přihlašování do internetového bankovnictví biometrické informace

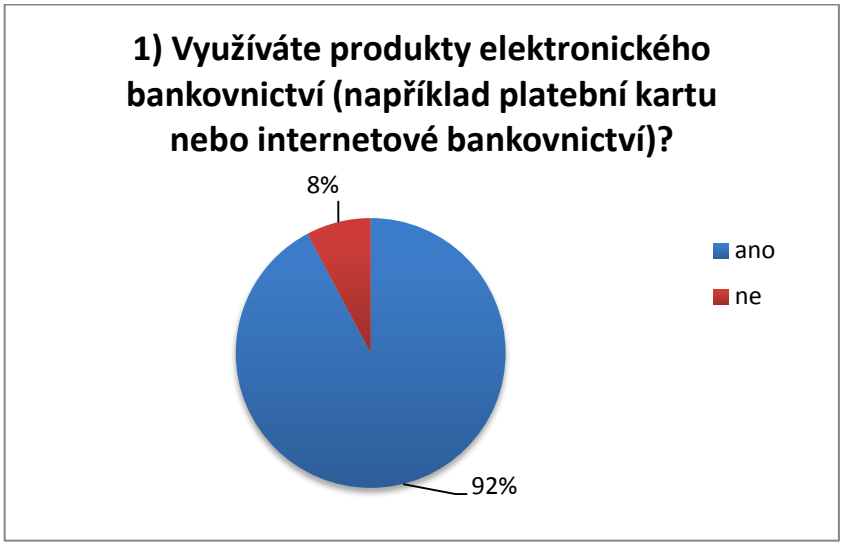
**H3** – Alespoň 60% dotazovaných nad 29 let si myslí, že internetové bankovnictví není bezpečné

**H4** – Více než 80% dotazovaných klientů Komerční banky, ČSOB, České spořitelny a mBank je spokojeno s funkčností a spolehlivostí internetového bankovnictví

**H5** – Více než 42% dotazovaných klientů Komerční banky si myslí, že jsou poplatky za používání produktů elektronického bankovnictví vysoké.

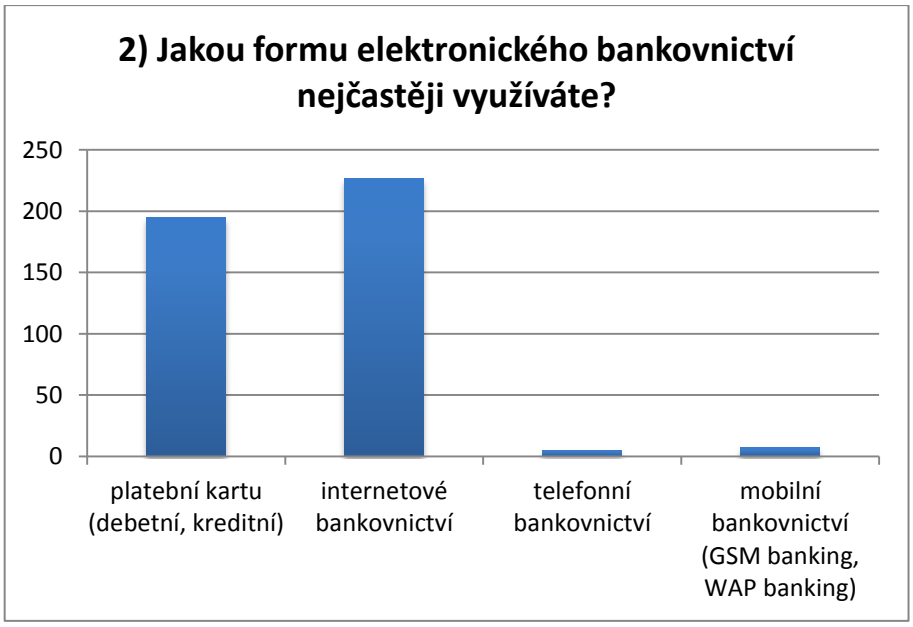
## 4.2 Vyhodnocení dotazníkového šetření

**Otázka č. 1**: Využíváte produkty elektronického bankovnictví (například platební kartu nebo internetové bankovnictví)? – byla filtrační, podle zvolené odpovědi se dotazník větvil dále. Odpověď „ano“ zvolilo 273 respondentů, kteří pokračovali otázkou č. 2. Odpověď „ne“ zvolilo 23 respondentů, kteří pokračovali otázkou č. 21.



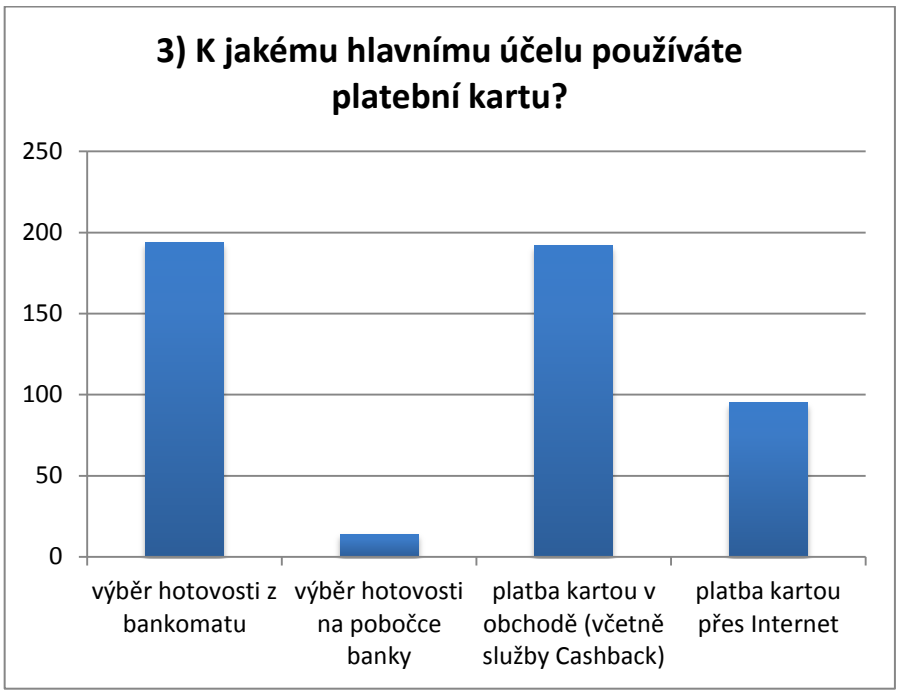

*Obr. 7 Otázka č. 1 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 2**: Jakou formu elektronického bankovnictví nejčastěji využíváte? U této otázky byla možnost více odpovědí. Respondenti nejčastěji využívají internetové bankovnictví (227 uživatelů z 273 dotázaných) a platební kartu (195 uživatelů). Naopak telefonní a mobilní bankovnictví využívá mizivé množství dotázaných, tzn. 5 respektive 7 respondentů.




*Obr. 8 Otázka č. 2 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 3**: K jakému hlavnímu účelu používáte platební kartu? Také v této otázce respondenti mohli zvolit více odpovědí. Z nejčastějších odpovědí lze vyvodit, že respondenti používají platební kartu k výběrům hotovosti z bankomatu (195 dotázaných) a také k platbě v obchodě (192 dotázaných), méně pak k platbám na Internetu (95 dotázaných). K výběru hotovosti na pobočce banky využívá platební kartu pouze 14 dotázaných.




*Obr. 9 Otázka č. 3 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 4**: Využíváte kreditní kartu? Kreditní kartu využívá 164 dotázaných (55%), nevyužívá 132 dotázaných (45%)

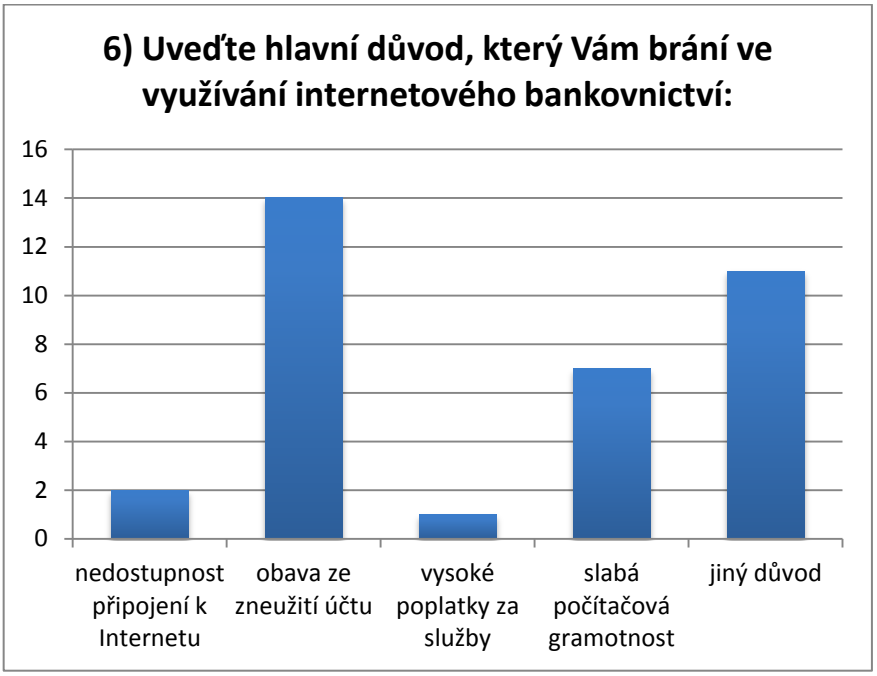

*Obr. 10 Otázka č. 4 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 5**: Jak často se přihlašujete do internetového bankovnictví? Tato otázka zjišťovala, jak často se klienti přihlašují do internetového bankovnictví. Pokud respondent zvolil odpověď „vůbec, internetové bankovnictví nevyužívám“ byl přesměrován na otázku č. 6, v případě jiné odpovědi na otázku č. 7.

Denně se do internetového bankovnictví přihlašuje 44 dotázaných (15%), jednou za týden 159 dotázaných (54%), jednou za měsíc 58 dotázaných (19%) a 35 dotázaných, tedy 12% dotázaných, internetové bankovnictví nevyužívá vůbec.


*Obr. 11 Otázka č. 5 dotazníkového šetření (vlastní zpracování)*

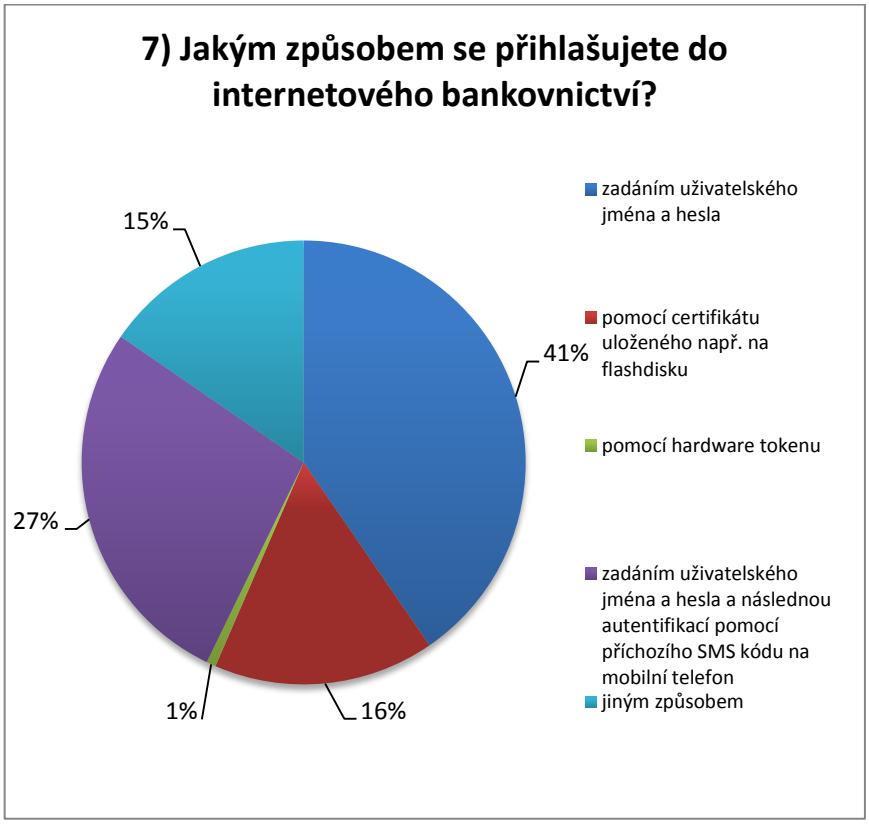
**Otázka č. 6**: Uveďte hlavní důvod, který Vám brání ve využívání internetového bankovnictví: Tato otázka měla zjistit důvody, kvůli kterým respondenti v otázce č. 5 zvolili možnost, že vůbec nevyužívají internetové bankovnictví. Respondenti mohli zvolit více možností. Nejčastější odpověď byla možnost „obava ze zneužití účtu“ (14 dotazovaných) a „slabá počítačová gramotnost“ (7 dotazovaných). Jiný důvod uvedlo 11 dotázaných a někteří konkrétně vypsali, že nemají potřebu využívat internetové bankovnictví nebo že využívají internetové bankovnictví příbuzných. Po této odpovědi respondenti nevyužívající internetové bankovnictví pokračovali otázkou č. 21.




*Obr. 12 Otázka č. 6 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 7**: Jakým způsobem se přihlašujete do internetového bankovnictví?

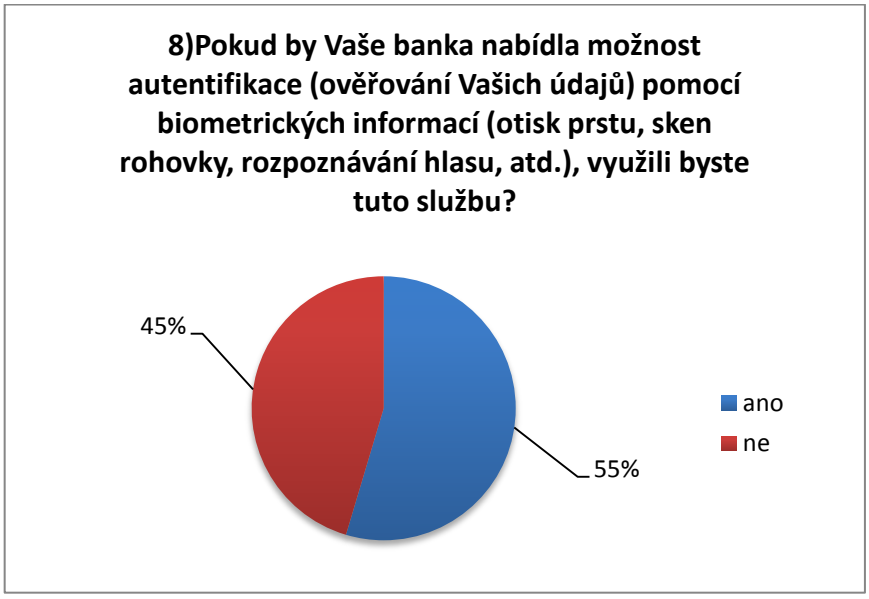
Zadáním uživatelského jména a hesla se do internetového bankovnictví přihlašuje 119 respondentů (41%), 83 respondentů (27%) využívá tutéž možnost, avšak navíc s autentifikací pomocí příchozího SMS kódu na mobilní telefon. Pomocí certifikátu se přihlašuje 47 respondentů (16%) a hardware token využívají pouze 2 respondenti. Jiným způsobem se přihlašuje 45 respondentů.




*Obr. 13 Otázka č. 7 dotazníkového šetření (vlastní zpracování)*

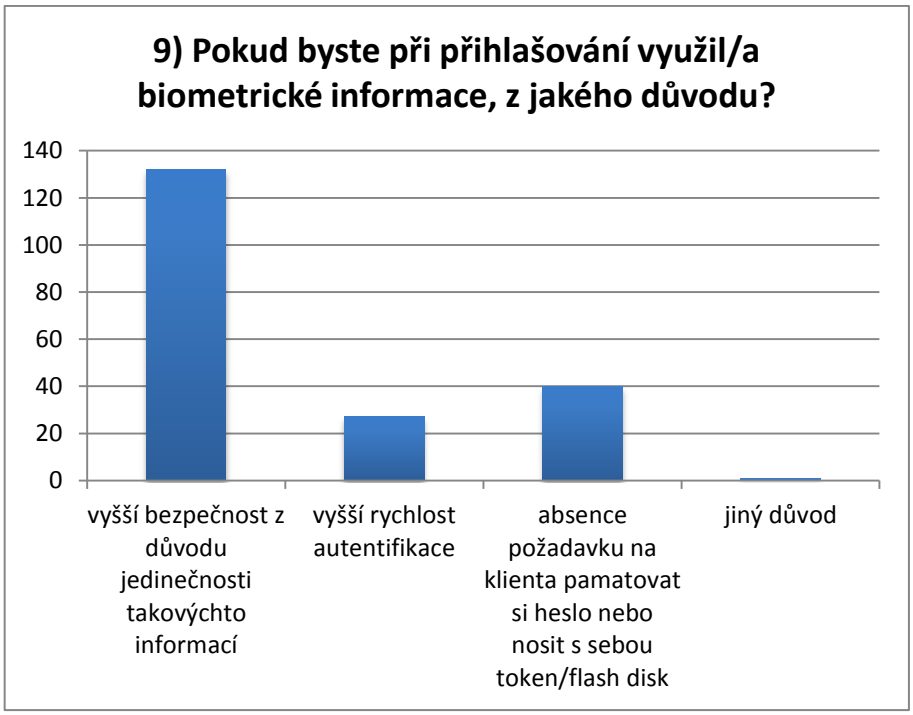
**Otázka č. 8**: Pokud by Vaše banka nabídla možnost autentifikace (ověřování Vašich údajů) pomocí biometrických informací (otisk prstu, sken rohovky, rozpoznávání hlasu, atd.), využili byste tuto službu?

Cílem této otázky bylo zjistit, jestli by respondenti využili možnosti přihlášení internetového bankovnictví pomocí biometrických informací, pokud by jim to jejich banka nabídla. Respondenti, kteří zvolili „ano“ (142 dotázaných), pokračovali dále otázkou č. 9, v opačném případě, při volbě odpovědi „ne“ (118 dotázaných), tyto respondenty čekala otázka č. 10.




*Obr. 14 Otázka č. 8 dotazníkového šetření (vlastní zpracování)*

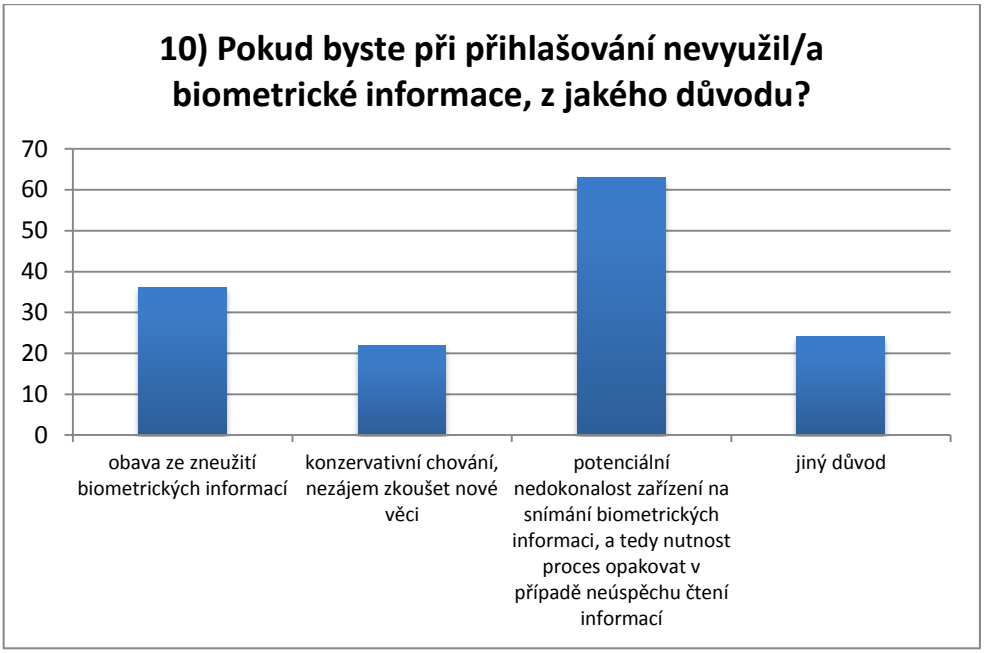
**Otázka č. 9**: Pokud byste při přihlašování využil/a biometrické informace, z jakého důvodu? Zde byla možnost výběru více odpovědí. Jako nejčastější odpověď byla uváděna odpověď týkající se vyšší bezpečnosti (132 dotázaných)




*Obr. 15 Otázka č. 9 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 10**: Pokud byste při přihlašování nevyužil/a biometrické informace, z jakého důvodu? Nejčastější odpověď u této otázky byla čistě hypotetická a to „vyšší bezpečnost z důvodu jedinečnosti takovýchto informací“ (63 dotázaných). V případě, že by byli snímače

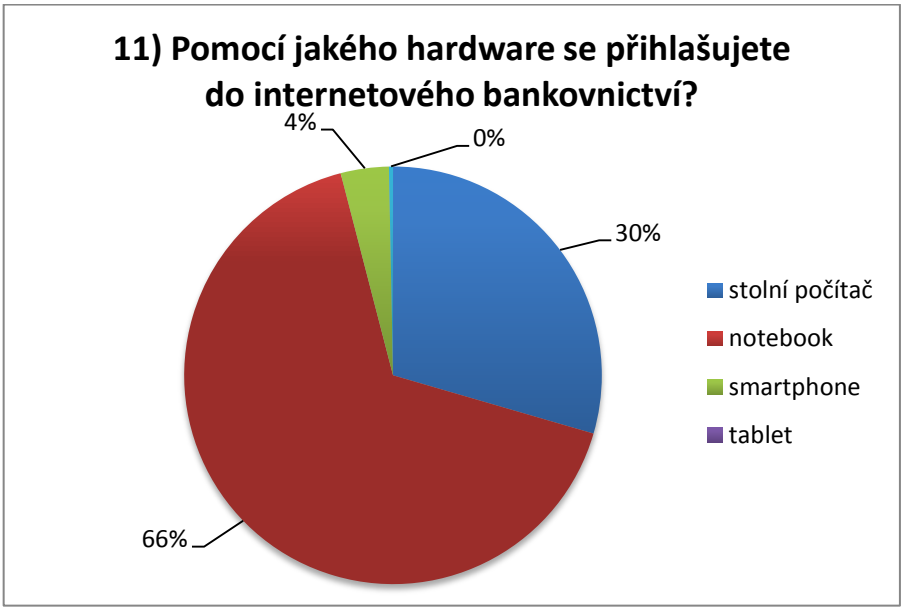
a čtečky biometrických informací dokonalé a tento problém odpadá, se ale zneužití informací obává 36 dotázaných. Konzervativní chování a nezájem zkoušet nové věci uvádí jako důvod nevyužití 22 dotázaných.




*Obr. 16 Otázka č. 10 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 11**: Pomocí jakého hardware se přihlašujete do internetového bankovnictví?

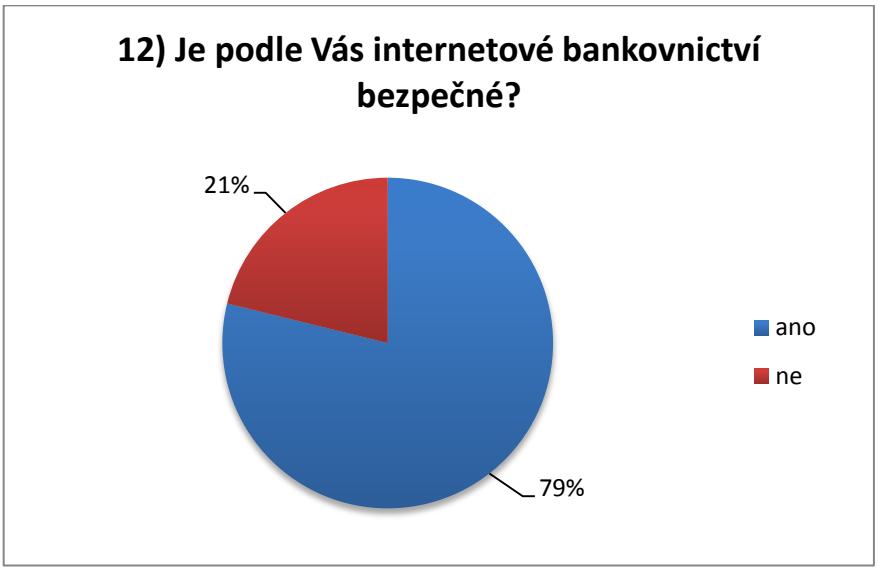
Opět možnost více odpovědí. Většina respondentů se připojuje pomocí notebooku. Dále pomocí stolního počítače a smartphonu. Přes tablet se nepřipojuje žádný respondent.




*Obr. 17 Otázka č. 11 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 12**: Je podle Vás internetové bankovnictví bezpečné?

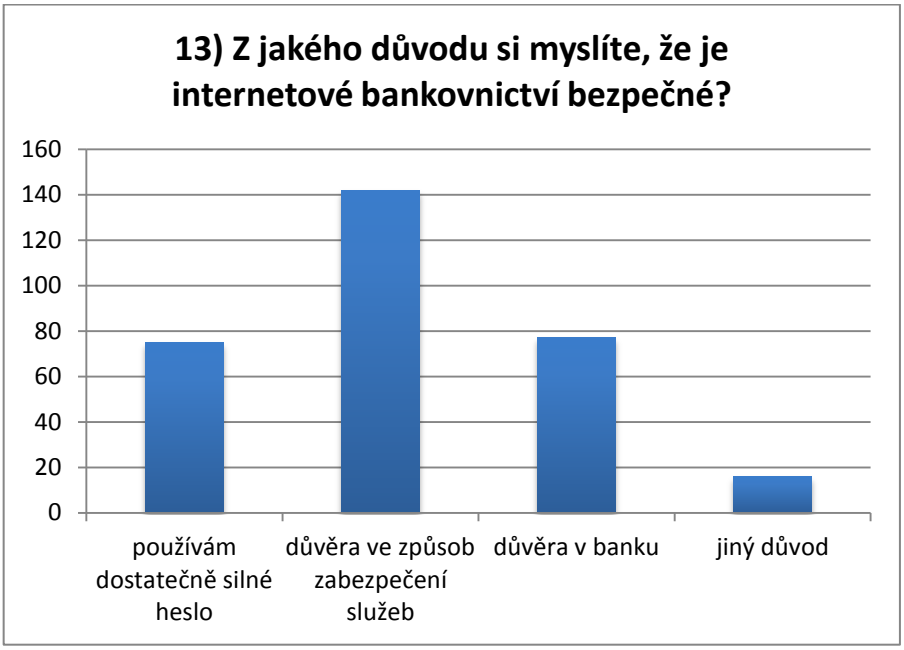
Internetové bankovnictví je bezpečné pro 205 dotázaných, na které čekala otázka č. 13. Opačného názoru je 55 dotázaných, kteří pokračovali otázkou č. 14.




*Obr. 18 Otázka č. 12 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 13**: Z jakého důvodu si myslíte, že je internetové bankovnictví bezpečné?

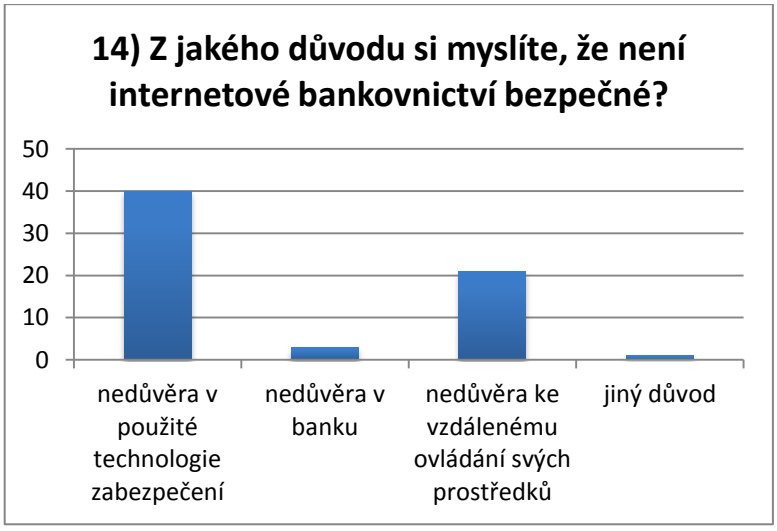
Že je internetové bankovnictví bezpečné z důvodu použití silného hesla si myslí 77 respondentů, bance důvěřuje 76 respondentů a 143 respondentů důvěřuje ve způsob zabezpečení služeb. Respondenti měli možnost zvolit více odpovědí.




*Obr. 19 Otázka č. 13 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 14**: Z jakého důvodu si myslíte, že není internetové bankovnictví bezpečné?

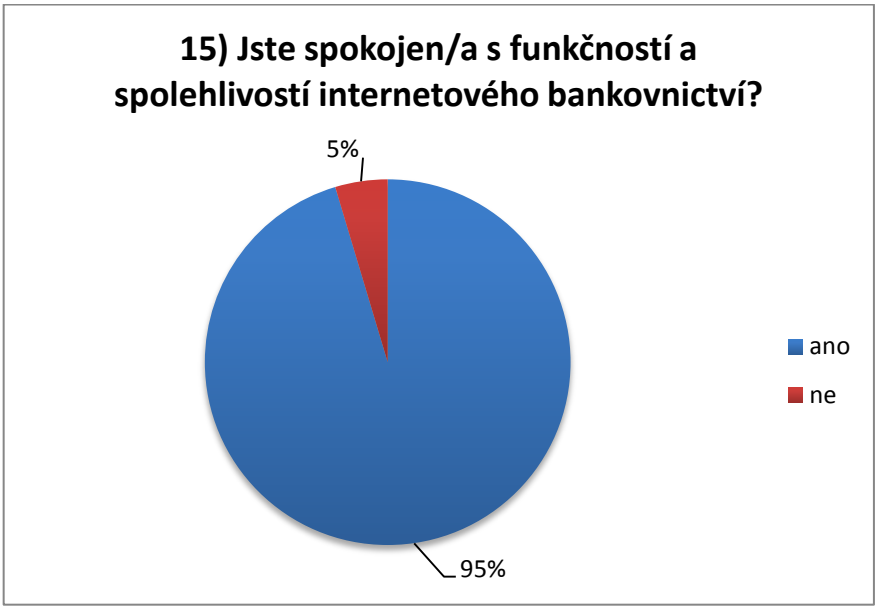
Nedůvěru k použitým technologiím zabezpečení vyjádřilo v odpovědi 40 dotázaných, dále 21 dotázaných nedůvěřuje vzdálenému ovládání svých prostředků a bance nedůvěřují 3 dotázaní.




*Obr. 20 Otázka č. 14 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 15**: Jste spokojen/a s funkčností a spolehlivostí internetového bankovnictví?

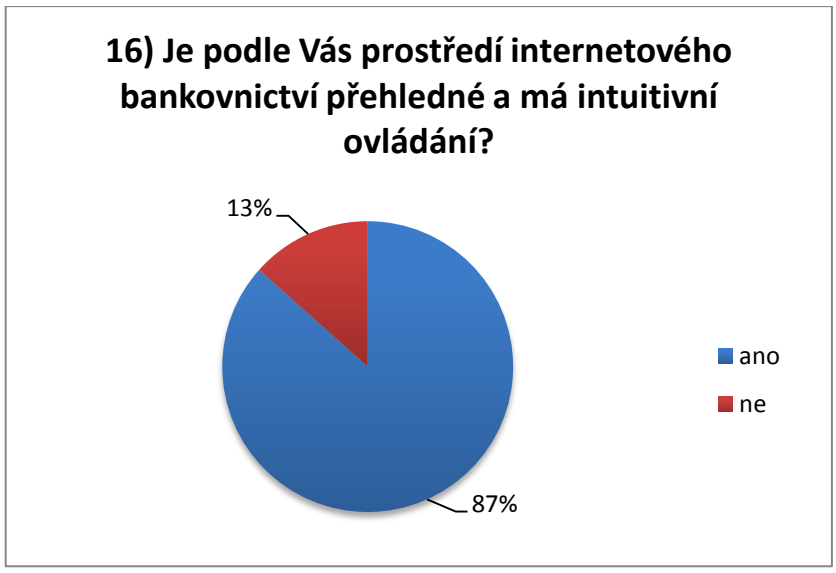
Z odpovědí vyplývá, že 247 respondentů (95%) je spokojeno s funkčností a spolehlivostí internetového bankovnictví. To si nemyslí zbylých 12 respondentů.




*Obr. 21 Otázka č. 15 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 16**: Je podle Vás prostředí internetového bankovnictví přehledné a má intuitivní ovládání?

S přehledností a ovládáním prostředí internetového bankovnictví je spokojeno 226 dotázaných (87%), 35 dotázaných není.




*Obr. 22 Otázka č. 16 dotazníkového šetření (vlastní zpracování)*

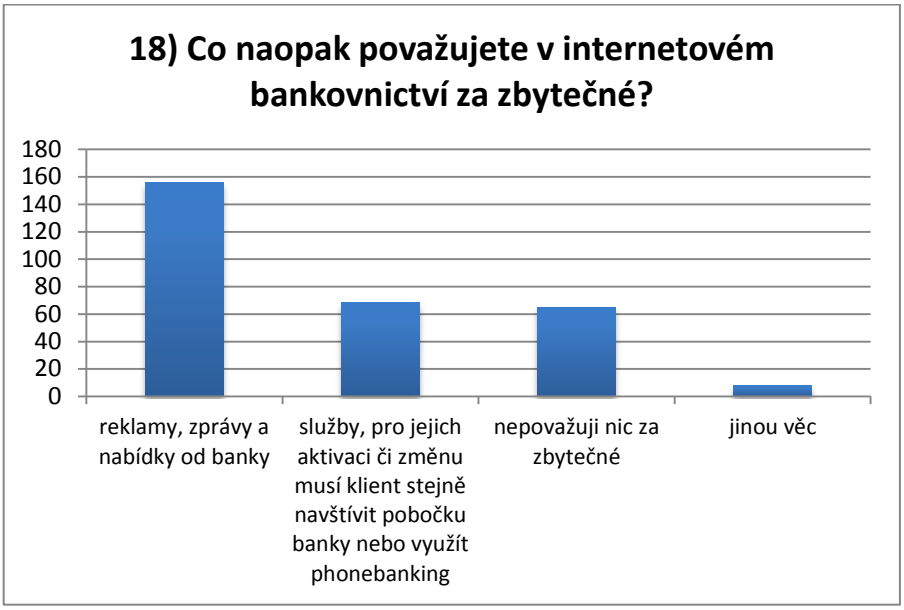
**Otázka č. 17**: Jaké služby internetového bankovnictví využíváte nejčastěji?

Odpovědi na otázku č. 17 ukázaly, že respondenti nejvíce využívají jednorázový příkaz k úhradě a zjištění zůstatku na účtu. Méně využívané služby byly zobrazení elektronického výpisu z účtu a trvalý příkaz k úhradě.


*Obr. 23 Otázka č. 17 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 18**: Co naopak považujete v internetovém bankovnictví za zbytečné?

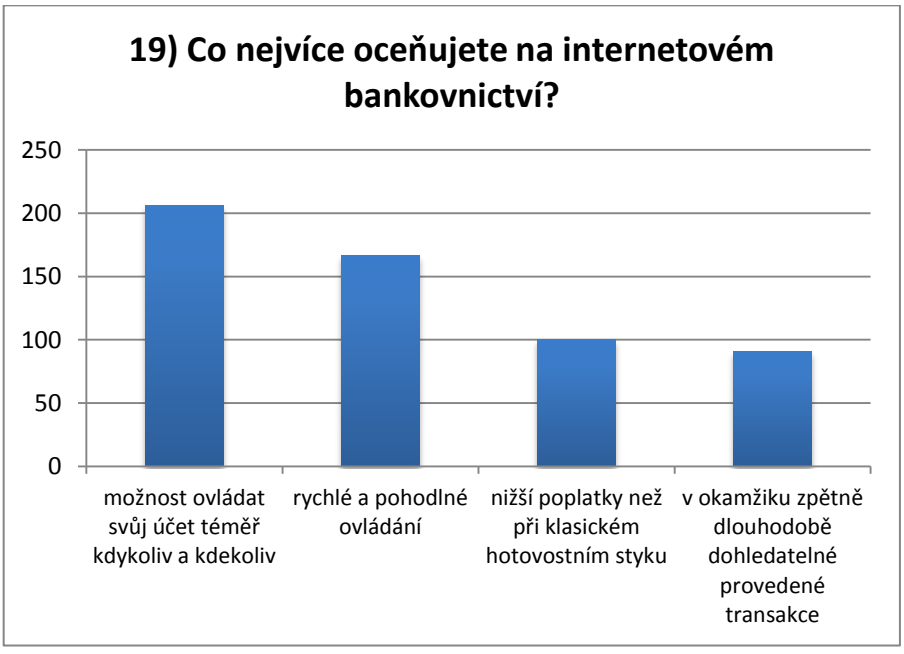
Reklamy, zprávy a nabídky z banky považuje za zbytečné 156 dotázaných. Služby, pro jejich aktivaci či změnu musí klient stejně navštívit pobočku banky nebo využít phonebanking, považuje za zbytečné 68 respondentů. Jako příklad lze zmínit případ autora této práce, kdy při blokaci ztracené platební karty musel ještě využít služby telefonního bankovnictví pro blokaci a vystavení náhradní platební karty, přestože v nabídce internetového bankovnictví byla možnost nechat kartu zablokovat a tudíž zbytečná. Operátor telefonního bankovnictví sdělil, že přes internetové bankovnictví se platební karta zablokovat takto nedá. 65 respondentů nepovažuje v nabídce internetového bankovnictví za zbytečné nic.




*Obr. 24 Otázka č. 18 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 19**: Co nejvíce oceňujete na internetovém bankovnictví?

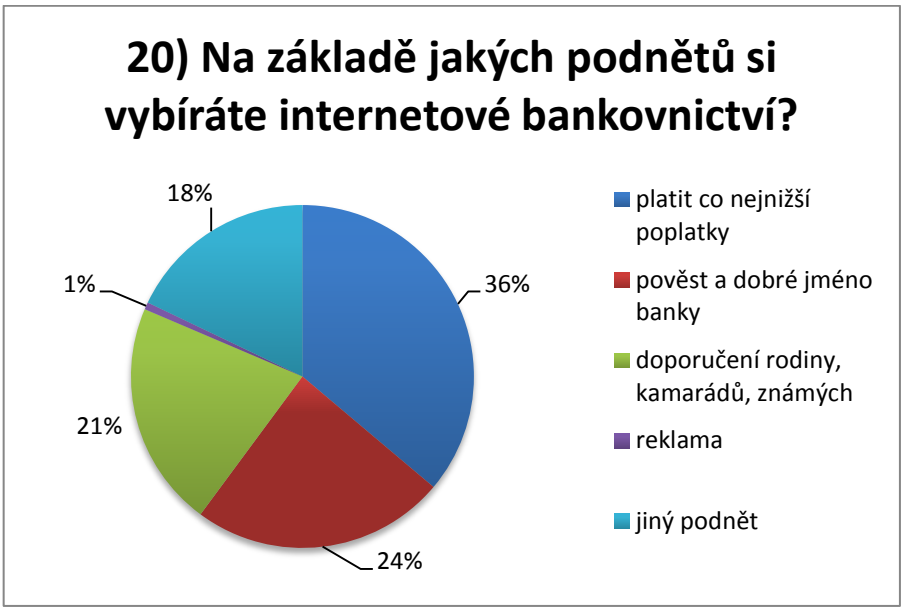
Možnost ovládat svůj účet téměř kdykoliv a kdekoliv na internetovém bankovnictví oceňuje 206, rychlé a pohodlné ovládání 167, nižší poplatky než při hotovostním styku 100 a dohledatelné provedené transakce 91 respondentů. I tato otázka měla možnost volby více odpovědí.




*Obr. 25 Otázka č. 19 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 20**: Na základě jakých podnětů si vybíráte internetové bankovnictví?

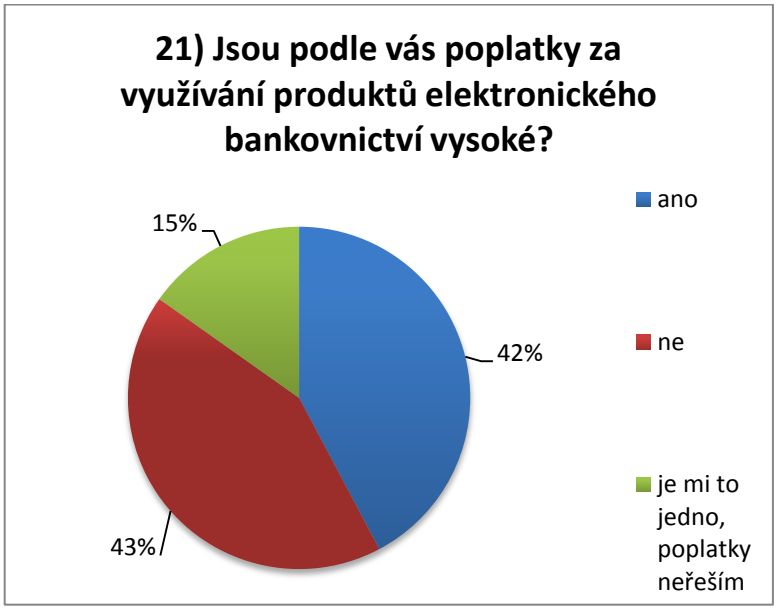
Na základě co nejnižších poplatků si internetové bankovnictví vybírá 107 dotázaných (36%), pověst a dobré jméno banky mělo vliv na výběr u 71 dotázaných (24%) a doporučení rodiny, kamarádů a známých mělo váhu u 63 dotázaných (21%). Naproti tomu reklama nemá na dotázané skoro žádný vliv (1%). Odpovědi respondentů, kteří si vybírají internetové bankovnictví na základě jiného podnětu, byly nejčastější, že si internetové bankovnictví přímo nevybírají, ale podřídí se nabídce banky, u které mají zřízený běžný účet.




*Obr. 26 Otázka č. 20 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 21**: Jsou podle vás poplatky za využívání produktů elektronického bankovnictví vysoké?

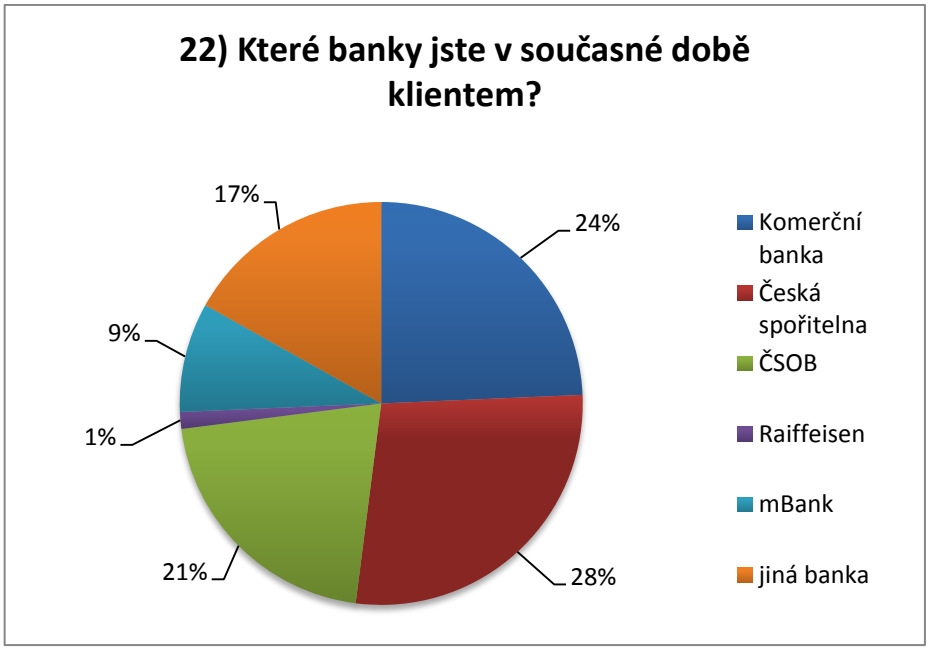
Z hlediska úrovně poplatků za poskytované služby jsou názory respondentů téměř vyrovnané. Za vysoké je považuje 125 respondentů (42%), 126 respondentů (43%) si to nemyslí a 45 (15%) respondentům je to jedno.




*Obr. 27 Otázka č. 21 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 22**: Které banky jste v současné době klientem?

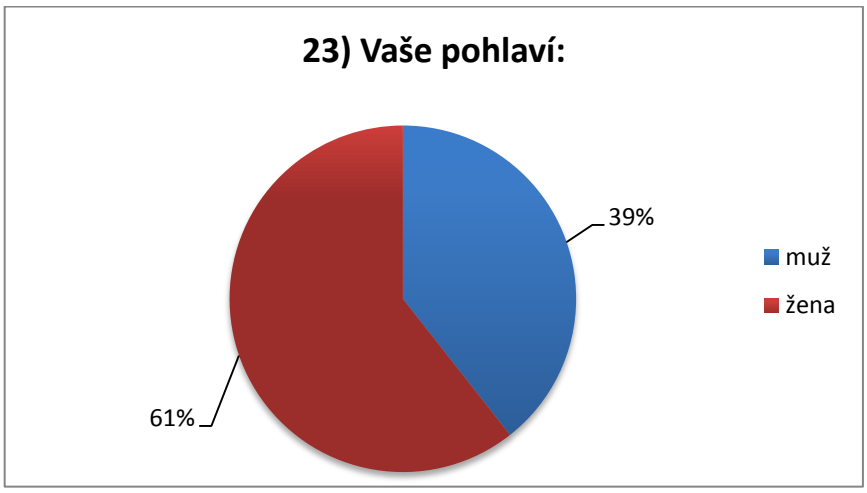
Tento dotazník vyplňovali klienti různých bank, největší počet zaujímali klienti České spořitelny (82 dotázaných) a Komerční banky (72 dotázaných).




*Obr. 28 Otázka č. 22 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 23**: Vaše pohlaví:

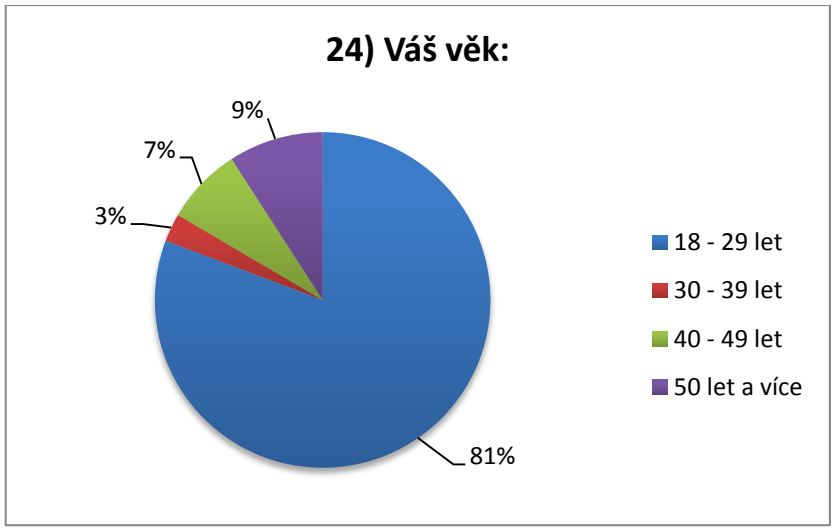
V dotazníku převažovaly ženy (180 respondentů) nad muži (116 respondentů).




*Obr. 29 Otázka č. 23 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 24**: Váš věk:

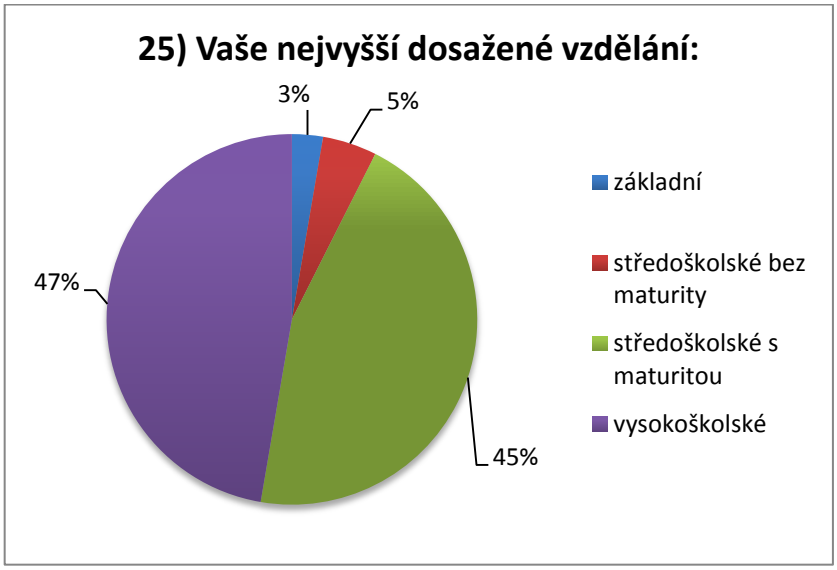
V kolonce věk uvedlo 239 dotazovaných věk 18-29 let, 57 dotazovaných je starší než 29 let, z toho 8 dotazovaných ve věku 30 až 39 let, 22 dotazovaných ve věku 40- 49 let a 27 dotazovaných má nad 50 let.




*Obr. 30 Otázka č. 24 dotazníkového šetření (vlastní zpracování)*

**Otázka č. 25**: Vaše nejvyšší dosažené vzdělání:

U respondentů převažovalo vysokoškolské vzdělání, a to v 140 případech. Středoškolské vzdělání s maturitou jako nejvyšší dokončené vzdělání uvedlo 134 respondentů, bez maturity 14 respondentů a 8 respondentů uvedlo základní vzdělání.




*Obr. 31 Otázka č. 25 dotazníkového šetření (vlastní zpracování)*

## 4.3 Vyhodnocení hypotéz

**H1** – Podle výpočtů kombinovaných z dat otázky č. 1 a otázky č. 24 využívá alespoň nějaký produkt elektronického bankovnictví 92,89% respondentů starších 18 let a zároveň mladších než 30 let. Hypotézu tedy přijímáme.

**H2** – Podle výpočtů kombinovaných z dat otázky č. 8 a otázky č. 25 by 38,35% respondentů s nižším než vysokoškolským vzděláním při přihlašování do internetového bankovnictví nevyužilo biometrické informace. Hypotézu tedy zamítáme.

**H3** – Podle výpočtů kombinovaných z dat otázky č. 12 a otázky č. 24 vyplývá, že 30,43% respondentů starších 29 let nepovažuje internetové bankovnictví za bezpečné. Hypotézu tedy zamítáme.

**H4** – Výpočty kombinované z dat otázky č. 15 a otázky č 23 ukázaly, že 95,52% dotázaných je spokojeno s funkčností a spolehlivostí internetového bankovnictví Komerční banky, 100% dotázaných je spokojeno s funkčností a spolehlivostí internetového bankovnictví České spořitelny, 91,07% dotázaných s funkčností a spolehlivostí internetového bankovnictví ČSOB a 100% dotázaných je spokojeno s funkčností a spolehlivostí internetového bankovnictví mBank. Hypotézu tedy přijímáme.

**H5** – Výpočty kombinované z dat otázky č. 21 a otázky č 22 ukázaly, že 47,22% klientů Komerční banky je nespokojeno s poplatky za produkty elektronického bankovnictví. Hypotézu tedy přijímáme.

# 5 ANALÝZA VYBRANÝCH PRODUKTŮ ELEKTRONICKÉHO BANKOVNICTVÍ

Tato kapitola je zaměřena na analýzu a následné doporučení vhodného produktu elektronického bankovnictví pro retailového klienta. Při hodnocení produktů budu také vycházet z výsledků dotazníkového šetření v předešlé kapitole, kde klienti ve většině případů uvedli, že hlavní vliv na rozhodování při výběru internetového bankovnictví mají co nejnižší poplatky za dané služby. Analýza bude tedy provedena z hlediska poplatků za využívání daných produktů. Banky, ve kterých budou produkty srovnávány, jsou následující: Česká spořitelna, ČSOB, Komerční banka, GE Money Bank a mBank.

## 5.1 Srovnání vybraných produktů

### 5.1.1 Platební karty

*Tab. 1 Srovnání poplatků za používání platebních karet pro občany (vlastní zpracování dle aktuálních sazebníků ČS, ČSOB, KB, GE Money Bank a mBank)*

| Operace | Název banky | | | | |
|---|---|---|---|---|---|
| | Česká spořitelna | ČSOB | Komerční banka | GE Money Bank | mBank |
| Název karty | Visa Classic | Maestro | Visa | Maestro | Visa |
| Používání karty (ročně) | 400 Kč | 480 Kč | 490 Kč | 468 Kč | zdarma |
| Vydání náhradní karty | 200 Kč | 250 Kč | 200 Kč | 150 Kč | 100 Kč |
| Dotaz na zůstatek: | | | | | |
| bankomat vlastní banky | zdarma | zdarma | 3 Kč | zdarma | nelze |
| bankomat cizí banky | 20 Kč | 9 Kč | 10 Kč | 10 Kč | zdarma |
| Změna PIN v bankomatu | 6 Kč | zdarma | 50 Kč | zdarma | 25 Kč |
| Platba kartou u obchodníka | zdarma | zdarma | zdarma | zdarma | zdarma |
| Vklad hotovosti | | | | | |
| vkladovým bankomatem | 6 Kč | zdarma | nelze | zdarma | zdarma |
| na přepážce banky | zdarma | zdarma | zdarma | zdarma | zdarma |
| Výběr hotovosti prostřednictvím | | | | | |
| bankomatu vlastní banky | 6 Kč | 6 Kč | 5 Kč | zdarma | Nelze |
| bankomatu cizí banky | 40 Kč | 35 Kč | 35 Kč | 40 Kč | 9 Kč |
| bankomatu v zahraničí | 125 Kč | 80 Kč + 0,5% | 1%, min. 100 Kč | 100 Kč + 0,5 % | 35 Kč |
| služby Cashback | 6 Kč | zdarma | zdarma | zdarma | zdarma |
| služby Cash advance | 40 Kč | 150 Kč + 0,5% | 1,0 %, min. 100 Kč | 1 %, min. 30 Kč | 35 Kč |

Všechny srovnávané banky nabízejí platební karty k založenému běžnému účtu a až na mBank vyžadují za používání karty poplatek, který je účtován měsíčně a strháván

z běžného účtu klienta. Ztráta nebo zcizení karty nevyjdou pro klienta levně, je účtován poplatek za vydání nové karty v rozmezí 100 – 250 Kč. Dotaz na zůstatek účtu ve vlastním bankomatu je ve většině bank zdarma, až na Komerční banku a mBank, která vlastní bankomaty neprovozuje, ale kompenzuje tento nedostatek svým klientům tak, že nezpoplatňuje dotaz na zůstatek v cizích bankomatech. Hlavní účel platební karty a to platba kartou u obchodníka je u všech bank zdarma. Taktéž vklady hotovostí prostřednictvím vkladového bankomatu a na přepážce banky jsou zdarma, až na výjimku v podobě České spořitelny, která si účtuje 6 Kč za vklad prostřednictvím vkladového bankomatu a Komerční banku, která vkladové bankomaty nenabízí.

Výběry v hotovosti ve vlastním bankomatu jsou zpoplatněny malými částkami v rozmezí v hodnotách 5 Kč a 6 Kč, v případě GE Money Bank jsou zdarma. To už neplatí u výběru hotovosti z cizích bankomatů, kde si banky účtují poplatky okolo 40 Kč. Světlá výjimka je opět mBank, která nabízí 3 výběry měsíčně zdarma, poté za 35 Kč, pokud klient splní podmínku, že za měsíc u obchodníků zaplatí za zboží v hodnotě větší než 4000 Kč.

Výběr hotovosti v zahraničí je zatížen vysokým poplatkem, který se u 3 bank skládá z fixního poplatku plus procent z objemu vybírané částky. Pokud má klient možnost, měl by využít služby Cashback a vybrat si tak hotovost u obchodníka, u kterého platil kartou a ušetřit si tak případný poplatek za použití bankomatu. Kromě České spořitelny všechny banky nabízejí tuto službu zdarma. Cash advance, tedy výběr hotovosti na pobočce banky nebo ve směnárně zatěžují banky vysokým poplatkem.

### 5.1.2 Platební karty – student

*Tab. 2 Srovnání poplatků za používání platebních karet pro studenty (vlastní zpracování dle aktuálních sazebníků ČS, ČSOB, KB a GE Money Bank)*

| Operace | Název banky | | | |
|---|---|---|---|---|
| | Česká spořitelna | ČSOB | Komerční banka | GE Money Bank |
| Název karty | Visa Classic | MasterCard Standard | Maestro | VISA Classic |
| Používání karty (ročně) | zdarma | zdarma | zdarma | zdarma |
| Vydaní náhradní karty | 200 Kč | 250 Kč | 200 Kč | 150 Kč |
| Dotaz na zůstatek | | | | |
| bankomat vlastní banky | zdarma | zdarma | 2,50 Kč | zdarma |
| bankomat cizí banky | 20 Kč | 9 Kč | 10 Kč | 10 Kč |
| Změna PIN | 6 Kč | zdarma | 50 Kč | 49 Kč |
| Platba kartou u obchodníka | zdarma | zdarma | zdarma | zdarma |

| | | | | |
|---|---|---|---|---|
| Vklad hotovosti | | | | |
| vkladovým bankomatem | 6 Kč | zdarma | nelze | zdarma |
| na přepážce banky | zdarma | zdarma | zdarma | zdarma |
| Výběr hotovosti prostřednictvím | | | | |
| bankomatu vlastní banky | zdarma | zdarma | zdarma | zdarma |
| bankomatu cizí banky | 40 Kč | 35 Kč | 35 Kč | 40 Kč |
| bankomatu v zahraničí | 125 Kč | 80 Kč+ 0,5 % | 1 výběr zdarma | 0,5 % + 100 Kč |
| služby Cashback | 6 Kč | zdarma | zdarma | zdarma |
| služby Cash advance | 40 Kč | 150 Kč + 0,5 % | 1,0 %, min. 100 Kč | 1,0 %, min. 30 Kč |

Platební karty nabízené ke studentským účtům mají stejná specifika jako karty k běžným účtům, mBank speciální studentský účet nenabízí. Avšak banky nabízejí studentům vedení karty a výběry z vlastního bankomatu zdarma, Komerční banka navíc jeden výběr ze zahraničí zdarma, za druhý a další výběr účtuje poplatek 1% z vybírané částky, minimálně 100 Kč. Všechny ostatní poplatky zůstávají v nezměněné výši.

### 5.1.3 Kreditní karty

*Tab. 3 Srovnání poplatků za používání kreditních karet (vlastní zpracování dle aktuálních sazebníků ČS, ČSOB, KB, GE Money Bank a mBank)*

| Operace | Název banky | | | | |
|---|---|---|---|---|---|
| | Česká spořitelna | ČSOB | Komerční banka | GE Money Bank | mBank |
| Název karty | Chytrá karta ČS | ČSOB Kreditní karta | A karta | MoneyCard | mKreditka |
| Výše úvěrového limitu | 5000 – 500000 Kč | až 250000 Kč | 10000 – 250000 Kč | až 150000 Kč | až 150000 Kč |
| Výše úrokové sazby (p.a.) | 19,08% | 19,90% | 19,90% | 25,08% | 23,80% |
| Bezúročné období (dny) | 55 | 55 | 45 | 50 | 54 |
| Minimální povinná měsíční splátka | 3,20% | 5 %, min 500 Kč | 5% + úrok | 2% | 3%, min 50 Kč |
| Zasílání měsíčního výpisu z účtu | zdarma | zdarma | Zdarma | zdarma | zdarma |
| Vydání karty | 199 Kč | zdarma | Zdarma | zdarma | zdarma |
| Dotaz na zůstatek: | | | | | |
| bankomat vlastní banky | zdarma | zdarma | 3 Kč | 10 Kč | nelze |
| bankomat cizí banky | 20 Kč | 9 Kč | 10 Kč | 10 Kč | 10 Kč |
| Změna PIN | 6 Kč | zdarma | 50 Kč | 49 Kč | 25 Kč |
| Bezhotovostní příkazu skrz: | | | | | |
| internetové bankovnictví | 2 Kč | nelze | 1% | 1% | 1,5 % min. 30 Kč |
| bankomat | 6 Kč | 30 Kč + 1,5% | 1% | 1% | nelze |
| přepážku banky | 15 Kč | 30 Kč + 1,5% | 1% | 1% | nelze |
| Výběr hotovosti prostřednictvím: | | | | | |
| bankomatu vlastní banky | 6 Kč | 6 Kč + 1,5 % | 1 %, min. 30 Kč | 39 Kč | nelze |

| | | | | | |
|---|---|---|---|---|---|
| bankomatu cizí banky | 40 Kč | 35 Kč + 1,5 % | 1 %, min. 100 Kč | 89 Kč | 49 Kč |
| bankomatu v zahraničí | 125 Kč | 80 Kč + 1,5 % | 1 %, min. 100 Kč | 1 % + 100 Kč | 49 Kč |
| služby Cashback | 6 Kč | zdarma | zdarma | 15 Kč | zdarma |
| služby Cash advance | 65 Kč | 150 Kč + 1,5 % | 1,0 %, min. 100 Kč | 100 Kč + 1,5 % | 99 Kč |
| Platba kartou u obchodníka | zdarma | zdarma | zdarma | zdarma | zdarma |

Kreditní karty fungující na bázi revolvingového úvěru nabízí všechny vybrané banky. Hlavním odlišujícím se znakem je výše úvěrového limitu, který je možno sjednat v případě České spořitelny až do výše 500 000 Kč. Úvěr je úročen rozdílnou úrokovou sazbou, která se pohybuje v rozmezí 19% až 23% p.a.. Pokud klient splatí svůj závazek během bezúročného období, neplatí z poskytnutého úvěru žádné úroky.

Kreditní karta by hlavně měla být využívána k placení u obchodníků, které je zdarma, ostatní služby jsou zpoplatněny vysokými poplatky, několikanásobně většími než u debetních karet. Bezhotovostní příkazy se s ní nevyplatí zadávat a výběry ať už z vlastního, cizího nebo bankomatu v zahraničí jsou ohodnoceny vysokým poplatkem. Služba Cashback je v případě GE Money Bank zpoplatněna 15 Kč, v případě České spořitelny 6 Kč, u ostatních bank zdarma.

Jako nejvýhodnější ze srovnání vychází Chytrá karta České spořitelny, která nabízí nejvýhodnější úrokovou sazbu 19,08% a přitom nejdelší bezúročné období 55 dnů.

### 5.1.4 Internetové bankovnictví

*Tab. 4 Srovnání poplatků za používání internetového bankovnictví pro občany (vlastní zpracování dle aktuálních sazebníků ČS, ČSOB, KB, GE Money Bank a mBank)*

| Operace | Název banky | | | | |
|---|---|---|---|---|---|
| | Česká spořitelna | ČSOB | Komerční banka | GE Money Bank | mBank |
| Název služby | SERVIS 24 | InternetBanking 24 | MojeBanka | Internet Banka | mKonto |
| Zřízení služby | zdarma | zdarma | Zdarma | zdarma | zdarma |
| Měsíční poplatek | 100 Kč | 40 Kč | 39 Kč | 49 Kč | zdarma |
| Příchozí platby | 5 Kč | 6 Kč | 5 Kč | 5 Kč | zdarma |
| Odchozí platby | 2 Kč | 3 Kč | 4 Kč | 6 Kč | zdarma |
| Inkaso a platby SIPO: | | | | | |
| Zřízení | zdarma | zdarma | Zdarma | zdarma | zdarma |
| Zrušení | zdarma | zdarma | Zdarma | zdarma | zdarma |
| Realizace inkasa | 5 Kč | 6 Kč | 6 Kč | 6 Kč | zdarma |
| Zaslání přihlašovací SMS zprávy | 2 Kč | zdarma | Zdarma | zdarma | zdarma |

| | | | | | |
|---|---|---|---|---|---|
| Zaslání autorizační SMS zprávy | zdarma | zdarma | zdarma | zdarma | zdarma |
| Zaslání potvrzovací SMS zprávy | zdarma | 2 Kč | zdarma | zdarma | zdarma |
| Zaslání potvrzení transakce e-mailem | zdarma | zdarma | zdarma | zdarma | zdarma |
| Zasílání měsíčního výpisu z účtu e-mailem | zdarma | zdarma | zdarma | zdarma | zdarma |
| Zasílání měsíčního výpisu z účtu poštou | 5 Kč + poštovné | 20 Kč | 20 Kč | 15 Kč | 30 Kč |

Zřízení služby internetového bankovnictví nabízí všechny banky zdarma. Česká spořitelna účtuje pro běžné účty měsíční poplatek 100 Kč, pro sporožirové účty 25 Kč. ČSOB vede internetové bankovnictví za 40 Kč, Komerční banka 39 Kč a GE Money Bank 49 Kč.

Odchozí platby prostřednictvím internetového bankovnictví jsou obecně levnější než příchozí platby. Zřízení a zrušení inkasa a SIPO plateb banky nabízejí zdarma, realizace jednotlivých plateb potom v případě České spořitelny za 5 Kč, v případě ostatních bank za 6 Kč. Zasílání přihlašovacích, autorizačních a potvrzovacích SMS zpráv na klientův mobilní telefon je s výjimkou ČSOB (2 Kč za potvrzovací SMS) u ostatních bank zdarma.

Pro banky a pro klienta je přijatelnější zasílat měsíční výpis z účtu elektronickou cestou, tzn. na klientův e-mail. V tomto případě klient neplatí nic, v případě zaslání si většinou účtují poplatek, který pokryje jejich náklady na tisk výpisu a poštovné.

V tomto textu o poplatcích za internetové bankovnictví zatím nepadla žádná zmínka o mBank, která jako jediná ze srovnávaných bank má veškeré operace prováděné přes internetové bankovnictví zdarma, kromě zasílání měsíčního výpisu z účtu poštou.

### 5.1.5 Internetové bankovnictví – student

*Tab. 5 Srovnání poplatků za používání internetového bankovnictví pro studenty (vlastní zpracování dle aktuálních sazebníků ČS, ČSOB, KB a GE Money Bank)*

| Operace | Název banky | | | |
|---|---|---|---|---|
| | Česká spořitelna | ČSOB | Komerční banka | GE Money Bank |
| Název služby | SERVIS 24 | InternetBanking 24 | MojeBanka | Internet Banka |
| Zřízení služby | zdarma | zdarma | zdarma | zdarma |
| Měsíční poplatek | zdarma | zdarma | zdarma | zdarma |

| | | | | |
|---|---|---|---|---|
| Příchozí platby | 5 Kč | zdarma | zdarma | zdarma |
| Odchozí platby | 2 Kč | zdarma | 6 Kč | 6 Kč |
| Inkaso a platby SIPO: | | | | |
| Zřízení | zdarma | zdarma | zdarma | zdarma |
| Zrušení | zdarma | zdarma | zdarma | zdarma |
| Realizace inkasa | 5 Kč | 6 Kč | 6 Kč | 6 Kč |
| Zaslání přihlašovací SMS zprávy | 2 Kč | zdarma | zdarma | zdarma |
| Zaslání autorizační SMS zprávy | zdarma | zdarma | zdarma | zdarma |
| Zaslání potvrzovací SMS zprávy | zdarma | zdarma | zdarma | zdarma |
| Zaslání potvrzení transakce e-mailem | zdarma | 1 Kč | zdarma | zdarma |
| Zasílání měsíčního výpisu z účtu e-mailem | zdarma | zdarma | zdarma | zdarma |
| Zasílání měsíčního výpisu z účtu poštou | 5 Kč + poštovné | 20 Kč | 20 Kč | 15 Kč |

Oproti běžným účtům nabízejí banky v rámci internetového bankovnictví pro studenty výhody, které hlavně spočívají v absenci měsíčního poplatku za využívání služby. Také příchozí platby jsou zdarma, s výjimkou České spořitelny. Odchozí platby účtuje GE Money Bank a Komerční banka sazbou 6 Kč, Česká spořitelna sazbou 2 Kč, ČSOB má odchozí platby zdarma. V porovnání s běžnou nabídkou bank zůstává realizace inkasních a SIPO plateb u studentské nabídky nezměněna jako i příchozí SMS zprávy na klientův mobilní telefon a zasílání měsíčního výpisu z účtu.

## 5.2 Doporučení pro jednotlivé typy retailových klientů

- **Občan**

V rámci nabídky produktů elektronického bankovnictví pro občany bych doporučoval využít služeb mBank. Pokud by klient aktivně využíval platební kartou k platbám u obchodníků v měsíčním objemu více než 4000 Kč, měl by poté 3 výběry z bankomatu zdarma.

Pokud by klient měl zájem využívat kreditní kartu, poté bych doporučovat využívat kartu pouze k platbám u obchodníků a na Internetu. Je nevýhodné využívat kreditní kartu k výběrům z bankomatu a k bezhotovostním příkazům. V každém případě by se měl klient snažit splatit své závazky během bezúročného období, které v tomto případě činí 54 dní.

Internetové bankovnictví má mBank prakticky bez poplatků a nemá v rámci tohoto srovnání v žádné jiné bance z hlediska poplatků konkurenci.

- **Student**

V rámci nabídky produktů elektronického bankovnictví pro studenty bych doporučil využít nabídky ČSOB. ČSOB nabízí studentům vedení platební karty typu MasterCard Standard zdarma. Prostřednictvím této platební karty může student vložit hotovost na pokladně i přes vkladový bankomat. Platba v obchodě včetně služby Cash back je také zdarma. Studenty také jistě potěší možnost zdarma si změnit přístupový PIN kód ke kartě v bankomatu. Pokud si bude student pečlivě vybírat bankomaty ČSOB a nebude vybírat hotovost z bankomatů ostatních bank, pak bude mít výběry zdarma.

Také internetové bankovnictví ČSOB s názvem ČSOB Internetbanking 24 nebude pro studenta z hlediska poplatků žádná nadměrná zátěž. Měsíční poplatek, příchozí i odchozí platby bude mít zdarma. Jediný poplatek se týká realizace plateb inkasa a SIPO plateb, kterých ale studenti nemívají moc.

# ZÁVĚR

Cílem této bakalářské práce bylo doporučit vhodnou nabídku elektronického bankovnictví pro jednotlivé typy retailového klienta. Nejprve bylo v praktické části provedeno dotazníkové šetření ohledně spokojenosti uživateli elektronického bankovnictví mezi klienty bank. Byly zjišťovány názory respondentů, které se týkaly různých aspektů elektronické bankovnictví, největší část byla věnována názorům klientů na internetové bankovnictví. Dá se tedy říct, že klienti, kteří využívají internetové bankovnictví, jsou spokojeni s funkčností a spolehlivostí internetového bankovnictví bez ohledu na to, které banky jsou klientem.

Při výběru internetového bankovnictví klienti obvykle kladou důraz platit co nejnižší poplatky a následně tedy byla provedena analýza z hlediska poplatků za vybrané produkty elektronického bankovnictví ve vybraných bankách a to České spořitelně, ČSOB, Komerční bance, GE Money bank a mBank. Nabídku bank pro retailovou klientelu jsem posléze roztřídil na občana a studenta. Z aktuálních sazebníků bank a úrokových lístků jsem zahrnul do tabulek nejdůležitější poplatky za služby spojené s používáním platebních karet, kreditních karet a internetového bankovnictví.

V rámci nabídky produktů elektronického bankovnictví pro občany tedy vyšla nejvhodnější volba mBank. Pokud klient nebude vyžadovat výpis z účtu zasílaný poštou, jistě potom ocení internetové bankovnictví bez poplatků. Pokud bude aktivně využívat platební kartu k platbám u obchodníků, ušetří tím za poplatky spojené s výběrem z bankomatu.

V rámci nabídky produktů elektronického bankovnictví pro studenty byla doporučena nabídka banky ČSOB, která nabízí pro studenty studentský účet ČSOB Studentské konto Plus.

Na závěr lze tedy označit bezhotovostní styk prostřednictvím produktů elektronické bankovnictví za výhodnější než při klasickém hotovostním styku nejen z hlediska poplatků za používání služby. Pro klienta je výhodou také uspořený čas, který může využít jinou činností. Rychlost zadávání a vyřízení transakcí je rychlejší, než například zadávání příkazu k úhradě na přepážce pobočky banky. Nemluvě o nutnosti dopravit se na zadané místo a vynahradit si čas ze svého dne. Produkty elektronického bankovnictví lze tedy doporučit všem klientům bank, kteří chtějí ušetřit svůj čas a zadávat tak své transakce v pohodlí svého domova, na místech, kde mají přístup k Internetu a kde mají signál pro mobilní telefon.

# SEZNAM POUŽITÉ LITERATURY

DVOŘÁK, Petr, 2005. Bankovnictví pro bankéře a klienty. 3. přeprac. a rozšíř. vyd. Praha: Linde, 681 s. ISBN 80-7201-515-X

MÁČE, Miroslav. Platební styk: klasický a elektronický. První vydání. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5

MATYÁŠ, Václav, KRHOVJÁK, Jan. Autorizace elektronických transakcí a autentizace dat i uživatelů. Vyd. 1. Brno: Masarykova univerzita, 2008. 128 s. 1. ISBN 978-80-210-4556-9

POLOUČEK, Stanislav et al. Bankovnictví. 1. vydání. Praha : C. H. Beck, 2006. 716 s. ISBN 80-7179-462-7

## Internetové zdroje

BEZPEČNÝ INTERNET. *Phishing a pharming* [online]. [cit. 2012-05-16]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

CA.CZ. *Jak fungují SSL certifikáty* [online]. [cit. 2012-05-16]. Dostupné z: https://www.ca.cz/jak-to-funguje/

CAMO. *Autentifikace* [online]. [cit. 2012-05-16]. Dostupné z: http://www.camo.cz/descr.php?id=ajc

CLEVERANDSMART. *Autentizace: prognóza vývoje v dalších letech* [online]. [cit. 2012-05-16]. Dostupné z: http://www.cleverandsmart.cz/autentizace-prognoza-vyvoje-v-dalsich-letech/

ČESKÁ REPUBLIKA. Zákon o platebním styku. In: *Zákon č. 124/2002 Sb.* Dostupné z: http://business.center.cz/business/pravo/zakony/platebni_styk/cast3.aspx

ČESKÁ SPOŘITELNA. *Sazebník*. [online]. [cit. 2012-05-16]. Dostupné z: http://www.csas.cz/banka/nav/osobni-finance/sazebnik-d00013266

ČSOB. *Sazebník pro fyzické osoby – občany ve znění k 1. 5. 2012*. [online]. [cit. 2012-05-16]. Dostupné z: http://www.csob.cz/cz/Csob/Sazebniky/Stranky/Sazebnik-pro-fyzicke-osoby-obcany.aspx

ENTRUST. *Identity guard sample* [online]. [cit. 2012-05-16] Obrázek ve formátu GIF. Dostupné z: http://www.entrust.com/images/products/identity-guard-sample.gif

FINANČNÍ VZDĚLÁVÁNÍ. *Používání platebních karet* [online]. [cit. 2012-05-16]. Dostupné z: http://www.financnivzdelavani.cz/webmagazine/page.asp?idk=320

FINANCE.CZ. *Přímé bankovnictví* [online]. [cit. 2012-05-16]. Dostupné z: http://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

GE MONEY BANK. *Sazebník*. [online]. [cit. 2012-05-16]. Dostupné z: http://www.gemoney.cz/ge/cz/1/zakaznicky-servis/sazebniky-poplatku?docid=281

GRUNA, Pavel. *Marketingový výzkum spokojenosti klientů mezi retailovými uživateli elektronického bankovnictví*. [cit. 2012-05-16]Dostupné z: https://docs.google.com/spreadsheet/ccc?key=0Ajxk5oJQtZcFdGliSDEtekEwLUpUR1ZIMkY3b0t2dlE#gid=0

HOAX.CZ. *Co je to phishing* [online]. [cit. 2012-05-16]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

IWOZ.CZ. *GE Money CZ – bankovní aplikace pro iPhone* [online]. [cit. 2012-05-16]. Dostupné z: http://www.iwoz.cz/novinky/ge-money-cz-bankovni-aplikace-pro-iphone/

KOMERČNÍ BANKA. *Sazebník KB pro občany*. [online]. [cit. 2012-05-16]. Dostupné z: http://www.sazebnik-kb.cz/file/cms/cs/sazebniky/kb-sazebnik-1.pdf?20120416073139

MBANK. *Sazebník bankovních poplatků*. [online]. [cit. 2012-05-16]. Dostupné z: http://www.mbank.cz/informace-k-produktum/sazebnik-osobni-finance/

PENÍZE.CZ. *Co dělat, když ztratíte platební kartu* [online]. [cit. 2012-05-16]. Dostupné z: http://www.penize.cz/15748-co-delat-kdyz-ztratite-platebni-kartu

PENIZE.CZ. *Jak funguje kreditní a charge karta* [online]. [cit. 2012-05-16]. Dostupné z: http://www.penize.cz/80266-jak-funguje-kreditni-a-charge-karta

POKERSTARS.COM. *RSA security token* [online]. [cit. 2012-05-16] Obrázek ve formátu JPG. Dostupné z: http://www.pokerstars.com/images/token.jpg

RADOMÍR, Ščurek. *Biometrické metody identifikace osob v bezpečnostní praxi*. 2008. Dostupné z: http://www.vsb.cz/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf. [cit. 2012-05-16]Studijní text. Vysoká škola báňská.

SDRUŽENÍ PRO BANKOVNÍ KARTY. *Souhrnná statistika SBK za rok 2011*. 2011. Dostupné z: http://statistiky.cardzone.cz/download/sbk_statistika_2011.pdf

SHOPCENTRIK. *3D-secure* [online]. [cit. 2012-05-16]. Dostupné z:http://www.shopcentrik.cz/slovnik/3d-secure.aspx

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BPIN Bankovní bezpečnostní kód distribuovaný společně se SIM kartou

BTS Base Transceiver Station - vysílač a přijímač radiových signálů

CVC Card Verification Code - číslo sloužící pro zvýšení zabezpečení držitelů platebních karet

DNA Deoxyribonukleová kyselina - nositelka genetické informace

GPS Global Positioning System - vojenský globální družicový polohový systém

HTTPS Hypertext Transfer Protocol Secure - nadstavba síťového protokolu HTTP, umožňuje zabezpečit spojení

iOS mobilní operační systém vytvořený společností Apple

Kč Česká koruna

p.a. per annum - roční frekvence úročení

PIN personal identification number- osobní identifikační číslo

SIPO Soustředěné inkaso plateb obyvatelstva

SIM Subscriber identity module - identifikační karta sloužící pro identifikaci účastníka v mobilní síti

SMS Short message service - služba krátkých textových zpráv

SSL Secure Sockets Layer – komunikační protokol

TAN Transaction authentication number

WAP Wireless Application Protocol - systém pro zajištění provozu elektronických služeb na mobilních telefonech.

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK