Digitální peníze

Bc. Ladislav Blicha

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ladislav Blicha**
Osobní číslo:	**A14362**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Digitální peníze**
Téma anglicky:	**Digital Money**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury a pramenů, které se vztahují ke zpracovávanému tématu.**
2. **Vymezte fenomenologické a etiologické otázky včetně právního rámce spojené s digitálními penězi a jejich přeměnou na peníze fyzické.**
3. **Analyzujte současný stav zabezpečení a autentizačních metod ve vztahu ke kybernetickým útokům (pomocí botnetů), porovnejte společné specifické znaky a identifikujte rizika.**
4. **Navrhněte organizační schéma a režimová opatření pro zajištění požadovaného stavu.**
5. **Výstupy z praktické části kvalifikační práce aplikujte ve vlastních návrzích a závěrech, získaná data vyhodnoťte a zpracujte do grafů a tabulek.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007. ISBN 978-80-247-1766-1.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.**
3. **KLUFA, František. Elektronické platební prostředky: jak se vyhnout rizikům. Praha: Sdružení českých spotřebitelů, 2013. Průvodce spotřebitele. ISBN 978-80-87719-07-7.**
4. **MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.**
5. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5.**
6. **SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 23. května 2017

…….
podpis diplomanta

ABSTRAKT

Táto diplomová práca sa zameriava na problematiku digitálnych peňazí, elektronického bankovníctva a bezpečnosti. V teoretickej časti sú vymedzené základné pojmy a zhrnutý súčasný stav zabezpečenia i dostupných technológií. Súčasťou je aj pasáž venovaná internetovým útokom a ich analýze. Praktická časť zahŕňa dotazníkový prieskum a návrhy bezpečnostných odporúčaní. V závere diplomovej práce je prognóza ďalšieho vývoja v oblasti zabezpečenia a elektronického bankovníctva.

Klíčová slova: elektronické bankovníctvo, bezpečnosť, internetbanking, smartbanking, autentizácia, autorizácia, internetové útoky

ABSTRACT

This diploma thesis focuses on the issue of digital money, electronic banking and security. The theoretical part defines the basic concepts and summarizes the current state of security and the available technologies. Part of it is the passage dedicated to the internet attacks and their analysis. The practical part includes a questionnaire survey and suggestions for security recommendations. At the end of the diploma thesis is the prognosis of further development in the area of security and electronic banking.

Keywords: electronic banking, security, internetbanking, smartbanking, authentication, authorization, internet attacks

POĎAKOVANIE

Týmto by som chcel poďakovať vedúcemu svojej diplomovej práce PhDr. Mgr. Stanislavovi Zelinkovi za cenné rady, pripomienky a odborné vedenie pri spracovaní tejto diplomovej práce.

Ďalej patrí veľké poďakovanie mojej rodine za ich trpezlivosť a podporu, ktorú vynakladali počas celého štúdia.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

S pojmom peniaze sa každý človek stretáva na dennej báze. Pravidelné aktivity ako nákup v obchode, platenie faktúr a vyúčtovaní alebo cestovné náklady sú neoddeliteľnou súčasťou pravidelného kontaktu s financiami a peniazmi ako takými. Peniaze preto plnia veľmi dôležitú úlohu v procese výmeny tovarov a služieb. Vývoj foriem platobných prostriedkov a konkrétne peňazí viedol k používaniu razených kovových mincí a následne k peniazom papierovým, čiže bankovkám. Zároveň sa vynorila otázka, ako tieto formy peňažného obehu ešte zjednodušiť, urýchliť a taktiež lepšie zabezpečiť. To viedlo k zavedeniu bezhotovostných prevodov a transakcií. Bezhotovostné platobné prostriedky sa s rozvojom platobných systémov a technologického vývoja dostávali čoraz viac do popredia. To malo za následok výrazné zmeny na poli ekonomiky, finančníctva a bankovníctva. Informačná revolúcia a globalizácia vyvíjali čoraz väčší tlak na bankový sektor a poskytované služby. Jednou z foriem bezhotovostných peňazí sa s rozšírením internetu a mobilných služieb stali elektronické peniaze. Konceptom elektronických peňazí sa naštartovala éra digitálnych a virtuálnych platobných metód a prostriedkov, ktoré sa vyskytujú v online sfére. Rozvoj nových informačných a telekomunikačných technológií umožnil významne rozšíriť ponuku produktov i služieb a posunúť komunikáciu medzi bankou a klientom na novú úroveň.

Komunikácia elektronickou cestou má nesporne mnoho výhod, ako je úspora času, nákladov a zároveň pohodlie a komfort zákazníka, ktorý má možnosť vyriešiť všetky svoje požiadavky kedykoľvek a kdekoľvek. Na druhej strane prináša nové bezpečnostné riziko spojené predovšetkým s technickým zabezpečením elektronického bankovníctva. Veľa ľudí berie toto riziko na ľahkú váhu a mnohokrát nedodržujú základné pravidlá a rady pri správe svojho elektronického účtu. Kybernetická kriminalita postihuje vo veľkej miere práve tento sektor, kde sa naivní a dôveryhodní ľudia stávajú ľahkým terčom útokov na ich elektronické peniaze. Bohužiaľ väčšina klientov elektronického bankovníctva nemá povedomie o možných hrozbách a rizikách, s ktorými môžu prísť do styku.

S masovým rozšírením internetového pripojenia a inteligentných komunikačných zariadení sa táto problematika týka širokej verejnosti a aktuálna úroveň informovanosti o potenciálnych útokoch a hrozbách je značne nedostačujúca.

Táto diplomová práca si dáva za cieľ poukázať na aktuálne hrozby, poslúžiť ako preventívne opatrenie v prípade útoku na finančné prostriedky a dostať túto problematiku do širšieho povedomia u bežných ľudí.

Práca pozostáva z dvoch hlavných častí a to teoretickej a praktickej. Teoretická časť podáva ucelený pohľad na súčasný stav v oblasti elektronických peňazí a bankovníctva. Detailne sa zameriava na oblasť zabezpečenia a komunikačných metód. Následne popisuje rôzne typy útokov a hrozieb spojených s digitálnymi peniazmi a ich premenou na peniaze fyzické. Praktická časť práce sa venuje prieskumu o povedomí internetovej bezpečnosti, kde sa snaží identifikovať kritické oblasti a navrhnúť preventívne opatrenia v podobe praktických rád, zásad a pravidiel.

I. TEORETICKÁ ČASŤ

1 ELEKTRONICKÉ BANKOVNÍCTVO

Elektronické bankovníctvo a elektronické peniaze ako dva hlavné pojmy tejto práce, budú postupne rozobrané a popísané z hľadiska vývoja, výhod, nevýhod, typov prístupu, zabezpečenia a rizík, ktoré so sebou prinášajú. Elektronická správa finančných prostriedkov je v dnešnej dobe už úplne bežnou praxou a teší sa veľkej obľúbenosti ako na strane klientov, tak aj na strane jednotlivých finančných inštitúcií.

1.1 Definícia a vývoj

Banky boli od svojho vzniku po dlhý čas obmedzené len na osobný kontakt pri komunikácii s klientmi. Bolo teda potrebné, aby sa klient dostavil na pobočku banky osobne. Tento spôsob komunikácie a spracovania požiadaviek bol veľmi nákladný, či už časovo alebo finančne. Navyše s tým bolo spojené riziko chybovosti pri manuálnom prepise a spracovaní pokynov. Hnacím motorom vývoja boli okrem technologického pokroku predovšetkým dva aspekty – úspora nákladov a obmedzenie vplyvu ľudského faktora. V druhej polovici 20. storočia sa situácia začala výrazne meniť, z dôvodu prudkého technologického vývoja. Finančné inštitúcie začali mať k dispozícií širokú škálu nových komunikačných kanálov.

Za začiatky elektronického bankovníctva je možné považovať vznik platobných kariet, ktorý sa datuje už na začiatok 20. storočia. Ďalšou významnou etapou bolo zahájenie obsluhy klientov prostredníctvom telefónnych liniek. Následný nástup osobných počítačov a mobilných technológií umožnil vznik ďalších typov komunikácie prostredníctvom SMS správ, modemu a predovšetkým internetu. Využitie internetu ako komunikačného média spôsobilo enormný rozmach a rozšírenie tejto služby medzi širokú verejnosť.

Elektronické bankovníctvo, často označované aj ako priame alebo vzdialené, využíva rôzne formy elektronickej komunikácie priamo medzi bankou a jej klientmi. Vo výsledku môže byť klient v kontakte so svojimi peniazmi pomocou kanálov vzdialeného prístupu 24 hodín denne, prakticky odkiaľkoľvek. Pojem elektronického bankovníctva sa neustále vyvíja spolu s možnosťami vzdialeného prístupu a nových trendov v informačnom a komunikačnom sektore. Preto je táto oblasť bankovníctva stále veľmi dynamická a inovatívna.

Medzi charakteristické rysy elektronického bankovníctva sa radia [1]:

- Poskytovanie služieb prebieha prostredníctvom elektronického kanálu.

- Klient s určitým technickým vybavením komunikuje s automatickým informačným systémom banky.
- Klient musí byť jednoznačne identifikovateľný prostredníctvom autentizačného mechanizmu a právo vykonať požadovanú operáciu musí byť overené autorizačným procesom.
- Vyžadujú sa vysoké nároky na bezpečnosť komunikácie a zabezpečenie citlivých údajov.

1.2 Prínosy a riziká

Bankovníctvo je jedna z oblastí, kde sa novinky z technologického sveta prejavujú skoro obratom. Najviac je ovplyvnené práve odvetvie elektronického bankovníctva. S určitosťou je možné konštatovať, že prínosy a výhody značne prevažujú nad nevýhodami a možnými rizikami. Veľmi dôležitým parametrom je bezpečnosť a dôvera pri vzdialenej správe finančných prostriedkov, keďže banky disponujú veľkým množstvom osobných a citlivých údajov.

1.2.1 Prínosy

Elektronické bankovníctvo sa teší vo svete i Českej republike veľkej obľúbenosti. Je to samozrejme spojené s výhodami, ktoré prináša zúčastneným subjektom. Medzi najčastejšie prínosy pre klienta sa radia:

- Úspora času
- Nižšie ceny za služby
- Možnosť prístupu k účtu 24 hodín denne odkiaľkoľvek
- Pohodlie, rýchlosť a komfort
- Diskrétnosť
- Komplexné a nadštandardné služby

Elektronická forma prístupu a spracovania transakcií prináša výhody aj pre banky samotné, ako napríklad:

- Zníženie chybovosti pri spracovaní pokynov a operácií
- Nižšie náklady na prevádzku a ľudské zdroje
- Vyššia efektivita
- Zvýšenie konkurencieschopnosti a podielu na trhu
- Zvýšenie kvality poskytovaných služieb

1.2.2 Riziká

Každá minca má dve strany a rovnako to platí aj v tomto prípade. Nové technológie so sebou prinášajú aj riziká ich zneužitia. Práve obavy o zaistenie dostatočnej úrovne bezpečnosti pri používaní služieb elektronického bankovníctva vzbudzujú nedôveru u určitých skupín obyvateľstva. Banky síce investujú obrovské čiastky do zabezpečenia svojej infraštruktúry a systémov, ale rovnako sofistikované sú aj podvodné útoky kybernetických zločincov.

Z pohľadu klientov prichádzajú do úvahy nasledujúce riziká a nevýhody:

- Nedostatočné zabezpečenie komunikačných kanálov a riziko zneužitia
- Nutnosť disponovať vhodným technickým vybavením a sieťovým pripojením
- Potrebná vedomosť ovládať nové technológie
- Chýbajúci osobný kontakt a prípadná podpora alebo asistencia

Banky nesú zodpovednosť a záväzok voči svojim klientom. Každá negatívna okolnosť môže viesť k odlivu klientov ku konkurencii. V rámci elektronického bankovníctva čelia finančné inštitúcie nasledujúcim negatívnym vplyvom:

- Vyššie vstupné náklady pre vybudovanie služieb elektronického bankovníctva
- Riziko úniku citlivých údajov klientov
- Neustály dohľad a zdokonaľovanie zabezpečenia systémov
- Riziko straty dôvery a reputácie pri závažnom pochybení

1.3 Legislatíva

Činnosť bankového sektora je regulovaná širokou právnou úpravou a legislatívou. Význam elektronického bankovníctva presahuje hranice Českej republiky a preto je ovplyvňovaný celým radom medzinárodných noriem a smerníc. Pre Českú republiku je smerodajná predovšetkým legislatíva Európskej Únie, ktorej je Česká republika členom.

1.3.1 Legislatíva Európskej únie

Po vytvorení jednotného európskeho trhu sa finančné systémy jednotlivých štátov vzájomne prepojili. Bolo preto potrebné v rámci spoločnej integrácie upraviť príslušnú legislatívu peňažných trhov a platobných systémov. Oblasť elektronického bankovníctva určujú predovšetkým nariadenia, smernice a odporúčania vydané orgánmi Európskej únie. Základnou právnou normou je *Smernica Európskeho parlamentu a Rady 2000/46/ES* z 18. septembra 2000 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva. Smernica ukladá povinnosť spätnej výmeny elektronických peňazí držaných vo forme elektronických platobných prostriedkov. Táto smernica bola v roku 2009 nahradená novou *Smernicou Európskeho parlamentu a Rady 2009/110/ES* zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorá výraznejšie mení koncept vydávania elektronických peňazí. S tým súvisí aj prehĺbenie dôvery verejnosti v elektronické platobné systémy a zlepšenie právnej istoty občanov.

Ďalšími právnymi normami, ktoré sa venujú tejto téme sú *Smernica 97/7/ES Európskeho parlamentu a Rady* z 20. mája 1997 o ochrane spotrebiteľa vzhľadom na zmluvy na diaľku a *Smernica Európskeho parlamentu a Rady 2002/65/ES* z 23. septembra 2002 o poskytovaní finančných služieb spotrebiteľom na diaľku, ktorá pozmenila a doplnila staršiu *Smernicu 97/7/ES*.

Mimo vyššie uvedených smerníc je významné aj *odporúčanie č. 97/489/ES* z 30. júla 1997 o transakciách uskutočnených pomocou elektronických platobných nástrojov, ktorého cieľom bolo zvýšiť dôveru voči elektronickým platobným prostriedkom. Odporúčanie na rozdiel od smerníc nie je záväzným právnym aktom.

1.3.2 Legislatíva Českej republiky

Východiskom k téme elektronických peňazí je v českom práve *Zákon č. 21/1992 Sb., o bankách*, ktorý obsahuje vymedzenie termínu elektronické peňažné prostriedky. Tými chápe platobné prostriedky, ktoré uchovávajú svoju hodnotu v elektronickej podobe a sú prijímané okrem svojho vydavateľa aj inými osobami. Obdobne k tejto problematike pristupuje aj *Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech*, ktorý však navyše obsahuje aj definíciu elektronických peňazí a elektronických platobných prostriedkov [2].

Konkrétne zákon definuje dva spôsoby chápania elektronických platobných prostriedkov:

- Prostriedky vzdialeného prístupu k peňažnej hodnote – kde sa spravidla vyžaduje identifikácia držiteľa osobným identifikačným číslom prideleným vydavateľom alebo identifikácia iným spôsobom.
- Elektronické peňažné prostriedky – uchovávajú peňažnú hodnotu v elektronickej podobe. Táto peňažná hodnota sa následne označuje termínom elektronické peniaze.

S účinnosťou od 1.11.2009 bol tento zákon zrušený a nahradený novým *Zákonom č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů*, kde sú elektronické peniaze v §4 definované nasledovne [3]:

(1) Elektronickými penězi je peněžní hodnota, která

a) představuje pohledávku vůči tomu, kdo ji vydal,

b) je uchovávaná elektronicky,

c) je vydávaná proti přijetí peněžních prostředků za účelem provádění platebních transakcí a

d) je přijímána jinými osobami než tím, kdo ji vydal.

Zákon ďalej komplexne upravuje oblasť platobného styku a definuje rôzne práva a povinnosti ako napríklad dodržovanie lehôt pri peňažných prevodoch, zodpovednosť pri zneužití platobnej karty, či pravidlá pri vydávaní elektronických peňazí.

Pomerne novým zákonom, ktorý taktiež spadá do okruhu záujmov tejto diplomovej práce a ktorý sa venuje kriminálnym trestným činnom v kybernetickom priestore, je *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti*. Tento zákon upravuje práva a povinnosti osôb, pôsobnosť a právomoci orgánov verejnej moci v oblasti kybernetickej bezpečnosti. Všeobecne môžeme pod pojmom kybernetická kriminalita chápať páchanie trestnej činnosti, v ktorej sú aktívnou zložkou informačné technológie ako súhrn technického a programového vybavenia vrátane dát. Kybernetickým priestorom sa rozumie virtuálna oblasť, kde spolu komunikujú a pracujú rôzne informačné systémy, počítače a počítačové siete. V kybernetickom priestore prebieha spracovávanie a výmena informácií, digitálne dáta sú prenášané a ukladané v elektronickej podobe.

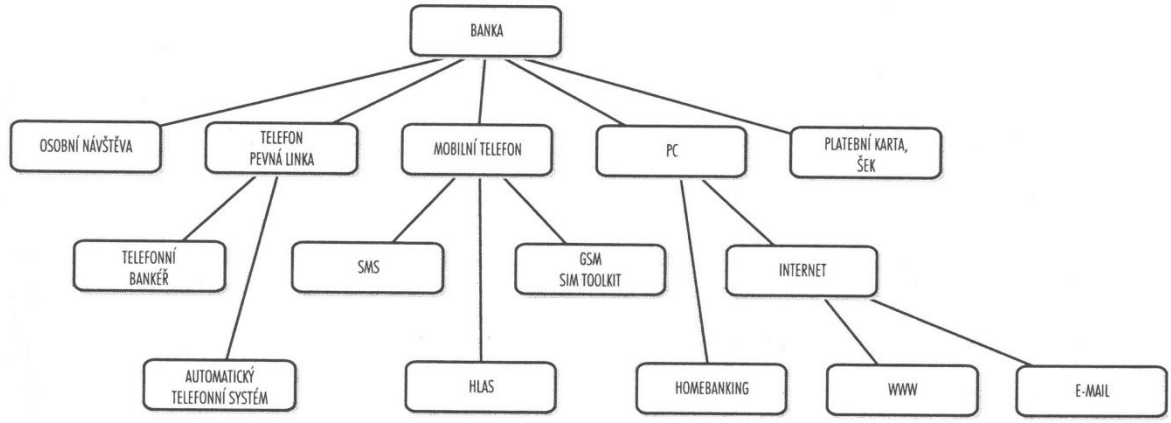
2 SÚČASNÝ STAV A TECHNOLÓGIE

Elektronické bankovníctvo si prešlo od svojho vzniku určitým vývojom. Každá doba priniesla nový nástroj alebo možnosť ako komunikovať s bankou a spravovať svoje financie na diaľku, bez nutnosti návštevy pobočky. V nasledujúcich podkapitolách budú rozobraté aktuálne najviac využívané typy technológií a metódy prístupu.

2.1 Typy a možnosti prístupu

Každý komunikačný kanál medzi klientom a bankou vyžaduje potrebné technické vybavenie a prenosové médium. Veľká väčšina komunikácie prebiehala a prebieha prostredníctvom telefónu (pevná linka, mobil), počítača a internetu.

Dnes je priame bankovníctvo súčasťou ponuky prakticky všetkých bankových inštitúcií. Spôsoby a možnosti vzdialeného prístupu sa menia s dobou a niektoré z nich sú už v dnešnej dobe prežité a nepoužívané.



Obr. 1. Prostriedky vzdialeného prístupu [4]

2.1.1 Zastarané metódy prístupu

Pre úplnosť je správne uviesť dnes už málo používané alebo vôbec nepoužívané metódy prístupu [5].

- **GSM banking** – ide o službu elektronického bankovníctva, ktorá pomocou mobilného telefónu umožňuje klientovi spravovať svoj účet buď prostredníctvom SMS

správ alebo pomocou technológie SIM Toolkit. Služba SIM Toolkit využíva aplikáciu, ktorá je nainštalovaná priamo na SIM karte mobilného operátora. Táto špeciálna aplikácia pridáva do mobilného telefónu nové menu s aktivovanou ponukou služieb. V prípade SMS správ je pre spracovanie požiadaviek potrebné dodržať presne stanovenú formu správy, na ktorú banka obratom zašle požadovanú odpoveď.

- **WAP banking** – vyskytuje sa už veľmi zriedka. Umožňuje spojenie s bankovým účtom prostredníctvom mobilného telefónu vybaveného technológiou WAP (Wireless Application Protocol). Pomocou zjednodušeného prehliadača a autorizačného kľúča je možné zadávať jednoduché príkazy. V dnešnej dobe už WAP nahradili internetové prehliadače, prípadne bankové aplikácie v chytrých telefónoch.
- **PDA banking** – ide o akýsi prienik mobilného a internetového typu prístupu, ku ktorému sa používa vreckový počítač PDA (Personal Digital Assistant). Táto služba nebola veľmi rozšírená a dnes ju už úplne vytlačili mobilné telefóny.

2.1.2 Platobné karty

Platobné karty boli prvým prostriedkom, ktorý umožňoval vzdialený prístup k bankovému účtu elektronickou cestou. V súčasnosti sa vo veľkej miere podieľajú na každodennom platobnom styku. Využívajú sa pri výbere hotovosti z bankomatov, ale primárne na bezhotovostné platenie, či už prostredníctvom platobného terminálu v obchodoch alebo elektronicky na internete. Platobné karty prešli rôznymi vývojovými štádiami až k dnešnej plastovej podobe. Fyzikálne vlastnosti a presne dané rozmery (85,6 x 54,0 x 0,76 mm) sú definované v medzinárodnej norme ISO 3554. Norma taktiež špecifikuje všetky potrebné náležitosti, ktoré má karta obsahovať. Na prednej strane je to meno a logo vydavateľa karty, číslo karty (16 až 19 číslic - identifikujú typ karty, vydavateľa a majiteľa karty), BIN kód (Bank Identification Number), meno držiteľa karty a doba jej platnosti. Na zadnej strane sa nachádza podpisový prúžok a nosič záznamu dát o platobnej karte.

Okrem zmienených náležitostí sa na platobnej karte nachádzajú aj ochranné prvky ako hologram a CVC/CVV kód, ktoré sťažujú jej falšovanie alebo zneužitie. Overovací trojmiestny kód CVC/CVV sa nachádza na zadnej strane karty a zaisťuje tým základné bezpečnostné opatrenie. Tento kód je vyžadovaný u všetkých internetových platieb, kde platobná karta nie je fyzicky prítomná a kde nie je možné autorizovať platbu pomocou PINu.

Platobné karty je možné deliť sa základe rôznych kritérií. Medzi hlavnú klasifikáciu patrí rozdelenie podľa spôsobu zúčtovania transakcií [6]:

- **Debetná karta** – najrozšírenejší typ, viazaná na bankový účet klienta. Umožňuje platby za tovar alebo služby a výber hotovosti do výšky zostatku na účte.
- **Kreditná karta** – umožňuje klientovi čerpať spotrebiteľský úver. Klient využíva na platby peniaze banky do výšky úverového limitu. Zapožičané finančné prostriedky musí v stanovenom termíne splatiť, spravidla za zjednaný úrok, prípadne využiť bezúročné obdobie. Len čo je úver alebo jeho časť splatená, môže ho klient opakovane čerpať – tzv. revolvingový úver.
- **Charge karta** – historicky najstarší typ platobných kariet. Funkcia je veľmi podobná kreditnej karte, avšak nedochádza k čerpaniu úveru, ale odloženiu splatnosti prevedených platieb v stanovenej lehote. Následne banka klientovi vystaví faktúru s výpisom vykonaných transakcií, ktorú klient uhradí v plnej výške. Tento typ kariet je poskytovaný len majetným a overeným klientom.

Ďalším kritériom delenia platobných kariet je spôsob ich prevedenia, kde sa rozlišujú dva druhy [6]:

- **Elektronické** – sú použiteľné iba pre bezhotovostné transakcie, ktoré sú okamžite overené, ako je výber z bankomatu alebo platby v obchodoch s elektronickým platobným terminálom.
- **Embosované** – identifikačné údaje sú na tejto karte vyrazené (embosované) reliéfnym písmom. Dôvodom je možnosť snímať údaje aj u obchodníkov, ktorí nevlastnia online platobný terminál, ale len mechanické zariadenie (tzv. imprinter).

Posledným významným aspektom platobných kariet sú použité technológie pri uchovávaní dát. Medzi tieto technológie patrí [6]:

- **Magnetický prúžok** – je umiestnený na zadnej strane karty a sú na ňom uložené údaje o karte potrebné k vykonaniu platby alebo výberu z bankomatu. Nevýhodou magnetického prúžku je jeho nízky stupeň zabezpečenia proti zneužitiu a taktiež obmedzená kapacita pamäte. Ide o technológiu, ktorá je už zastaraná a vytlačená čipovou technológiou.

- **Elektronický čip** – v čipovej platobnej karte je na prednej strane zabudovaný programovateľný mikroprocesor s pamäťou. Čip umožňuje vyššie zabezpečenie a lokálne overenie identifikačných údajov o držiteľovi karty. Čipové karty sú taktiež oveľa spoľahlivejšie a odolnejšie voči mechanickému poškodeniu.
- **Hybridné karty** – kombinujú obidve technológie dohromady a spojujú ich výhody. Tento typ kariet obsahuje ako magnetický prúžok, tak aj čip pre záznam údajov a komunikáciu s platobnými terminálmi.

Najnovším vzostupným trendom v oblasti platobných kariet je bezkontaktná technológia platieb. Bezkontaktné platenie si našlo za pomerne krátku dobu veľkú obľubu vďaka svojej jednoduchosti, rýchlosti a komfortu. Platba prebehne obyčajným priložením karty k platobnému terminálu za využitia technológie NFC (Near Field Communication). NFC čip zaručuje bezpečnú bezdrôtovú komunikáciu dvoch zariadení na krátku vzdialenosť niekoľkých centimetrov. Do čiastky 500 Kč sa dá kartou bezkontaktne platiť bez ďalšej autorizácie. U vyššej sumy je potrebné štandardne zadať PIN kód pre autorizáciu transakcie. Keď karta zaznamená niekoľko po sebe nasledujúcich bezkontaktných transakcií, je držiteľ karty vyzvaný k vloženiu karty do terminálu a zadaniu PIN kódu, a to bez ohľadu na výšku platby. Tento limit stanovuje banka podľa miery využitia a môže zohľadňovať množstvo, hodnotu alebo náhodný prvok. Toto opatrenie slúži k potvrdeniu, že užívateľ karty je jej právoplatným držiteľom, a tým znižuje možnosť podvodu v prípade ukradnutia alebo straty karty.

Bezpečnosť bezkontaktného platenia je hodne diskutovanou témou, ale z pohľadu zákazníkov výhody používania jednoznačne prevýšili potenciálne riziko zneužitia. V prípade, že dôjde k odcudzeniu platobnej karty a klient túto skutočnosť neodkladne oznámi svojej banke, sú mu ukradnuté prostriedky vrátené na jeho účet.

Obr. 2. Symboly umožňujúce bezkontaktné platby [7]

2.1.3 Phonebanking

Phonebanking alebo telefonické bankovníctvo je po platobných kartách historicky druhým priamym komunikačným kanálom, ktorý sa dočkal hromadného rozšírenia a ktorý je aj v súčasnej dobe stále využívaným produktom vďaka svojej jednoduchosti a technickej nenáročnosti. Pri komunikácii s bankou prostredníctvom telefónneho spojenia je možné rozlíšiť dva typy spracovania pokynov. Pre jednoduchšie, najmä pasívne operácie sa využíva automatický hlasový automat IVR (Interactive Voice Response). V IVR systéme môže klient zadávať pokyny pomocou stlačenia jednotlivých klávesov telefónu na základe ponúkaných možností. Druhou alternatívou je priame prepojenie na operátora call centra, s ktorým je možné riešiť zložitejšie požiadavky alebo prípadné nejasnosti. Najčastejšie využívanou cestou je kombinácia oboch prístupov, kde je najprv komunikácia začatá skrz IVR systém a v prípade potreby dochádza k prepojeniu do call centra na telefónneho bankára. Hlavnou výhodou nasadenia IVR systému je úspora nákladov a možnosť obsluhy viacerých klientov zároveň [4].

2.1.4 Homebanking

Homebanking je forma elektronického bankovníctva, kde komunikácia medzi klientom a bankou prebieha cez počítač a špeciálny software. Software je dodávaný priamo bankou a je nutné ho mať na danom počítači nainštalovaný. Tento typ bankovníctva je cielený primárne na firemnú klientelu, kde je zadávanie platieb a sledovanie pohybov na účte každodenná činnosť. Obrovskou výhodou je prepojenie softwaru priamo s účtovníctvom tej danej firmy, čím je umožnené navzájom importovať a exportovať potrebné dáta [8].

Homebanking sa tešil najväčšej popularite na konci 90. rokov, ale s postupným rozšírením internetbankingu strácal na význame. V súčasnej dobe sa funkcie homebankingu a internetbankingu prelínajú, prípadne čiastočne doplňujú. Homebanking tak ostáva už len doménou firemných zákazníkov.

2.1.5 Internetbanking

Internetbanking alebo internetové bankovníctvo je aktuálne najpoužívanejšou formou elektronického bankovníctva, ktorú využíva celosvetovo široké spektrum populácie. Prenosovým médiom je pri komunikácií s bankou internet. Výhodou oproti homebankingu je ne-

závislosť na špeciálnom software, ktorý plne nahradzuje internetový prehliadač. Internetové bankovníctvo ponúka klientom širokú paletu operácií, možností a úkonov pri správe svojho bankového účtu. Klienti majú neustály prístup k informáciám na svojom bankovom účte v reálnom čase. Potenciál internetového bankovníctva nie je stále využitý na maximum a banky hľadajú nepretržite nové a nové možnosti jeho využitia.

Začiatok internetbankingu v Českej republike siaha do roku 1998, kedy túto formu elektronického bankovníctva začala svojim klientom ponúkať Fio družstevní záložna. K dispozícii boli základné služby, história transakcií a jednoduché prevody. V rovnakom roku zahájila svoju činnosť na poli internetbankingu aj Expandia Bank, ktorá ako prvá ponúkla klientom plnohodnotné internetové bankovníctvo. V roku 2000 ich nasledovala Komerční banka a o dva roky neskôr aj ČSOB a Česká spořitelna. V dnešnej dobe už ponúka internetbanking v určitej forme každá banka v Českej republike [4].

Využitie internetu v bankovníctve otvorilo novú éru komunikácie a vzdialenej správy firemných i osobných financií. Transakcie uskutočnené prostredníctvom internetbankingu sú niekoľkonásobne lacnejšie než transakcie realizované pomocou telefónu alebo priamo na pobočke. Banky samotné motivujú svojich klientov k využívaniu služieb internetového bankovníctva ako jednoduchého a efektívneho komunikačného kanálu. Jediným limitujúcim faktorom je pripojenie k internetu a aspoň základná počítačová gramotnosť.

Najviac diskutovanou témou je stále otázka bezpečnosti pri používaní a potenciálnom zneužití internetového bankovníctva. S rastom počtu užívateľov internetového bankovníctva rastie aj počet kybernetických útokov na účty klientov alebo aj na samotné systémy jednotlivých bánk. Preto banky investujú enormné prostriedky a úsilie do spôsobov ochrany prenášaných dát, citlivých údajov a platobných operácií. Konkrétne typy útokov a využívané spôsoby zabezpečenia budú predstavené a bližšie špecifikované v ďalších kapitolách tejto diplomovej práce.

2.1.6 Smartbanking

Posledným trendom dnešnej doby sa spolu s rozšírením chytrých telefónov (smartphonov) stáva smartbanking. Ide o prístup klienta k svojmu bankovému účtu prostredníctvom mobilnej aplikácie, vytvorenej priamo bankou, ktorú si nainštaloval do svojho chytrého telefónu alebo tabletu. Tieto bankové aplikácie sú dostupné v oficiálnych obchodoch najpou-

živanejších platforiem operačných systémov pre mobilné telefóny. Menovite App Store pre iPhone s iOS od spoločnosti Apple, Google Play pre smartphony s operačným systémom Android a Windows Store pre platformu Windows Phone alebo Windows 10 Mobile. Požiadavky na využívanie aplikácie pre smartbanking sú nastavené každou bankou na inú minimálnu úroveň verzie operačného systému na základe ponúkaných služieb a funkcií. Nutnosťou je samozrejme pripojenie k internetu, či už pomocou wifi siete alebo dátového tarifu. Väčšina bánk vyžaduje z dôvodu bezpečnosti pri prvom použití aktiváciu a spárovanie mobilného telefónu alebo tabletu s internetovým bankovníctvom.

Smartbanking je najmladší komunikačný nástroj elektronického bankovníctva. V Českej republike sa začal objavovať od roku 2011 a ako prvá ho na českom trhu poskytla svojim klientom Fio banka v máji 2011 pre operačný systém iOS a v auguste 2011 pre Android. Ďalšie banky sa postupne pridávali, keďže počet majiteľov chytrých telefónov raketovo rástol a banky v tejto oblasti videli veľký potenciál.

Bankové aplikácie poskytujú vo veľkej miere rovnaký užívateľský komfort pri spravovaní účtu ako internetbanking. Smartbanking neobsahuje všetky dostupné funkcie internetbankingu, ale banky pri pravidelných aktualizáciách svojich aplikácií ponuku funkcií a služieb neustále rozširujú. Výhodou smartbankingu ako zdroju informácií je napríklad prepojenie s GPS pri určovaní polohy najbližšieho bankomatu alebo pobočky. Ďalšou nespornou výhodou je okrem pohodlného a okamžitého prístupu k informáciám aj rýchla možnosť uskutočniť dôležitú platbu, zmeniť limit pre výber alebo platbu kartou, prípadne odcudzenú kartu zablokovať.

2.2 Elektronické peňaženky

Elektronické peňaženky sa rozšírili s nástupom internetu ako akási bezpečnejšia a lacnejšia alternatíva k bežným bankovým účtom a platobným kartám. Sú určené primárne na platenie malých čiastok za rôzne partnerské služby a produkty na internete. Princíp elektronickej peňaženky spočíva v uložení nejakej čiastky (kreditu) na virtuálny účet prostredníctvom bankového prevodu alebo platobnej karty. Tieto prostriedky je následne možné využívať na platby v internetových obchodoch, rôzne prevody a posielanie peňazí ostatným užívateľom systému. Výhodou elektronických peňaženiek je to, že sú bezplatné, transakcie na medzinárodnej úrovni sú lacnejšie ako v bankových inštitúciách a platby prebiehajú

okamžite. Z pohľadu bezpečnosti je u užívateľov vysoko cenená predovšetkým anonymita a nezávislosť na bankovom účte. Pri prípadnom zneužití sa útočník dostane len ku kreditu v elektronickej peňaženke, ktorý spravidla nebýva vysoký. Osobné účty, platobné karty a všetky citlivé informácie ostávajú nedotknuté a chránené.

Medzi najznámejšie a najpoužívanejšie elektronické peňaženky v Čechách sa radia PayPal, Skrill a GoPay [9].

2.2.1 PayPal

PayPal je najznámejší a najpoužívanejší internetový systém, ktorý sprostredkováva bezhotovostné platby po celom svete. V Európe zaisťuje tieto služby dcérska spoločnosť PayPal (Europe) S.à r.l. et Cie, S.C.A. registrovaná v Luxembursku. Užívateľské účty sú identifikovateľné na základe mailovej adresy. PayPal umožňuje vybrať ako primárnu menu českú korunu, ale bohužiaľ stránky tejto služby nie sú plne preložené do českého jazyka, čo môže byť pre niektorých ľudí odradzujúce. Cez PayPal je možné platiť vo veľkom množstve internetových obchodov, ktoré tento typ úhrady podporujú. Umožňuje tiež prijímať a odosielať platby medzi všetkými registrovanými užívateľmi. Tým sa výrazne šetria náklady za vysoké poplatky pri zahraničných transakciách a čas, keďže všetky platby sú prevedené okamžite.

2.2.2 Skrill

Skrill je nový názov pre pôvodné meno medzinárodnej internetovej peňaženky MoneyBookers. Spoločnosť, ktorá prevádzkuje túto službu, je registrovaná v Londýne. Skrill je na rozdiel od PayPalu plne dostupný v českom jazyku a ponúka obdobné služby a funkcie. Využívajú ho aj mnohé české internetové spoločnosti a obchody. Vhodný je predovšetkým pre medzinárodné platby, kde sa dá oproti bankovým prevodom výrazne ušetriť.

2.2.3 GoPay

Spoločnosť GOPAY s.r.o. je prvou nebankovou inštitúciou elektronických peňazí, ktorá je držiteľom licencie od Českej národnej banky. GoPay podlieha plnej regulácii Českej národnej banky a je oprávnená prijímať obchodné platby menom tretích strán. Elektronická

peňaženka GoPay umožňuje platby vo veľkej väčšine internetových obchodov v Českej republike. Ďalej užívateľom ponúka posielanie peňazí v rámci svojej siete, prevody finančných prostriedkov na bankové účty, výbery a vklady. Pre základné využívanie systému nie je potrebné žiadne overenie identity, okrem telefónneho čísla a mailovej adresy. Takýto neoverený účet má finančné a platobné limity. Zvýšením stupňa overenia získa užívateľ vyššie, až bezlimitné možnosti využitia svojho účtu a ďalšie typy platieb.

2.2.4 Predplatené platobné karty

V poslednej dobe sú najviac obľúbenou a využívanou formou elektronických peňaženiek predplatené viacúčelové platobné karty. Takéto karty, ako už názov napovedá, je možné využiť namiesto hotovosti k úhradám menších položiek pre rôzne účely v sieti daných poskytovateľov. Karta nie je viazaná na konkrétny bankový účet a užívateľ si ju nabije len na požadovanú sumu, akú potrebuje. Základnou výhodou je anonymita, keďže na zriadenie predplatenej karty nie je potrebné disponovať bankovým účtom a taktiež deliť sa o osobné údaje. Predplatená karta je vhodná na platby v internetových obchodoch, hlavne u ľudí, ktorí majú obavy zo zneužitia údajov o svojej debetnej alebo kreditnej karte. Využívajú ju aj rodičia v podobe vreckového pre deti a mládež. Karta sa dá použiť aj na ďalšie bežné operácie ako je výber z bankomatu alebo platba za nákup v obchode. Určite nie každému bude tento typ karty vyhovovať, hlavne z dôvodu pomerne vysokých poplatkov spojených s užívaním karty, nastavených platobných limitov a ďalších obmedzení. Z bankových domov ponúkajú tento typ kariet len ČSOB a Česká spořitelna. Do segmentu predplatených kariet sú zapojené aj nebankové subjekty, ktoré môžu klientom priniesť určitú pridanú hodnotu. V súčasnej dobe je možné si vybrať z nasledujúcej ponuky predplatených kariet [10]:

- Blesk peněženka – možnosť dobíjania cez terminály Sazky
- Napka – určená pre mladých ľudí vrátane mobilnej aplikácie
- Biip – predplatená karta vhodná najmä pre deti a mladistvých
- Cool karta – určená iba pre klientov ČSOB a Ery Poštovní spořitelny
- Dobrá karta COOP – dostupná vo vybraných predajniach siete COOP
- FreePay – novinka od spoločnosti Prepaid Solutions
- MyUnicard – vydávaná ČSOB, distribútorom je firma mobile2card a.s.

2.3 Digitálne meny

Protipólom k centralizovaným bankovým systémom sa v posledných rokoch stali digitálne alebo virtuálne meny. Ide o ďalšie štádium vývoja elektronických peňazí, ktoré vznikajú nezávisle na vládach jednotlivých štátov ako meny decentralizovaných platobných systémov. Kľúčovými vlastnosťami sú decentralizácia, transparentnosť a anonymita. Digitálne meny preto nie je možné kontrolovať alebo ovplyvňovať vládou, centrálnymi bankami alebo inými inštitúciami. Decentralizovaná sieť je založená na verejnej distribuovanej databáze, ktorá sa nazýva blockchain a kde sa zaznamenávajú všetky transakcie v platobnom systéme. Nízke transakčné poplatky a rýchlosť prevodu finančných prostriedkov zaujali aj tradičné bankové domy. Ich cieľom je využiť blockchainové technológie v štandardnom centralizovanom bankovom systéme, aby došlo k zefektívneniu prevodov peňazí a zníženiu nákladov pri transakciách.

Spomedzi niekoľkých stoviek existujúcich virtuálnych mien je najznámejšou a najpoužívanejšou menou bitcoin (BTC), ktorá vznikla v začiatkoch histórie digitálnych mien v roku 2009. Medzi ďalšie celosvetovo rozšírené digitálne meny je možné zaradiť napríklad Ripple, Litecoin, Dogecoin alebo Ethereum. Bitcoin patrí konkrétne medzi kryptomeny, ktoré sú postavené na asymetrickej kryptografii pri výpočtoch a potvrdzovaní transakcií. Celkový počet bitcoinov je jednoznačne daný algoritmom na počet 21 miliónov a momentálne je jeden bitcoin deliteľný až na 8 desatinných miest. Vytváranie nových bitcoinov funguje na základe výpočtov zložitých matematických funkcií (ťažby) pomocou výpočtového výkonu všetkých počítačov v distribuovanej sieti. Každý počítač zapojený v sieti zároveň spracováva transakcie pri prevodoch bitcoinov medzi jednotlivými užívateľmi. Bitcoiny môžu byť uložené na počítači vo forme súboru alebo uchovávané pomocou služieb tretích strán. Hodnota bitcoinu sa postupne menila na základe ponuky a dopytu, pričom sa nevyhla ani vysokým výkyvom počas svojho vývoja. V súčasnosti pomerne rýchlo narastá počet subjektov, ktoré sú ochotné prijímať bitcoin ako platidlo za tovar alebo služby [11].

Obr. 3. Vývoj ceny bitcoinu proti USD [12]

Keďže ide o pomerne anonymný prostriedok prevodu peňazí, bez kontroly štátnych orgánov, sú digitálne meny často zneužívané pri platbách na čiernom trhu a na nákup ilegálneho tovaru. Ďalšími kriminálnymi aktivitami môžu byť legalizácia príjmov z trestnej činnosti, obchodovanie s ľuďmi alebo daňové úniky.

Postoj k digitálnym menám je nielen v Českej republike značne komplikovaný. Česká národná banka (ČNB) bitcoin za menu, investičný nástroj alebo peňažnú jednotku nepovažuje. Zo svojej podstaty podľa Českej národnej banky nejde ani o bezhotovostný peňažný prostriedok, či elektronické peniaze. Z toho dôvodu obchodovanie s bitcoinom nevyžaduje povolenie ČNB a nepodlieha jej dohľadu. Obchodovanie s bitcoinom tým pádom nemá žiadnu právnu ochranu alebo garanciu zo strany štátu a príslušnej legislatívy [13].

Bitcoin svojím konceptom predstavuje zaujímavý fenomén vo svete financií. Napriek tomu, že bitcoiny momentálne nepredstavujú vážnejšie riziko pre bežné platobné systémy alebo cenovú stabilitu, budú aj naďalej starostlivo sledované regulačnými orgánmi. V budúcnosti je vysoko pravdepodobné vytvorenie právneho rámca na národnej, európskej alebo medzinárodnej úrovni.

3 ZABEZPEČENIE ELEKTRONICKÉHO BANKOVNÍCTVA

Zabezpečenie elektronického bankovníctva a bezpečnosť uložených finančných prostriedkov sú kľúčovými faktormi pre všetkých užívateľov. Zabezpečenie elektronických platieb je v Českej republike na nadštandardnej úrovni, keďže české banky majú zavedenú širokú škálu bezpečnostných pravidiel. Okrem účinnej identifikácie a autentizácie klientov sa používajú aj zabezpečené komunikačné kanály, monitoring, vyhodnocovanie a predchádzanie rizík [14].

So stále rastúcim počtom užívateľov elektronického bankovníctva sa zvyšuje aj miera kybernetického ohrozenia. Otázka bezpečnosti elektronických platieb je pre finančné inštitúcie a vlády európskych štátov jednou z najdôležitejších. Z pohľadu bezpečnosti je nutné pri elektronickom kontakte vybudovať u klientov dôveru v tento systém. Okrem bezpečnostných pravidiel a sofistikovaných systémov na strane bánk sa otázka kybernetickej bezpečnosti stáva aj neoddeliteľnou súčasťou legislatívy a právnych predpisov.

3.1 Definícia pojmov

Pre prístup do bankového účtu je potrebné zadefinovať dve dôležité operácie, ktoré sa týkajú zabezpečenia elektronického bankovníctva. V prvom rade ide o identifikáciu a autentizáciu klienta a následne o autorizáciu jednotlivých operácií, ku ktorým má klient potrebné oprávnenie. Klient sa po úspešnom procese autentizácie prihlási do svojho bankového účtu, kde môže vykonávať pasívne činnosti ako je prehľad zostatku na účte, história transakcií, zobrazenie rôznych limitov a osobných údajov. Pre realizáciu aktívnych operácií, ako je napríklad zadanie platobného príkazu, je potrebné jednotlivé požiadavky dodatočne autorizovať, čím sa finálne potvrdí ich vykonanie [15].

3.1.1 Autentizácia

Autentizácia užívateľa je proces overenia jeho identity (totožnosti). Užívateľ sa identifikuje určitým, vopred dohodnutým spôsobom (typicky prideleným prihlasovacím menom) a zároveň umožní systému overiť predkladanú identitu. Tento proces odpovedá na otázku: „Je táto osoba skutočne tou, za ktorú sa vydáva?“

Vo všeobecnosti sa metódy autentizácie z princípu delia do troch kategórií podľa toho, čo užívateľ predkladá ako dôkaz svojej totožnosti. Prostriedky overenia sú založené na nasledujúcich spôsoboch [15]:

- znalosť užívateľa (heslo, PIN, ...)
- vlastníctvo predmetu (SIM karta, certifikát, ...)
- charakteristika užívateľa (biometrické údaje, podpis, ...)

Najjednoduchší a najpoužívanejší spôsob autentizácie je pomocou znalosti, čiže niečoho, čo užívateľ pozná alebo si pamätá. Typicky ide o heslo alebo PIN kód. Výhodou je, že ide o jednoduchú, abstraktnú formu overenia. Na druhej strane môže užívateľ svoje prístupové heslo zabudnúť, prípadne môže byť zistené a zneužité i bez jeho vedomia. Druhý spôsob autentizácie je postavený na vlastníctve fyzického predmetu, ktorý poskytuje ďalšiu úroveň overenia totožnosti. K tejto funkcii sa v prípade prístupu do elektronického bankovníctva používa napríklad certifikát, čipová karta alebo určitý typ kalkulátora. Do tejto skupiny fyzických zariadení patrí aj mobilný telefón, na ktorý sú zasielané jednorazové autentizačné kódy vo forme SMS správ. Posledným prostriedkom je overenia užívateľa na základe jeho osobnostnej charakteristiky a biologických údajov. Konkrétne ide primárne o biometrické prvky, ktoré sú nemenné a jedinečné pre každého človeka ako napríklad otlačok prsta, geometria tváre, sietnica a dúhovka oka. Tento typ overenia je v súčasnej dobe na vzostupe, keďže ide o veľmi rýchlu a pohodlnú metódu. Výhodou je taktiež skutočnosť, že sa nedá nič zabudnúť alebo stratiť. Z týchto dôvodov si našiel uplatnenie aj ako autentizačný nástroj pre prístup do počítača a mobilného telefónu.

Pre zvýšenie bezpečnosti a elimináciu nevýhod sa uvedené typy metód vzájomne kombinujú. Pri kombinácii dvoch metód hovoríme o dvojfaktorovej (dvojúrovňovej) autentizácii, v prípade kombinácie všetkých troch metód o trojfaktorovej alebo viacfaktorovej autentizácii. Použitím viacfaktorovej autentizácie sa rapídne zvyšujú nároky na úspešný útok, pretože útočník musí získať prístup k rôznym overovacím kanálom.

3.1.2 Autorizácia

Autorizácia užívateľa obvykle nasleduje po úspešnej autentizácii a spočíva v určení, čo daný užívateľ má alebo nemá právo v systéme vykonať. V elektronickom bankovníctve

prebieha okrem autorizácie klienta predovšetkým proces autorizácie jednotlivých aktívnych operácií.

Autorizácia elektronickej transakcie sa obvykle chápe ako súhlas klienta a zároveň overenie banky, či môže požadovaná transakcia skutočne prebehnúť. V tom je zahrnutá jednak autentizácia/autorizácia užívateľa a autentizácia dát spojených s transakciou, ale napríklad aj kontrola disponibilného zostatku na účte.

Aplikované autorizačné metódy v oblasti elektronického bankovníctva sú v podstate rovnaké ako tie autentizačné. U českých bánk sa najčastejšie používa spôsob autorizácie transakcie pomocou SMS kódu, ktorý príde na mobilný telefón klienta. Každá banka môže mať zvolené odlišné autentizačné a autorizačné metódy, ktoré sú kompatibilné s jej systémom elektronického bankovníctva.

3.2 Zabezpečenie internetbankingu

Internetbanking ako najpoužívanejší prostriedok vzdialenej správy bankového účtu si zasluhuje nadštandardnú mieru zabezpečenia, ktorá dodá klientom dostatočný pocit dôvery v túto službu. Na českom bankovom trhu neexistuje jednotný prístup k zabezpečeniu a ochrane internetového bankovníctva. Avšak implementované bezpečnostné prvky a metódy sa dajú rozdeliť do nasledujúcich oblastí: zabezpečenie prenosu dát a identifikácia banky, autentizácia klienta, autorizácia transakcií.

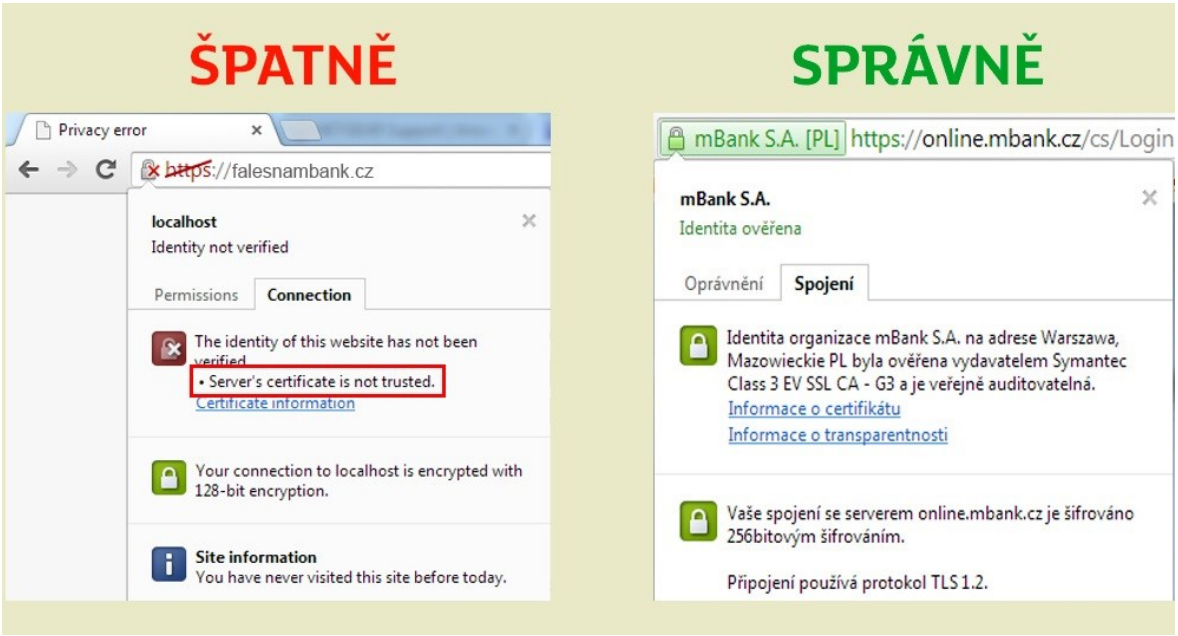
3.2.1 Zabezpečenie prenosu dát a identifikácia banky

Pri internetovom bankovníctve používa klient na komunikáciu so systémom banky webový prehliadač nainštalovaný v počítači. Pomocou prehliadača klient komunikuje so serverom banky, pričom je potrebné zaistiť aj overenie totožnosti banky samotnej. Aby sa predišlo odchyteniu a zneužitiu dôverných údajov, klient so serverom banky nadviaže zabezpečené spojenie. To v prostredí internetu umožňuje protokol HTTPS, ktorý používa dodatočnú šifrovaciu vrstvu poskytovanú kryptografickým protokolom TLS (Transport Layer Security), prípadne jeho predchodcom, protokolom SSL (Secure Socket Layer). Pre úspešné vytvorenie zabezpečeného spojenia je dôležité, aby klient vyžadoval komunikáciu s bankou prostredníctvom protokolu HTTPS, následne, aby sa server banky preukázal oficiálnym

SSL/TLS certifikátom a aby prehliadač klienta overil, že tento certifikát je dôveryhodný a platný. Príslušný certifikát obsahuje identifikačné údaje banky a je vydávaný certifikačnou autoritou, ktorá dokladuje jeho pravosť a dôveryhodnosť [16].

V tomto štádiu hrozí riziko, že útočník buď sleduje komunikáciu klienta s bankou, alebo sa snaží presmerovať klienta na svoju podvodnú stránku, ktorá sa tvári ako stránka banky. Podvrhnutá stránka útočníka bude mať spravidla inú webovú adresu a nebude mať platný certifikát. Záleží už potom len na klientovi, aby si túto okolnosť všimol a okamžite prerušil spojenie. Je doporučené riadiť sa nasledujúcimi zásadami pri prístupe k svojmu bankovému účtu prostredníctvom webového prehliadača.

1. Vždy do internetového bankovníctva pristúpiť cez oficiálne webové stránky banky.
2. Skontrolovať, že adresný riadok začína protokolom https:// nasledovaný správnou adresou internetového bankovníctva.
3. Overiť si zabezpečenie stránky platným certifikátom v podobe visiaceho zámku.



Obr. 4. Rozdiely pri podvrhnutej stránke banky [17]

3.2.2 Autentizácia užívateľa

V súčasnosti banky pre prístup do internetového bankovníctva používajú jednofaktorovú alebo častejšie dvojfaktorovú autentizáciu klienta. Zmyslom dôkladnej autentizácie je za-

ručiť istotu, že prístup k svojmu účtu dostane len vlastník alebo iná osoba, ktorá má oprávnenie s účtom manipulovať. Medzi spôsoby a typy overenia identifikácie užívateľa pri prihlasovaní do internetového bankovníctva sa radia užívateľské meno (prípadne identifikačné číslo) a heslo, certifikát, čipová karta, SMS kód a autentizačný kalkulátor [18].

- **Užívateľské meno a heslo** – najznámejší a najrozšírenejší spôsob autentizácie, ktorý je ale zároveň aj najmenej bezpečným. Takmer vždy sú kladené rôzne požiadavky na dĺžku hesla alebo na skupiny znakov, ktoré musia byť v hesle zastúpené. Dôležité je aj uvážlivé nastavenie počtu chybných pokusov, po ktorých dôjde k zablokovaniu účtu. Príliš málo povolených chybných pokusov môže viesť k zbytočnému zablokovaniu účtu. Na druhej strane príliš vysoký počet alebo dokonca neobmedzené množstvo pokusov značne zvyšuje šance prípadného útočníka na prelomenie hesla.
- **Certifikát** – klient dostane od banky digitálny certifikát v podobe súboru, ktorý používa pre overenie žiadosti o autentizáciu. Certifikát by mal byť uložený na bezpečnom externom médiu a k počítaču pripájaný len vtedy, keď je to potrebné. Nevýhodou je obmedzená platnosť certifikátu, ktorú si však klient vie samostatne predĺžiť.
- **Čipová karta** – bezpečnejšia podoba predchádzajúceho prístupu. Certifikát je uložený na kryptografickej čipovej karte a nikdy túto kartu neopustí, pretože karta samotná je schopná vykonávať potrebné kryptografické operácie. Tým sa znižuje riziko zachytenia citlivých údajov útočníkom. K čipovej karte je potrebné si zadovážiť certifikovanú čítačku čipových kariet a mať ju pripojenú k počítaču.
- **SMS kód** – banka posiela klientovi vygenerovaný jednorazový kód s obmedzenou časovou platnosťou na mobilný telefón v podobe SMS správy. Po zadaní tohto kódu je klient úspešne autentizovaný. Ide momentálne o najpoužívanejšiu metódu overenia totožnosti.
- **Autentizačný kalkulátor** – využíva princíp jednorazových kódov s obmedzenou časovou platnosťou ako v predchádzajúcom prípade. Avšak tu je kód generovaný technickým zariadením, ktoré klient vlastní. Táto metóda sa už prakticky nepoužíva a bola nahradená modernejšími technológiami.

3.2.3 Autorizácia operácie

Úspešná autentizácia klienta umožňuje vo väčšine prípadov len pasívny prístup k účtu a pre aktívnu prácu s účtom, typicky vykonanie finančnej transakcie, je vyžadované ďalšie overenie. Prostriedky pre autorizáciu požadovanej operácie sa dnes často nelíšia od prostriedkov autentizácie klienta. Stretávame sa skôr s kombináciou vyššie uvedených metód, kde sa k autentizácii použije slabšia metóda užívateľského mena a hesla a k autorizácii sa použije už niektorý zo sofistikovanejších spôsobov overenia.

3.2.4 Ďalšie techniky zabezpečenia

Okrem vyššie spomenutých techník k lepšiemu zabezpečeniu prispievajú aj služby a mechanizmy, ktoré sa na prvý pohľad môžu zdať ako drobnosti, avšak v bezpečnosti elektronického bankovníctva majú dôležitú úlohu. Tu patria mechanizmy ako napríklad automatické odhlásenie zo systému po určitej dobe nečinnosti, zasielanie notifikačných správ o pohyboch na účte alebo stanovenie maximálnych čiastok pre platobné operácie v rámci určitého časového úseku.

3.3 Zabezpečenie smartbankingu

Česká republika sa drží vo využívaní technických noviniek v bankovníctve na popredných miestach. Smartbanking zažíva prudký vzostup spolu s masovým rozšírením chytrých telefónov. Podiel bankových operácií zadávaných cez aplikácie v mobiloch sa zvyšuje a banky sú na tomto poli veľmi aktívne. Prakticky všetky bankové domy v Českej republike už majú svoju mobilnú aplikáciu a neustále pracujú na zlepšeniach a nových funkciách pre svojich klientov [19].

Užívateľské prostredie mobilných aplikácií býva zvyčajne rozdelené na nezabezpečenú časť, kde je možné nájsť verejné informácie ako kontaktné údaje banky, zoznam najbližších bankomatov a pobočiek, kurzový lístok, prehľad noviniek a aktualít alebo rôzne druhy kalkulačiek. Naopak zabezpečená časť už vyžaduje štandardný proces autentizácie a následnú autorizáciu požadovaných transakcií obdobne ako v internetovom bankovníctve. Užívateľ má po prihlásení k svojmu účtu k dispozícii prehľadný zoznam dostupných funkcií ako je zobrazenie zostatku na účte, zadanie platobného príkazu, vytvorenie šablóny, zobrazenie histórie transakcií alebo aj platbu pomocou QR kódu.

Prvým krokom k používaniu smartbankingu je nainštalovanie mobilnej aplikácie z overeného zdroja a jej následná aktivácia. Aktivácia sa naprieč jednotlivými bankami čiastočne líši, ale v zásade sa používajú dva spôsoby – aktivácia aplikácie pomocou nastavenia v internetovom bankovníctve alebo priame zadanie prihlasovacích údajov, ktoré sú rovnaké ako pre internetové bankovníctvo. Nasleduje spárovanie telefónu s účtom klienta a následne klient získava prístup k svojmu účtu podobne ako pri internetovom bankovníctve [19].

Zabezpečenie prístupu klienta k svojmu účtu prostredníctvom mobilného bankovníctva je takmer totožné ako cez internetové bankovníctvo, opäť je potrebné riešiť zabezpečenie komunikácie, autentizáciu klienta a autorizáciu transakcií. Každá banka volí trochu odlišný prístup k celkovému zabezpečeniu a využíva rôzne bezpečnostné prvky.

3.3.1 Zabezpečenie prenosu dát

Situácia je v tomto smere zhodná ako v prípade internetového bankovníctva. Mobilný telefón klienta komunikuje prostredníctvom verejnej siete so serverom banky a na vytvorení zabezpečeného, šifrovaného spojenia sa podieľa opätovne protokol SSL/TLS. Rozdiel oproti internetovému bankovníctvu spočíva v tom, že namiesto webového prehliadača, v ktorom je overenie šifrovaného spojenia dnes samozrejmosťou, v prípade mobilného bankovníctva má komunikáciu na starosti aplikácia vyvinutá bankou. Bohužiaľ stále existujú prípady, že mobilná aplikácia dostatočne neoveruje certifikát serveru, s ktorým komunikuje a klienta neupozorňuje na skutočnosť, že spojenie nemusí byť bezpečné [16].

3.3.2 Autentizácia užívateľa a autorizácia transakcií

Metódy sú opäť podobné ako v prípade internetového bankovníctva. Pri prvom spustení aplikácie je potrebné spárovať mobilný telefón s účtom klienta. Tu sa klient typicky autentizuje informáciou, ktorú pozná, napríklad prihlasovacie meno/identifikačné číslo používané už v internetovom bankovníctve spolu s patričným heslom. Po úspešnom spárovaní je potrebný pre vstup do aplikácie už len PIN kód, ktorý si užívateľ nastavil.

Tým opäť užívateľ získava pasívny prístup k účtu a pre aktívnu prácu je potrebné transakcie autorizovať. Autorizovať transakciu je možné napríklad zadaním PIN kódu, ktorý sa

používa už na autentizáciu, alebo zadaním jednorazového kódu, ktorý banka posiela prostredníctvom SMS.

Pre úspešný útok v tomto prípade je potrebné získať fyzický prístup k mobilnému telefónu a zároveň poznať kód, ktorým užívateľ vstupuje do aplikácie. Na rozdiel od internetového bankovníctva, pri ktorom je pri dvojfaktorovej autentizácii komunikácia rozdelená na dva kanály, je tu celá komunikácia viazaná len k jednému kanálu, čo zľahčuje prípadný útok.

Technologický rozvoj, ktorý oblasť mobilných telefónov neustále zažíva, otvára dvere aj využitiu tretieho typu autentizácie užívateľa a to prostredníctvom biometrických údajov, predovšetkým odtlačku prsta. V súčasnej dobe patrí už čítačka odtlačkov prstov k bežnej výbave mobilných telefónov strednej a vyššej triedy. Vďaka rýchlosti a pohodlnosti si tento spôsob prihlasovania rýchlo získal obľubu medzi užívateľmi, ktorí požadovali túto funkciu zakomponovať do existujúcich mobilných aplikácií ako ďalšiu možnosť autentizácie alebo autorizácie. Momentálne je tento biometrický prvok pri zabezpečení možné využiť v aplikáciách mobilného bankovníctva u Komerční banky, UniCredit Bank, Equa bank, mBank, MONETA Money Bank a najnovšie aj u ČSOB. Tento prvok výrazne zvyšuje bezpečnosť pri správe finančných prostriedkov prostredníctvom mobilného bankovníctva.

3.4 Bezpečnostné prvky a riziká

V prehľade zabezpečenia elektronického bankovníctva uvedenom v predchádzajúcich kapitolách je možné identifikovať rôzne typy rizík spojených s jednotlivými metódami. Väčšina z nich je spojená so správaním užívateľa elektronického bankovníctva ako najslabšieho článku celého systému. Avšak existujú aj riziká na strane banky alebo iných inštitúcií, na ktoré už klient žiadny vplyv nemá. Pre banky by mala byť bezpečnosť ich klientov na prvom mieste v budovaní dôvery a profesionality. Banky sa snažia neustále informovať o potenciálnych hrozbách a šíriť povedomie o potrebe bezpečného a obozretného správania sa, či vystupovania v internetovom prostredí. Väčšina bánk má na svojich stránkach uvedené bezpečnostné zásady a odporúčania vo forme pravidiel, ktorými by sa mal klient riadiť. Dodržiavanie týchto pravidiel výrazne zníži riziko zneužitia a umožní predísť prípadnému útoku [20].

Riziká, na ktoré je potrebné sa zamerať a rady, ktorých sa treba držať, sú rozumne zhrnuté v nasledujúcich bodoch, ktoré vydala Česká bankovní asociace [21].

Desatoro bezpečnosti České bankovní asociace:

1. *Pravidelne aktualizujte ochranné mechanizmy svojho počítača.*
2. *Rovnako ako počítač chráňte aj svoj chytrý telefón.*
3. *Programy a aplikácie inštalujte iba z dôveryhodných a overených zdrojov.*
4. *Prihlasovacie a osobné údaje zadávajte len na overených serveroch, v dôveryhodnom prostredí a nikomu ich neposkytujte.*
5. *Starostlivo si chráňte svoj PIN kód.*
6. *Pravidelne si meňte svoje heslá a vyhnite sa užívaniu rovnakých hesiel pre rôzne služby.*
7. *Neotvárajte e-maily a prílohy od neznámych a podozrivých odosielateľov.*
8. *Nakupujte iba u preverených a dôveryhodných online predajcov.*
9. *Venujte dostatok pozornosti upozorneniam vášho počítača a na webe banky.*
10. *Pokiaľ si nie ste istí a máte podozrenie, že sa deje niečo nekalého, vždy kontaktujte banku.*

4 INTERNETOVÉ ÚTOKY A HROZBY

Neúnavná rýchlosť technologického vývoja prináša stále nové a nové hrozby pre individuálnu a globálnu bezpečnosť. Technologický pokrok je dôvodom pre čoraz aktuálnejšiu tému kybernetickej bezpečnosti. Dnešný svet sa spolieha na každodenné využívanie technológií a ľudia sú závislí na používaní počítačov, mobilných telefónov a prístupu na internet. Moderné technológie uľahčujú na jednej strane život, ale na druhej strane úmerne s tým narastá zraniteľnosť voči kybernetickým útokom. Hrozba kybernetických útokov sa s veľkou intenzitou rozšírila zo striktne vymedzenej sféry do všetkých oblastí spoločenského života [22].

V súčasnej dobe dochádza k stále častejším útokom na počítače, programy či dáta samotné. Útoky sú čoraz viac sofistikovanejšie a účinnejšie vďaka globalizácii a rozšíreniu informačných technológií do všetkých oblastí bežného života. Hrozbu ako takú je možné chápať ako akt smerujúci k nežiaducej zmene informácie, chovania systému alebo ovplyvneniu jeho parametrov. Útok je následne faktickou realizáciou hrozby. Je možné vymedziť štyri skupiny základných hrozieb z hľadiska bezpečnosti informačného systému [23].

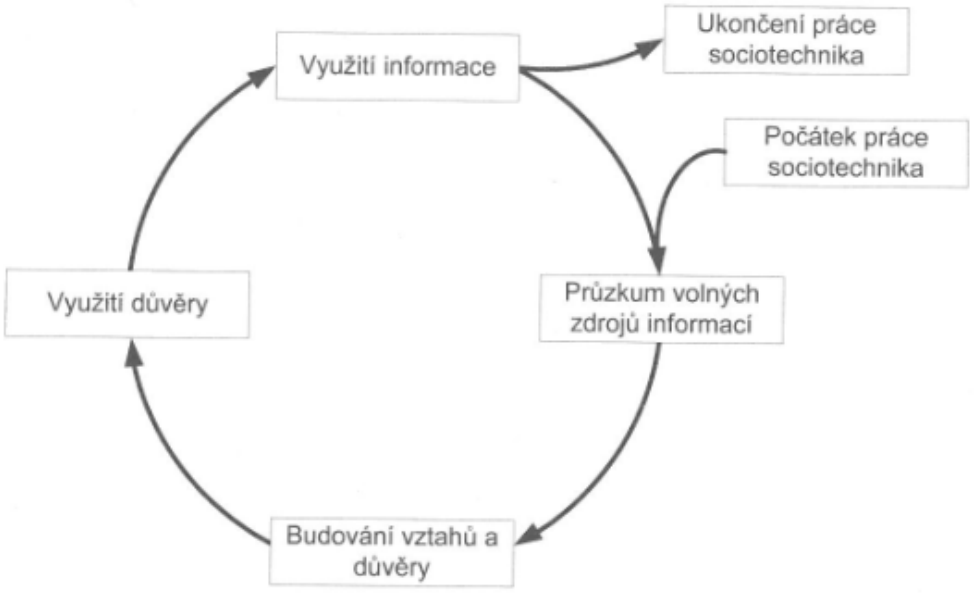
- **Únik informácie** – stav, kedy dôjde k vyzradeniu dôvernej informácie neautorizovanému subjektu.
- **Narušenie integrity** – predstavuje poškodenie, zmenu či vymazanie dát neautorizovaným subjektom.
- **Potlačenie služby** – úmyselné bránenie v prístupe legitímneho subjektu k informáciám alebo systémom.
- **Nelegitímne použitie** – využívanie informácií alebo zdrojov neautorizovaným subjektom či neadekvátnym spôsobom.

4.1 Sociálne inžinierstvo

Sociálne inžinierstvo využíva manipulačné techniky so zámerom získania tajných informácií. K účinnosti tejto techniky prispieva aj neopatrnosť, dôveryhodnosť a naivita obetí, ako najslabších článkov zabezpečenia počítačových systémov. Každý počítačový systém je do určitej miery závislý na ľudskom faktore. Z toho vyplýva, že táto technika je univerzálna, nezávislá na platforme, či druhu vybavenia a type zabezpečenia. Útočníci využívajú širokú škálu komunikačných nástrojov pre získanie čo najväčšieho množstva interných informá-

cií, ktoré im dopomôžu k žiadanému výsledku. Takýmito nástrojmi sú napríklad e-mail, telefónne hovory, SMS správy, sociálne siete, webové stránky, diskusné fóra a iné zdroje informácií. V dnešnej dobe sú predovšetkým sociálne siete a ich popularita ohromnou zásobou súkromných dát, ktoré vie útočník využiť vo svoj prospech [23].

Pri snahe o finančné obohatenie využívajú útočníci ako jednu z možností práve ukradnuté účty a podvodné identity na sociálnych sieťach. Pod falošnou identitou kontaktujú okruh potenciálnych obetí s prosbou o finančnú pomoc. Následne navedú obeť na podvodnú stránku, kde odchytia prihlasovacie údaje do internetového bankovníctva alebo nainfikujú počítač škodlivým softwarom. Manipulačné techniky sú tak sofistikované, že útočníkom nerobí problém vymámiť od dôveryhodných jedincov ani obsah autentizačných SMS správ.

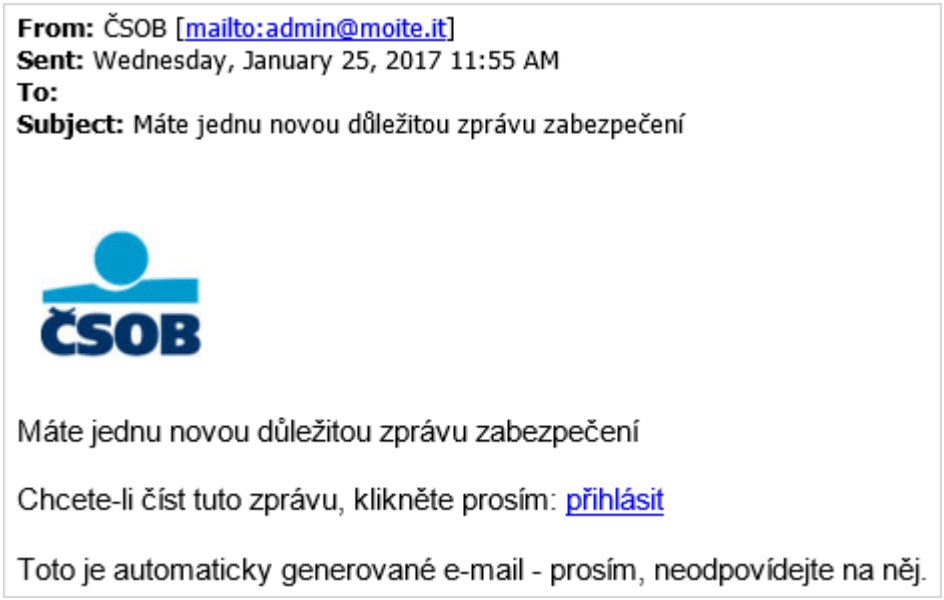


Obr. 5. Sociotechnický cyklus [23]

4.2 Phishing

Phishing je asi najznámejšia podvodná technika súvisiaca s elektronickým bankovníctvom. Princíp phishingu spočíva v rozosielaní falošných e-mailových správ, ktoré sa klamlivým spôsobom snažia vylákať od užívateľov citlivé údaje za pomoci prvkov sociálneho inžinierstva. Phishingové správy vyzerajú na prvý pohľad ako správy od vierohodných finanč-

ných inštitúcií. Presmerovaním na podvodné stránky sa snažia od dôveryhodných a nepozorných užívateľov vylákať prístupové údaje do internetového bankovníctva alebo informácie o platobnej karte. Podvrhnuté stránky sú na prvý pohľad prakticky totožné ako oficiálne stránky banky. Preto je zásadné vedieť ako phishing rozoznať a ako sa proti nemu brániť (viď. sekcia 3.2.1.). Je dôležité si taktiež uvedomiť, že žiadna banka nikdy od svojich klientov nepožaduje prihlasovanie údaje formou e-mailovej komunikácie [24].



Obr. 6. Ukážka phishingovej správy [25]

4.3 Pharming

Pharming funguje na podobnom princípe ako phishing, ale ide o sofistikovanejšie riešenie podvrhnutia podvodných stránok užívateľom. Útok je vedený na zmenu DNS (Domain Name System) záznamu, ktorý prekladá doménové mená na IP adresy. Existujú dva spôsoby realizácie útoku [26]:

- Útok na DNS server – v prípade, že sa útočník zmocní niektorého z DNS serverov, má možnosť presmerovať webové stránky internetového bankovníctva na podvrhnuté IP adresy. Užívateľ teda aj pri zadaní správnej webovej adresy svojej banky do internetového prehliadača bude presmerovaný na falošnú stránku vytvorenú útočníkom. Falošná stránka je opäť k nerozoznaniu od originálnej a užívateľ v dobrej viere nechtiac poskytne svoje prihlasovacie údaje útočníkovi.

- Útok na lokálne hosts súbory – ide o rovnaký princíp s menším dopadom, keďže k zmene DNS záznamu dôjde v hosts súbore operačného systému na konkrétnom napadnutom počítači.

4.4 Keylogger

Keylogger je nástroj, ktorý slúži k záznamu všetkých napísaných znakov na klávesnici. Vyskytuje sa buď v podobe mechanického zariadenia (hardware) alebo ako škodlivý program (software). Mechanické zariadenie sa pripojuje medzi klávesnicu a vstup do počítača a vyžaduje priamy prístup páchateľa k počítaču. Keylogger ako program býva skryte nainštalovaný a veľmi ťažko odhaliteľný. Účelom je sledovanie zaznamenávania akýchkoľvek vykonávaných aktivít. V pravidelných intervaloch keylogger odosiela súbor obsahujúci vstupy z klávesnice páchateľovi na určený server. Útočník môže následne súbor analyzovať a vyfiltrovať identifikačné a prístupové údaje, ktoré sa dajú zneužiť. Ako ochranu pred keyloggerom ponúkajú niektoré stránky internetového bankovníctva virtuálnu klávesnicu, kde sa znaky zadávajú pomocou počítačovej myši. Druhou možnosťou je používať spoľahlivý program pre správu hesiel, odkiaľ sa heslo v prípade potreby skopíruje do pamäte a následne vloží na príslušné miesto. Nie je teda nutné heslá na klávesnici manuálne vypisovať, čím sa eliminuje riziko ich odchytenia a sprostredkovania páchateľovi [27].

4.5 Malware

Malware je všeobecný pojem pre akýkoľvek škodlivý software, ktorý má útočníkovi zaistiť neoprávnený prístup k užívateľskému zariadeniu za účelom poškodiť, zneužiť alebo ukradnúť citlivé informácie. Z pohľadu bankového sektora jednoznačne ide o veľmi závažnú kybernetické hrozbu. Malware sa šíri prostredníctvom napadnutých webových stránok, v prílohe e-mailov alebo ako súčasť rôznych programov a voľne stiahnuteľných súborov. Medzi najznámejšie typy malwaru patrí spyware, adware, trojský kôň, počítačový červ, rootkit, ransomware a iné [27].

4.6 Ransomware

Ramsomware je špeciálnym typom malwaru, ktorý aktuálne budí asi najviac rozruchu na poli kybernetickej kriminality. Svojím brutálnym a deštruktívnym prístupom vyvoláva zúfalstvo u koncových užívateľov, ale i celých firiem a organizácií. Termín ransomware je odvodený z anglických slov ransom (výkupné) a malware. Vo všeobecnosti ide o škodlivý software distribuovaný na počítačové systémy, ktorého účelom je zašifrovanie a zneprístupnenie súborov, dokumentov a znemožnenie legitímneho prístupu k počítaču. Útočníci sa následne snažia svoju obeť vydierať a požadujú zaplatiť nemalé výkupné, väčšinou vo forme bitcoinov, za odblokovanie a znovuzískanie prístupu k systému. Ponuka na zaplatenie je spravidla časovo obmedzená, prípadne sa po uplynutí určitého limitu ešte navýši. Ak napadnutý nevyužije túto možnosť a nezaplatí, ransomware všetky dáta nenávratne zmaže [28].

Brániť sa pred útokom typu ransomware vyžaduje dodržiavať kombináciu preventívnych opatrení, ktoré dokážu minimalizovať riziko a tým ochrániť dáta, reputáciu i finančné prostriedky jednotlivých firiem. Medzi odporúčané spôsoby ochrany sa radia:

- Monitoring pre kontrolu webového prístupu
- Scan všetkých e-mailových príloh
- Scan všetkých externých médií
- Aktualizovaný operačný systém a software
- Pravidelná záloha dát
- Školenie zamestnancov

Obr. 7. Ilustratívny obrázok ransomwaru [27]

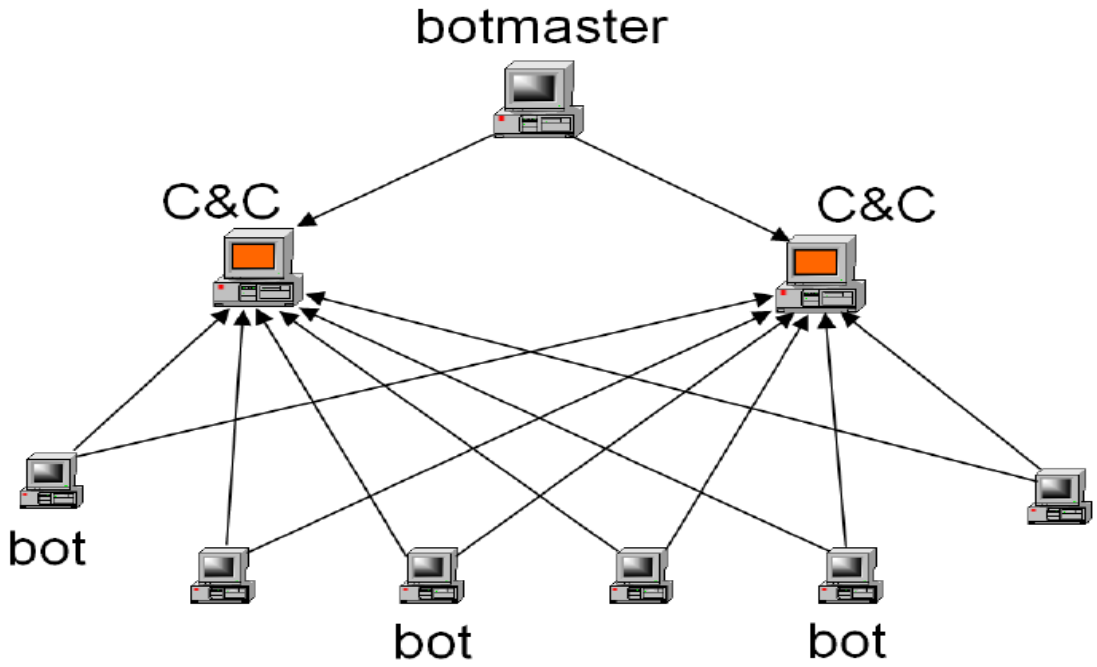
4.7 Botnet

Botnety sú považované za jednu z najväčších internetových hrozieb súčasnosti. Bot, odvodený od slova robot, je druh škodlivého kódu alebo program, ktorý umožňuje útočníkovi prevziať kontrolu nad napadnutým počítačom. Medzi základné vlastnosti bota patria nasledujúce charakteristické prvky:

- Infiltruje sa do cieľového systému bez vedomia užívateľa
- Snaží sa o replikáciu na ostatné systémy v lokálnej sieti
- Vykonáva preddefinované úlohy a príkazy automaticky a nezávisle
- Prijíma príkazy na diaľku cez určitý komunikačný kanál

Napadnuté počítače, niekedy nazývané ako „zombie“, tvoria rozsiahle botnetové siete v počte až stoviek tisíc počítačov. Botnety sú pod kontrolou tzv. C&C serverov (Command and Control) a ovládané botmasterom. C&C servery majú za úlohu riadiť sieť napadnutých počítačov, filtrovať a aktualizovať jednotlivé uzly a zadávať požadované príkazy. Architektúra botnetu môže byť buď centralizovaná, s jedným C&C serverom alebo decentralizovaná, kde je riadiacich serverov niekoľko a sú navzájom zastupiteľné. Druhou časťou botnetu sú samotné počítače užívateľov, spravidla využívajúce operačný systém MS Windows. Tie sa dajú nainfikovať škodlivým kódom rôznymi technikami ako napríklad otvorením mailovej prílohy, sťahovaním pochybného softwaru, odkazmi v spame, náhodným hádaním alebo odpočúvaním hesiel, sekvenčným prechádzaním IP adries s následným útokom na zraniteľné chyby v systéme. Po infikovaní a inštalácii škodlivého kódu sa počítač ozve C&C serveru, ktorému sa nahlási a požiada o ďalšie inštrukcie [29].

Botnet je sieťou typu klient-server a komunikácia v rámci botnetu prebieha na základe zvolenej architektúry a používaných protokolov (napr. IRC, HTTP/HTTPS). Využíva sa aj forma šifrovania za účelom chrániť botnet proti odhaleniu a odpočúvaniu.



Obr. 8. Príklad architektúry botnetu [30]

Najväčšou silou botnetu je práve počet ovládaných počítačov, ktoré disponujú obrovským výpočtovým výkonom. Primárnym účelom vytvárania botnetových sietí je generovanie zisku. Využitie botnetu nemá určené hranice a záleží na požiadavke tvorcu alebo osoby, ktorá si botnetovú sieť prenajme za určitý finančný obnos. Medzi najčastejšie požiadavky sa radí napríklad rozosielanie spamu, distribuované odoprenie služby (DDoS), odchytávanie sieťovej komunikácie (sniffing), odchytávanie stlačených kláves (keylogging), šírenie malwaru, masové krádeže identít, predaj proxy a výpočtového výkonu, ťažba kryptomien, manipulácia s online anketami, atď [31].

Príkladom botnetu je botnet Zeus, ktorý mal za úlohu zbierať dáta a prihlasovacie údaje k elektronickému bankovníctvu a vďaka nemu sa zločincom podarilo ukradnúť až milióny dolárov z rôznych bankových účtov.

5 ANALÝZA ÚTOKOV

Celá oblasť informačnej bezpečnosti prešla v posledných rokoch výraznými zmenami. Vyvolal ich markantný vzostup kybernetických rizík, nové typy a techniky útokov, sofistikované škodlivé programy a profesionalizácia útočníkov. Z týchto dôvodov predstavujú kybernetické útoky jednu z najväčších bezpečnostných hrozieb súčasnosti.

Kybernetická bezpečnosť je oproti tradičným hrozbám pomerne špecifická. V prvom rade sa týka ohromného počtu ľudí. Kybernetické hrozby sú navyše oveľa bezprostrednejšie, osobnejšie a pomerne ľahko uskutočniteľné. Útočník si vystačí s počítačom, prístupom na internet a vlastnými schopnosťami. Povaha kybernetického priestoru a celosvetové pokrytie umožňuje páchateľovi zaútočiť kedykoľvek a kdekoľvek v relatívne krátkom čase. Situáciu komplikuje aj zložité vypátranie útočníka a preukázanie jeho viny. Útočníci totiž ako zdroje útokov využívajú najmä napadnuté počítače užívateľov [22].

Banky robustne investujú do ochrany zabezpečenia a vnútorných monitorovacích nástrojov, ktoré pomáhajú odhaliť zneužitie identity klienta. Pre ochranu financií je taktiež nevyhnutná i pomoc samotných klientov. Zabezpečenie počítača, telefónu alebo spoľahlivého internetového pripojenia je plne v ich zodpovednosti. Je potrebné zvýšiť povedomie zodpovednosti klientov za prípadné nedodržanie bezpečnostných pravidiel. Banky každý prípad posudzujú individuálne a skúmajú nakoľko k odcudzeniu finančných prostriedkov došlo vinou alebo zanedbaním na strane klienta. Keď sa takáto skutočnosť preukáže, je dosť pravdepodobné, že mu vzniknutá škoda nebude kompenzovaná.

5.1 Pranie špinavých peňazí

Všetky typy internetových útokov majú jeden spoločný menovateľ, a tým je finančné obohatenie páchateľov. Prihlasovacie údaje, informácie o platobných kartách, či iné citlivé dáta majú pre útočníkov veľkú hodnotu. Takto nelegálne získané údaje musia byť v čo najkratšom čase zanalyzované a zneužité pre prevod alebo výber finančných prostriedkov z účtu obete. Útočníci si kvôli vlastnej ochrane a anonymite najímajú na tieto účely prostredníka, tzv. bieleho koňa. Biele kone sú zvyčajne osoby na okraji spoločnosti, v ťažkej životnej situácii, pod vplyvom drog, bezdomovci alebo osoby s nízkym intelektom. Biele kone sa získavajú na atraktívne inzeráty s ponukou práce z domova a skoro nulovými požiadavkami na uchádzača. Za pomerne nízku finančnú odmenu sú ochotní útočníkovi spro-

stredkovať požadovanú službu, ako je napríklad finančná transakcia, výber z bankomatu alebo návšteva pobočky, čím nevedomky prispievajú k legalizácii výnosov z trestnej činnosti. Týmto spôsobom sú útočníci schopní vyviesť peniaze z banky a následne si ich nechať zaslať pomocou spoločností, ktoré poskytujú rýchle hotovostné prevody do zahraničia (Western Union, Money Gram). Tým sa výrazné sťaží možnosť dohľadať finančný tok takto zlegalizovaných peňazí.

5.2 Návrh preventívnych opatrení

Univerzálny návod ako sa vyvarovať všetkým nástrahám a rizikám v prostredí internetu a obzvlášť pri zachádzaní s elektronickými peniazmi neexistuje. Banky sa snažia svoju úroveň zabezpečenia neustále zdokonaľovať. Najrizikovejším článkom je ale bohužiaľ klient sám. Najlepším spôsobom ako eliminovať čo najviac rizikových faktorov je dodržiavať vypracované postupy a návody jednotlivých bánk. Táto metodika v podobe bezpečnostného desatora obsahuje zásady, rady a postupy, pomocou ktorých sa dá vo veľkej miere útokom predchádzať. Každá banka má nejakú obdobu bezpečnostného desatora dostupnú na svojich stránkach. Dodržiavaním týchto postupov klient výrazne zníži riziko potenciálneho útoku voči svojej osobe.

Vo všeobecnosti sa dajú preventívne opatrenia zhrnúť do nasledujúcich štyroch oblastí:

- **Technické vybavenie** – ochrana a zabezpečenie počítača i mobilného telefónu sú základným kameňom úspechu v boji proti kybernetickým útokom. Je potrebné pravidelne aktualizovať operačný systém a aplikácie, používať antivírusový program, nesťahovať aplikácie a súbory z neoverených zdrojov, nenechávať zariadenie bez dozoru a uzamykať obrazovku. Rozumným opatrením je taktiež pravidelná záloha systému.
- **Opatrnosť** – pri používaní internetu je potrebné dbať na zvýšenú opatrnosť. Všímať si znaky zabezpečeného, šifrovaného spojenia a kontrolovať platnosť certifikátu a identitu banky na stránkach internetového bankovníctva. Ďalším pravidlom je nereagovať na podozrivé e-mailové správy, neotvárať žiadne neznáme prílohy a neinštalovať pochybné programy a aplikácie neznámeho pôvodu.
- **Starostlivosť** – k starostlivosti o bezpečnosť svojich financií patrí pravidelná kontrola pohybov na účte, dôkladná ochrana prihlasovacích údajov i PIN kódu a ich

neposkytovanie ďalším osobám. Prihlasovacie heslá je potrebné pravidelne meniť a nevoliť ľahko uhádnuteľné znaky.

- **Komunikácia** – všetky banky sa snažia o čo najefektívnejšiu komunikáciu so svojimi klientmi, šírenie osvety a zvýšenie povedomia o bezpečnosti v elektronickom prostredí. Predovšetkým je potrebné dôkladne kontrolovať zasielané informácie a sledovať prípadné upozornenia alebo varovania. V prípade akéhokoľvek podozrenia alebo problémov je potrebné neodkladne kontaktovať svoju banku.

II. PRAKTICKÁ ČASŤ

6 PRIESKUM O POVEDOMÍ INTERNETOVEJ BEZPEČNOSTI

Dotazníkový prieskum je najčastejším typom zberu informácií v rôznych záujmových rovinách. Na základe prieskumu potom dochádza k vyvodeniu záverov alebo ďalšiemu smerovaniu. Aplikácia prieskumu formou online dotazníka predstavuje rýchlu a efektívnu formu získavania informácií o konkrétnom tematickom okruhu.

Vytvorený prieskum o povedomí internetovej bezpečnosti v súvislosti s peniazmi sa zameriava na používanie elektronického bankovníctva a problematiku jeho zabezpečenia. Ďalej skúma povedomie ľudí v spojitosti s internetovými útokmi a hrozbami, ktoré môžu viesť ku krádeži peňažných prostriedkov. Výsledky sú prezentované vo forme grafov a tabuliek pre lepšiu výpovednú hodnotu.

6.1 Charakteristika a cieľ prieskumu

Dotazník obsahuje 31 otázok, ktorých plné znenie je uvedené v prílohe P I tejto diplomovej práce. V prílohe je umiestnený aj odkaz na webovú adresu, na ktorej bolo možné dotazník vyplniť. Celý dotazník využíva formu uzatvorených otázok s výberom práve jednej alebo viacerých možností. Prieskum prebiehal výhradne v elektronickej podobe na prelome apríla a mája v rámci Českej a Slovenskej republiky. Kompletné výstupy a výsledky prieskumu sú uložené v samostatnom Microsoft Excel súbore.

Dotazník zahrňuje niekoľko skúmaných oblastí. Prvá časť je zameraná na identifikačné údaje respondentov (pohlavie, vek, sociálny status a ukončené vzdelanie), druhá na používanie internetu (typy zariadení a druhy činností). Následne sa dotazník vetví podľa toho, či respondent využíva alebo nevyužíva služby elektronického bankovníctva. Ak nie, dotazník po uvedení ponúknutých dôvodov skončí. V opačnom prípade pokračuje časťou venovanou problematike elektronického bankovníctva, platobných kariet a v neposlednom rade bezpečnostných prvkov a možných rizík.

6.2 Vyhodnotenie prieskumu

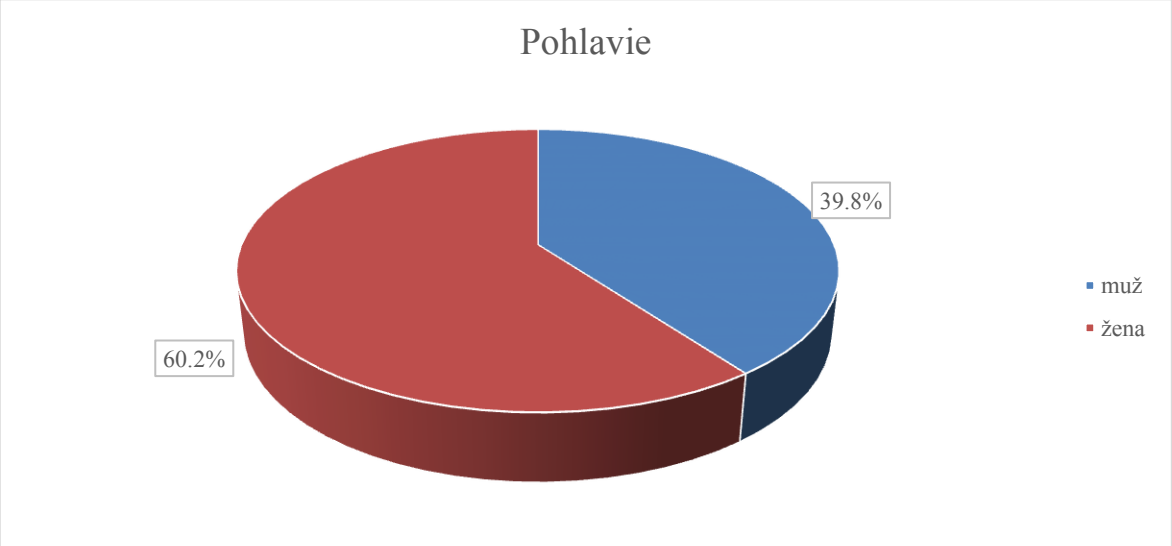
Prieskumu o povedomí internetovej bezpečnosti v súvislosti s peniazmi sa celkovo zúčastnilo 389 respondentov. Vyhodnotenie prieskumu a jednotlivých otázok je prezentované v prehľadnej forme za pomoci grafov a tabuliek.

Časť I – Identifikačné údaje

Prvé štyri identifikačné otázky sú určujúce pre zaradenie respondentov, ktorí sa zúčastnili prieskumu, do jednotlivých kategórií podľa pohlavia, veku, sociálneho statusu a najvyššieho ukončeného vzdelania.

Otázka: Pohlavie

Prvá otázka sa pýtala na pohlavie. Dotazník vyplnilo 389 respondentov, z toho 39,8 % mužov a 60,2% žien.

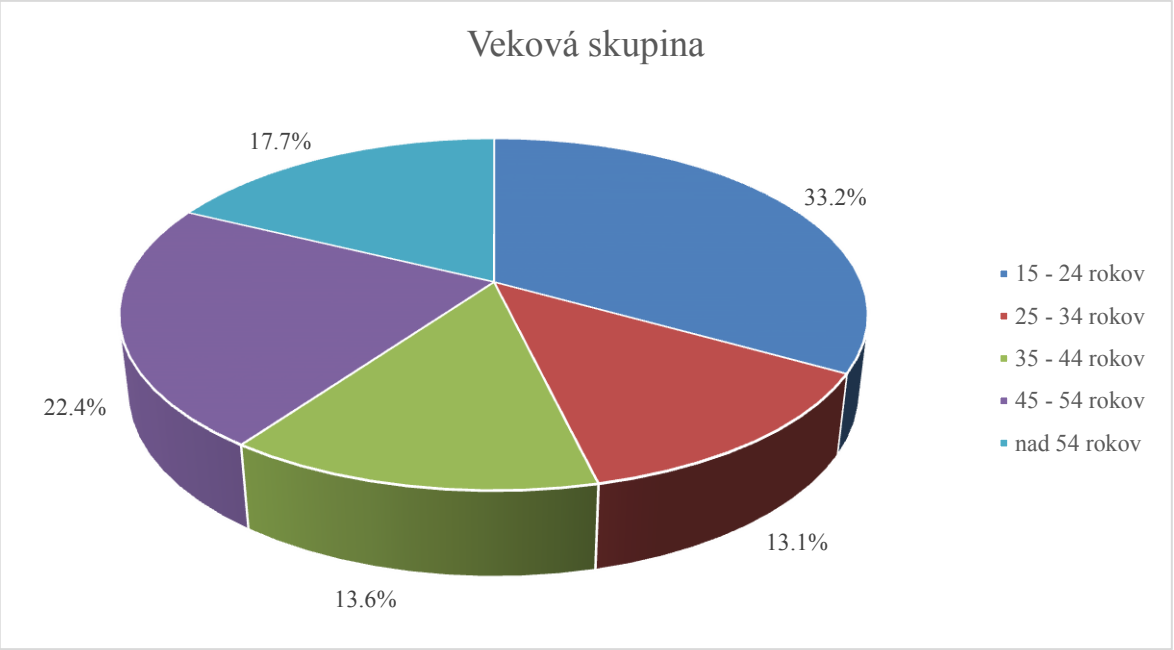


Obr. 9. Percentuálny pomer mužov a žien [zdroj vlastný]

Otázka: Veková skupina

Ďalším dôležitým ukazovateľom je vekové rozdelenie, pričom vekový rozsah je rozdelený do piatich kategórií. Prvú skupinu tvoria respondenti vo veku od 15 do 24 rokov. Druhú skupinu odpovedajúcich respondentov tvoria opýtaní vo veku od 25 do 34 rokov. V tretej skupine sa nachádzajú respondenti vo veku od 35 do 44 rokov, v štvrtej je rozmedzie od 45 do 54 rokov a v poslednej sú všetci vo veku nad 54 rokov.

Zastúpené sú všetky vekové kategórie pomerne vyrovnane, pričom najväčšiu skupinu tvoria mladí ľudia od 15 do 24 rokov (33,2%). Druhou početnou skupinou (22,4%) boli ľudia od 45 do 54 rokov. Ďalšou v poradí je skupina ľudí nad 54 rokov (17,7%). Približne rovnaké zastúpenie majú vekové kategórie od 25 do 34 rokov (13,1%) a od 35 do 44 rokov (13,6%).

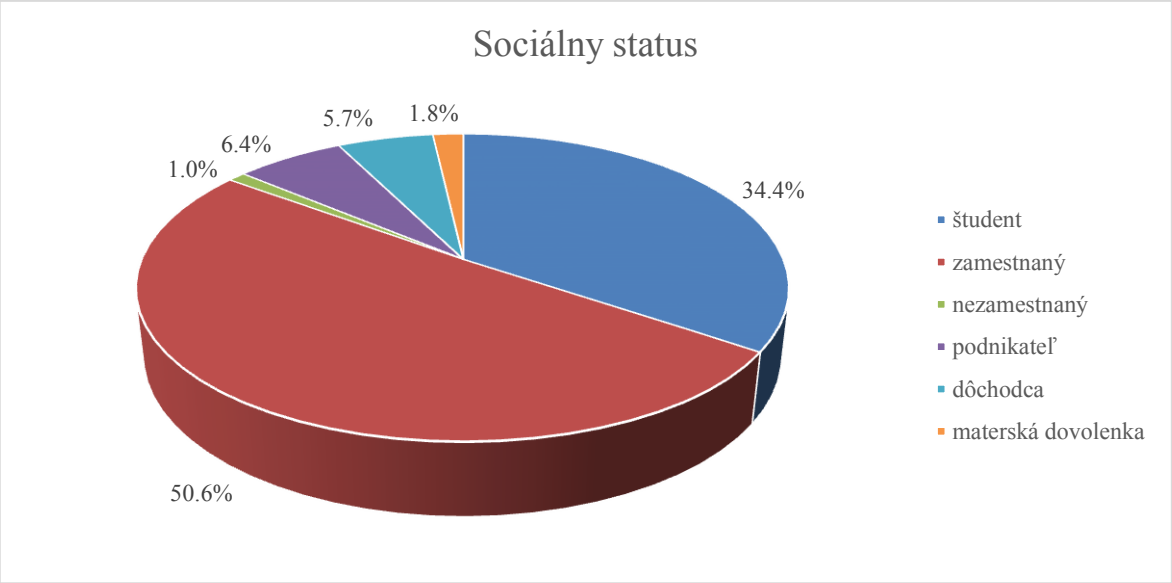


Obr. 10. Vekové rozdelenie respondentov [zdroj vlastný]

Otázka: Váš sociálny status

Tretia otázka mapovala sociálny status respondentov, ktorý bol rozdelený na kategórie: študent, zamestnaný, nezamestnaný, podnikateľ, dôchodca a respondenti na materskej dovolenke.

Zastúpenie majú všetky kategórie, pričom najväčší počet respondentov 50,6% tvorí skupina zamestnancov. Druhou najpočetnejšou skupinou boli študenti v pomere 34,4%. Ďalšie kategórie sú zastúpené v menšej miere a to nasledovne: nezamestnaní 1,0%, podnikatelia 6,4%, dôchodcovia 5,7% a mamičky na materskej dovolenke 1,8%.

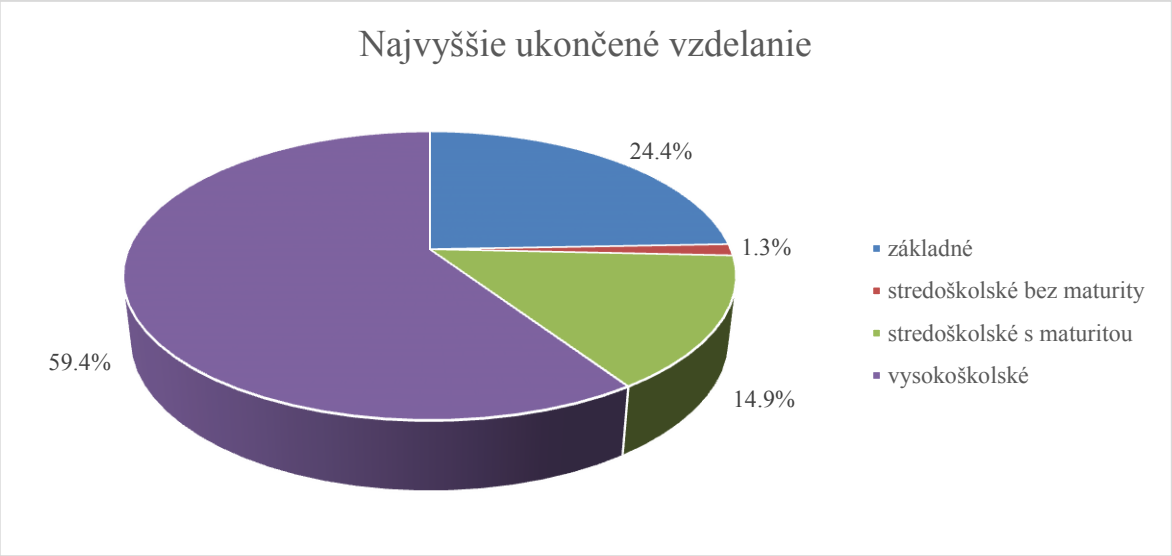


Obr. 11. Sociálny status respondentov [zdroj vlastný]

Otázka: Vaše najvyššie ukončené vzdelanie

Posledná otázka v rámci identifikačných údajov opýtaných sa týkala najvyššieho ukončeného vzdelania.

Najväčší počet respondentov, a to viac ako polovica, sú ľudia s vysokoškolským vzdelaním (59,4%). Druhá početná skupina má ukončené základné vzdelanie (24,4%), čo korešponduje s vekovou skupinou 15 – 24 rokov a sociálnym statusom študent. Treťou skupinou sú respondenti s ukončeným stredoškolským vzdelaním s maturitou (14,9%) a minoritný podiel v prieskumu tvorili respondenti s ukončeným stredoškolským vzdelaním bez maturity (1,3%).



Obr. 12. Dosiahnuté vzdelanie respondentov [zdroj vlastný]

Časť II – Používanie internetu

V tejto časti prieskumu sa respondentom položili dve otázky týkajúce sa zariadení, ktoré používajú pre prístup na internet a činností, ktoré robia online.

Otázka: Aké zariadenia používate pre prístup na internet?

Cieľom otázky bolo zmapovať najčastejšie používané zariadenia pre prístup na internet, pričom jeden respondent mohol uviesť aj viacero zariadení, pomocou ktorých pristupuje na internet.

Tab. 1. Používané zariadenia [zdroj vlastný]

Zariadenie	Percento respondentov používajúcich zariadenie
mobil/smartphone	70,2%
tablet	30,8%
notebook	82,0%
stolný počítač	49,6%
Iné	1,0%

Najväčší počet opýtaných 82,0% používa k prístupu na internet notebook. Stále viac a viac ľudí pristupuje na internet prostredníctvom svojho mobilného telefónu, čo sa potvrdilo aj v tomto prieskume, kde možnosť mobil/smartphone uviedlo až 70,2% respondentov. Tretím v poradí bol stolný počítač, ktorý používa skoro polovica všetkých opýtaných. Na po-

slednom mieste je tablet, ktorý používa iba 30,8% respondentov. Dokonca 1,0% opýtaných uviedlo aj iné zariadenie, ktoré používajú pre prístup na internet (Smart TV, Playstation).

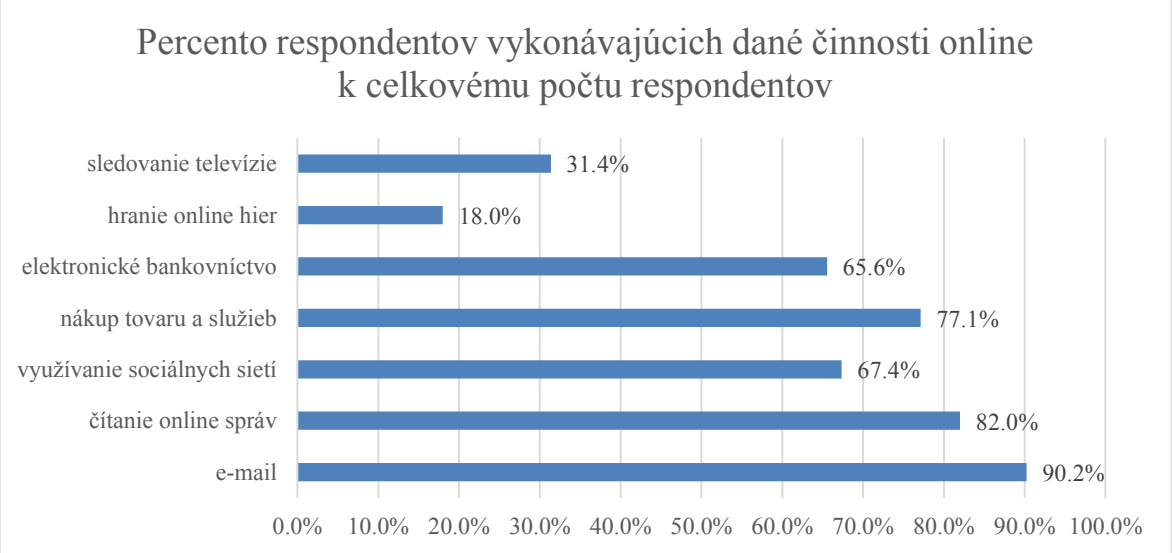
Zaujímavé je porovnanie, koľko rôznych zariadení využívajú respondenti pre prístup na internet. Najbežnejšie je podľa výsledkov prieskumu využívať 2 typy zariadení, keďže takto odpovedalo 34,7% respondentov. Až 3 rôzne zariadenia používa rovných 26,0% opýtaných. Nasleduje jedno zariadenie s 23,9%, 4 zariadenia uviedlo 14,7% respondentov a dokonca sa vyskytli v nepatrnej miere aj odpovede s 5 zariadeniami.

Tab. 2. Počet používaných zariadení [zdroj vlastný]

Počet zariadení	Percento respondentov používajúcich zariadenia
1 zariadenie	23,9%
2 zariadenia	34,7%
3 zariadenia	26,0%
4 zariadenia	14,7%
5 zariadení	0,7%

Otázka: Ktoré z nasledujúcich činností robíte online?

Táto otázka mapovala najčastejšie činnosti, ktoré respondenti robia online, pričom bolo možné zase zvoliť viacero odpovedí. Ako je možné vidieť v uvedenom grafe, až 5 činností sa teší pomerne veľkej obľube medzi respondentmi. Najviac používaný je e-mail s 90,2%, na opačnej strane sú potom sledovanie televízie a online hry.



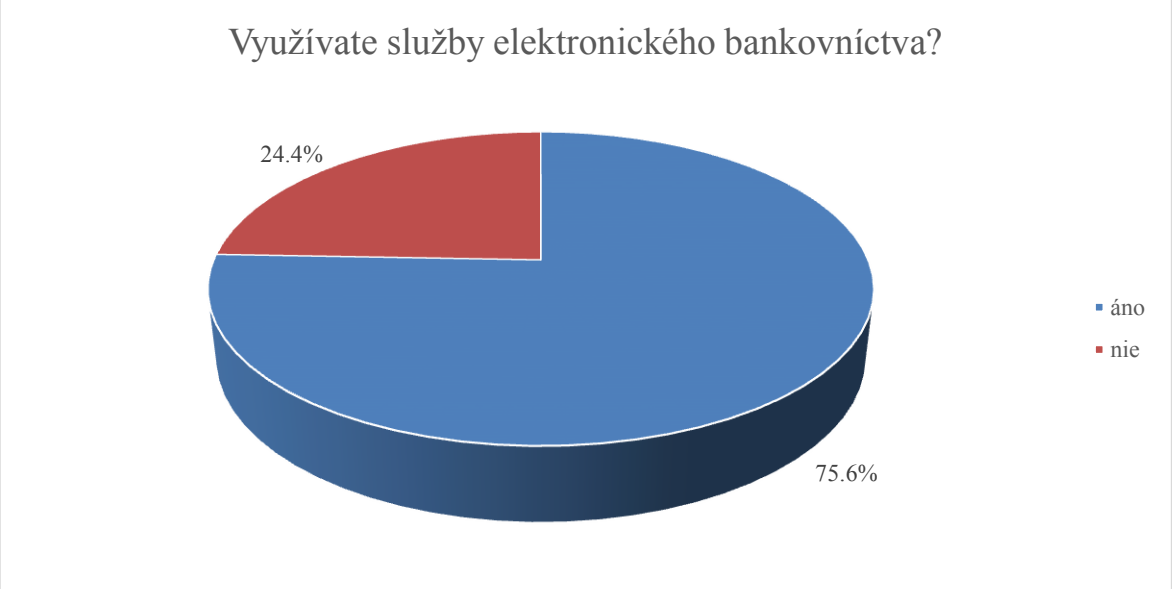
Obr. 13. Prehľad online činností [zdroj vlastný]

Časť III – Elektronické bankovníctvo

V tejto časti sa prieskum začína venovať otázkam týkajúcich sa elektronického bankovníctva. Základnou určovacou otázkou je, či ho respondenti využívajú alebo nie. Vzhľadom na odpoveď (áno/nie) sa dotazník rozdelil na dve sekcie Elektronické bankovníctvo – áno a Elektronické bankovníctvo – nie.

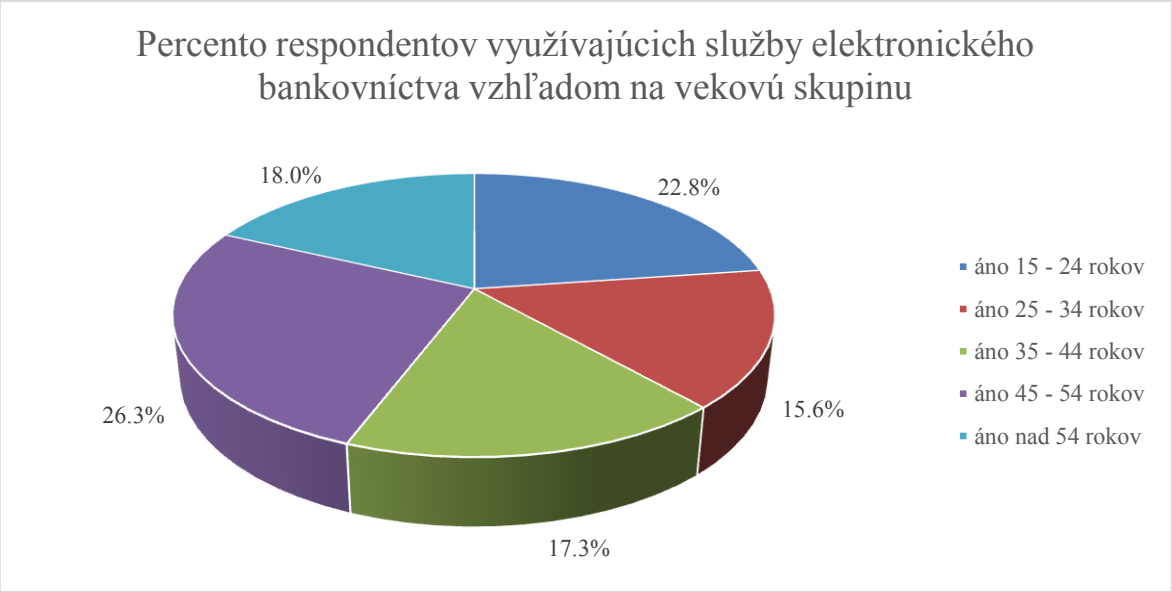
Otázka: Využívate služby elektronického bankovníctva?

Otázka ohľadne využívanie služieb elektronického bankovníctva rozdelila respondentov na dve skupiny. Väčšina opýtaných služby elektronického bankovníctva využíva. Takto odpovedalo 75,6%, čo zodpovedá počtu 294 respondentov. Zvyšok opýtaných 24,4% v počte 95 respondentov služby elektronického bankovníctva nevyužíva.

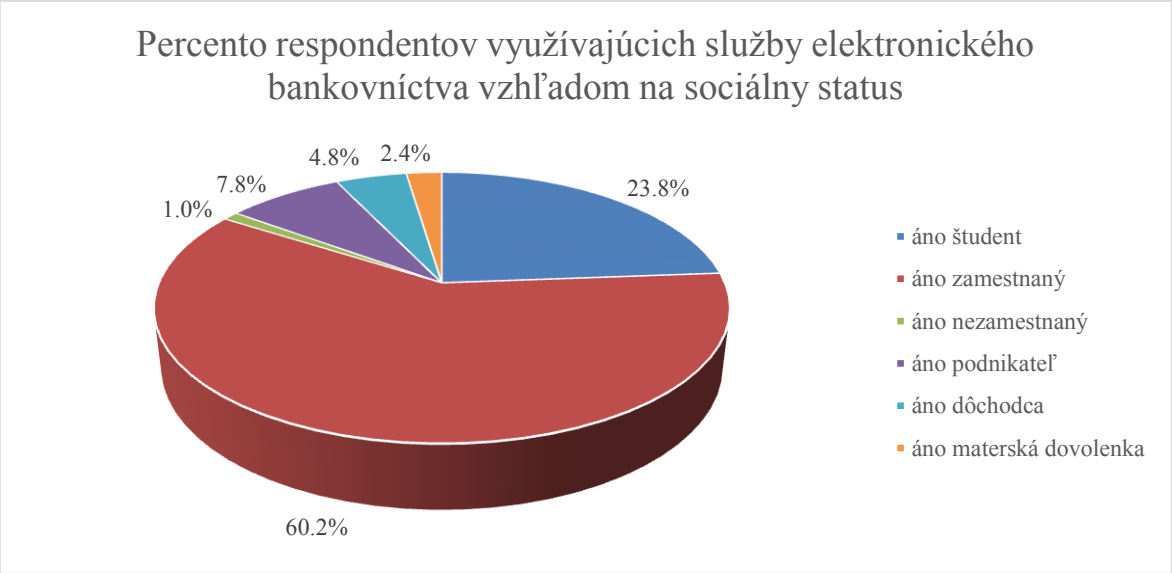


Obr. 14. Využívanie elektronického bankovníctva [zdroj vlastný]

Túto otázku je rozumné rozobrať viac do hĺbky, aby sa bližšie určili konkrétne skupiny ľudí, ktorí využívajú alebo nevyužívajú služby elektronického bankovníctva. Porovnávanie je možné realizovať na základe uvedených identifikačných údajov, t.j. vzhľadom na vek alebo sociálny status. Jednotlivé zistenia sú prezentované v nasledujúcich grafoch.



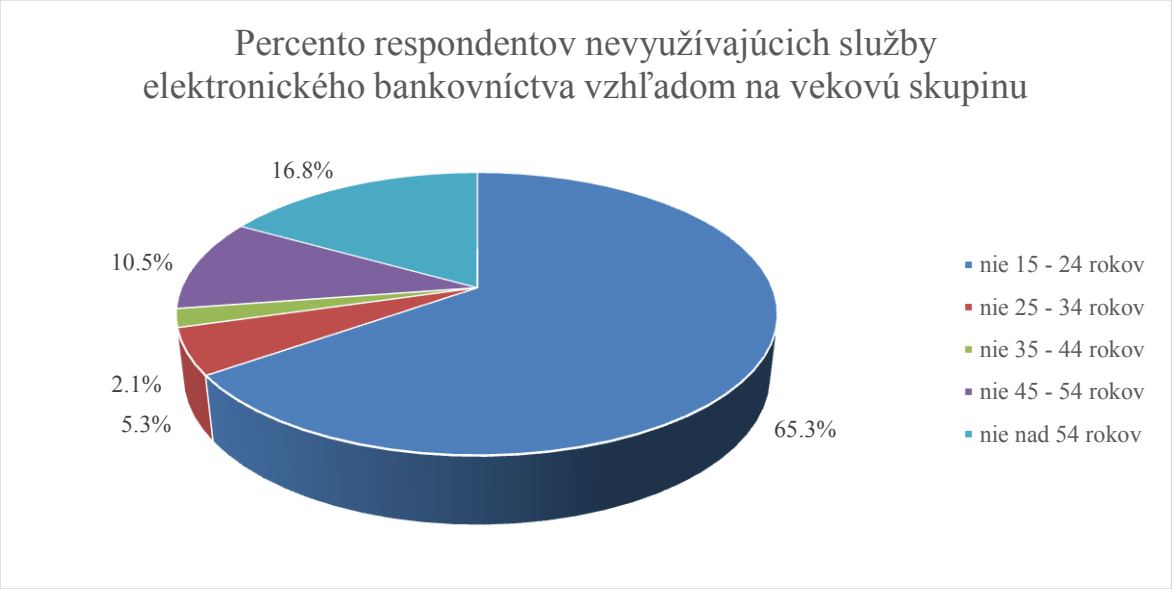
Obr. 15. Využívanie elektronického bankovníctva podľa veku [zdroj vlastný]



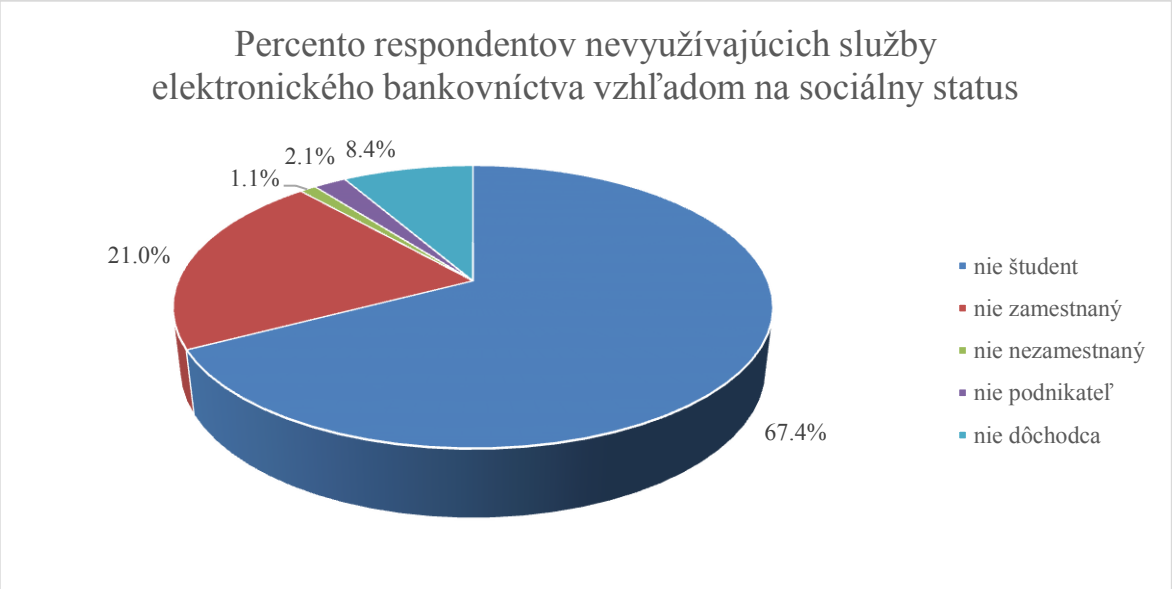
Obr. 16. Využívanie elektronického bankovníctva podľa sociálneho statusu [zdroj vlastný]

Percentuálne hodnoty vychádzajú zo vzorky 294 respondentov, ktorí odpovedali kladne na otázku využívania služieb elektronického bankovníctva. Porovnanie podľa veku je vzácne vyrovnané. Iba s malými rozdielmi sú zastúpené všetky vekové kategórie. Vzhľadom na sociálny status tvoria najpočetnejšiu skupinu 60,2% zamestnanci. Ďalšími v poradí sú s 23,8% študenti a so 7,8% podnikatelia. Ľudia na dôchodku využívajú elektronické bankovníctvo podľa očakávania len v malej miere.

Z 95 respondentov, ktorí odpovedali záporne sú najmladší a najstarší dve najpočetnejšie vekové skupiny. V prípade sociálneho statusu sa nachádzajú na prvom mieste s veľkým náskokom študenti s 67,4%, nasledovaní zamestnancami s 21,0% a dôchodcami s 8,4%.



Obr. 17. Nevyužívanie elektronického bankovníctva podľa veku [zdroj vlastný]



Obr. 18. Nevyužívanie elektronického bankovníctva podľa sociálneho statusu [zdroj vlastný]

Prehľadný rozpis percenta respondentov nevyužívajúcich služby elektronického bankovníctva vzhľadom na vekovú skupinu, sociálny status a aj najvyššie ukončené vzdelanie dáva nasledujúca tabuľka. Z nej vyplýva, že najvyššie percento respondentov, ktorí nevyužívajú služby elektronického bankovníctva (58,9%) je z vekovej skupiny 15 – 24 rokov, so sociálnym statusom študent a so základným vzdelaním, t.j. študenti stredných škôl. Opačným protipólom s výrazným zastúpením sú starší respondenti, buď ešte zamestnaní, alebo už na dôchodku.

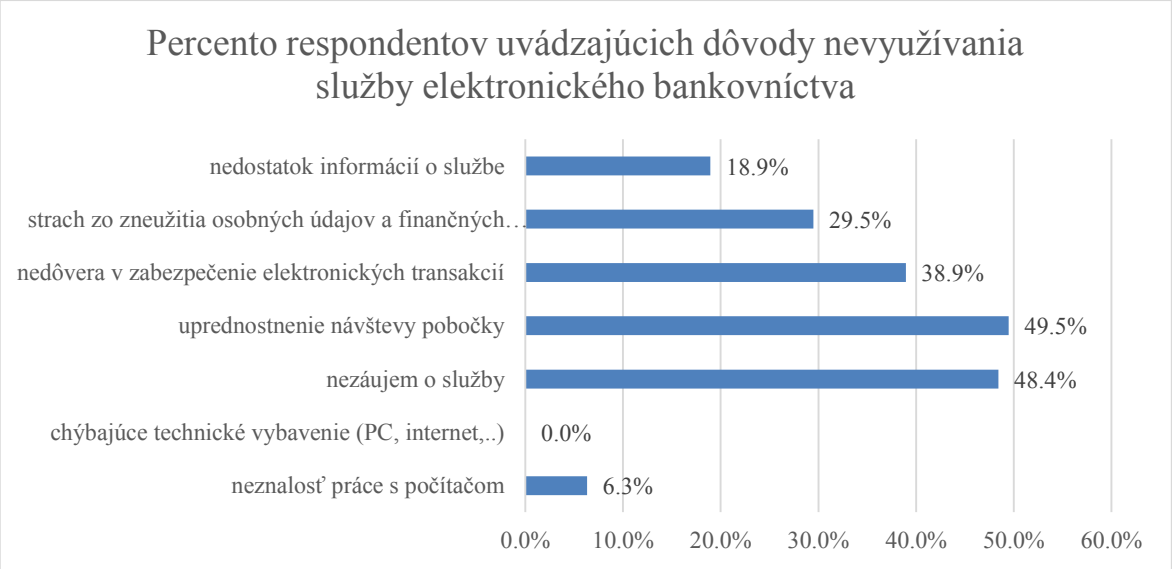
Tab. 3. Respondenti nevyužívajúci služby elektronického bankovníctva vzhľadom na vekovú skupinu, sociálny status a najvyššie ukončené vzdelanie [zdroj vlastný]

Veková skupina	Sociálny status	Najvyššie ukončené vzdelanie	Percento
15 - 24 rokov	**študent**	**základné**	**58,9%**
15 - 24 rokov	študent	stredoškolské bez maturity	2,1%
15 - 24 rokov	študent	stredoškolské s maturitou	2,1%
15 - 24 rokov	študent	vysokoškolské	2,1%
25 - 34 rokov	študent	vysokoškolské	2,1%
25 - 34 rokov	zamestnaný	vysokoškolské	2,1%
25 - 34 rokov	podnikateľ	stredoškolské s maturitou	1,1%
35 - 44 rokov	zamestnaný	vysokoškolské	2,1%
45 - 54 rokov	**zamestnaný**	**vysokoškolské**	**8,4%**
45 - 54 rokov	nezamestnaný	vysokoškolské	1,1%
45 - 54 rokov	podnikateľ	vysokoškolské	1,1%
nad 54 rokov	**zamestnaný**	**stredoškolské s maturitou**	**7,4%**
nad 54 rokov	zamestnaný	vysokoškolské	1,1%
nad 54 rokov	dôchodca	stredoškolské s maturitou	1,1%
nad 54 rokov	**dôchodca**	**vysokoškolské**	**7,4%**

Sekcia: Elektronické bankovníctvo - nie

Otázka: Ak nevyužívate služby elektronického bankovníctva, aký máte dôvod? (vyznačte max 3 možnosti)

Od respondentov, ktorí nevyužívajú služby elektronického bankovníctva, bolo zaujímavé zistiť, aké sú dôvody, ktoré ich k tomu vedú. Bolo možné uviesť viacero odpovedí (max 3). Po tejto otázke bol dotazník pre túto skupinu respondentov ukončený.



Obr. 19. Dôvody nevyužívania elektronického bankovníctva [zdroj vlastný]

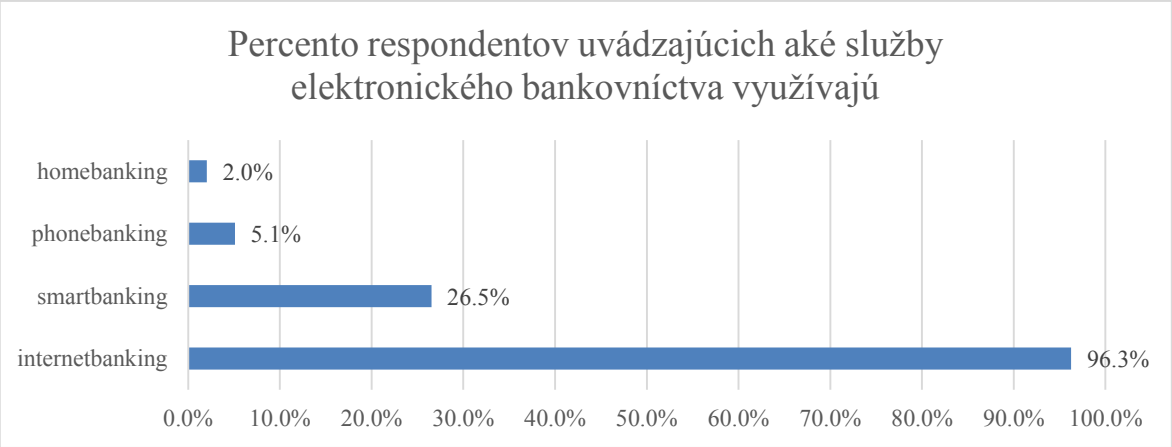
Z grafu vyplýva, že najčastejšie dôvody nevyužívania služby elektronického bankovníctva sú uprednostnenie návštevy pobočky (49,5%) a nezáujem o služby (48,4%). Ďalšími dôvodmi sú nedôvera v zabezpečenie elektronických transakcií (38,9%), strach zo zneužitia osobných údajov a finančných prostriedkov (29,5%), nedostatok informácií o službe (18,9%) a nakoniec neznalosť práce s počítačom (6,3%). Nikto z respondentov neuviedol chýbajúce technické vybavenie.

Sekcia: Elektronické bankovníctvo - áno

V prípade 294 respondentov, ktorí využívajú služby elektronického bankovníctva, sa skúmali ďalšie oblasti spojené s týmito službami – aké služby využívajú, ako často ich využívajú, z akých zariadení pristupujú do svojho elektronického bankovníctva, či sa obávajú rizika zneužitia prihlasovacích údajov, čo si myslia o zabezpečení internetbankingu a mobilných aplikácií, aké autentizačné prvky využívajú pre prístup na svoj bankový účet, či pristupujú k citlivým dátam cez verejné nezabezpečené wifi siete a ako si chránia prihlasovacie údaje do internetbankingu.

Otázka: Aké služby elektronického bankovníctva využívate?

Otázka zisťovala, aké konkrétne služby elektronického bankovníctva využívajú respondenti najčastejšie, pričom respondent mal možnosť zvoliť viacero odpovedí. Na výber boli základné typy prístupu pomocou rôznych komunikačných kanálov.

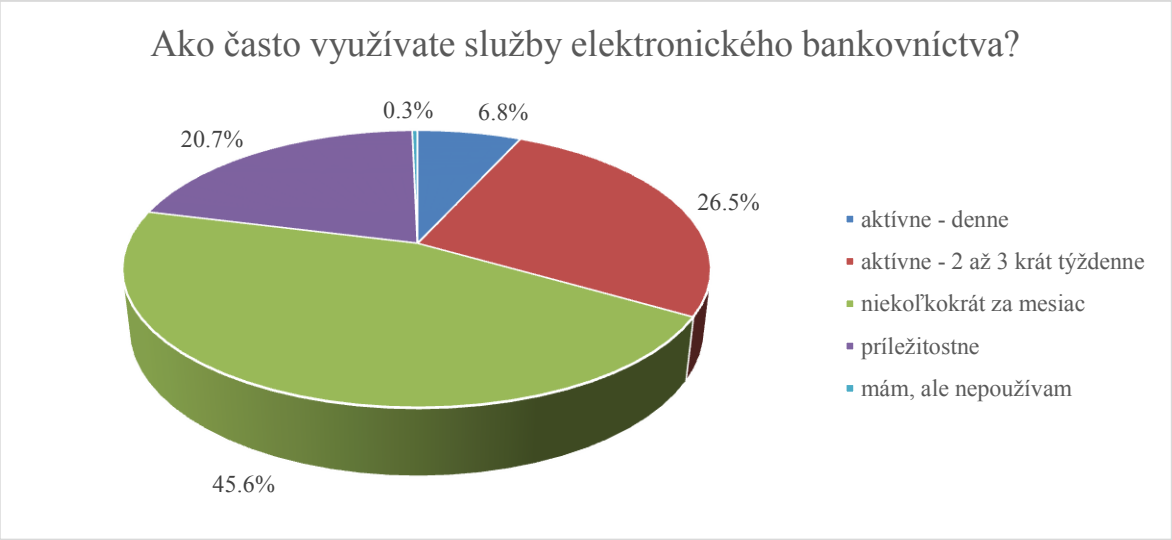


Obr. 20. Využívané služby elektronického bankovníctva [zdroj vlastný]

Až 96,3% respondentov uviedlo, že využíva internetbanking a 26,5% respondentov pristupuje k svojmu účtu prostredníctvom chytrého telefónu. Malé uplatnenie má phonebanking s 5,1% a iba 2,0% respondentov využíva homebanking.

Otázka: Ako často využívate služby elektronického bankovníctva?

Touto otázkou sa mapovala frekvencia využívania služieb elektronického bankovníctva. Najviac opýtaných (45,6%) uviedlo, že využíva služby elektronického bankovníctva niekoľkokrát za mesiac. Pomerne aktívne využíva služby 26,5% respondentov a príležitostne 20,7%. Na dennej báze využíva služby elektronického bankovníctva 6,8% respondentov.



Obr. 21. Frekvencia využívania elektronického bankovníctva [zdroj vlastný]

Bližšie je preskúmaná a stotožnená najpočetnejšia skupina 134 respondentov, ktorí využívajú služby elektronického bankovníctva niekoľkokrát za mesiac. Nasledujúca tabuľka ukazuje prehľadný rozpis percenta týchto respondentov vzhľadom na vekovú skupinu, sociálny status a najvyššie ukončené vzdelanie.

Tab. 4. Respondenti využívajúci elektronické bankovníctvo niekoľkokrát za mesiac vzhľadom na vekovú skupinu, sociálny status a najvyššie ukončené vzdelanie [zdroj vlastný]

Veková skupina	Sociálny status	Najvyššie ukončené vzdelanie	Percento
15 - 24 rokov	**študent**	**základné**	**9,0%**
15 - 24 rokov	**študent**	**stredoškolské s maturitou**	**7,5%**
15 - 24 rokov	študent	vysokoškolské	4,5%
25 - 34 rokov	študent	stredoškolské s maturitou	0,7%
25 - 34 rokov	študent	vysokoškolské	1,5%
25 - 34 rokov	**zamestnaný**	**vysokoškolské**	**9,7%**
25 - 34 rokov	nezamestnaný	vysokoškolské	0,7%
25 - 34 rokov	materská dovolenka	vysokoškolské	3,0%
35 - 44 rokov	študent	vysokoškolské	0,7%
35 - 44 rokov	**zamestnaný**	**vysokoškolské**	**16,4%**
35 - 44 rokov	podnikateľ	vysokoškolské	0,7%
45 - 54 rokov	zamestnaný	stredoškolské s maturitou	0,7%
45 - 54 rokov	**zamestnaný**	**vysokoškolské**	**21,6%**
45 - 54 rokov	podnikateľ	stredoškolské s maturitou	0,7%
45 - 54 rokov	podnikateľ	vysokoškolské	2,2%
nad 54 rokov	zamestnaný	stredoškolské s maturitou	3,0%

nad 54 rokov	**zamestnaný**	**vysokoškolské**	**9,0%**
nad 54 rokov	podnikateľ	stredoškolské s maturitou	0,7%
nad 54 rokov	podnikateľ	vysokoškolské	1,5%
nad 54 rokov	dôchodca	stredoškolské s maturitou	3,0%
nad 54 rokov	dôchodca	vysokoškolské	3,0%

Otázka: Z akých zariadení pristupujete do svojho elektronického bankovníctva?

Cieľom otázky bolo zistiť najčastejšie používané zariadenia pre prístup do elektronického bankovníctva. Opäť bolo možné uviesť aj viacero možností.

Z tabuľky je zrejmé, že najčastejšie využívaným prostriedkom pre prístup do elektronického bankovníctva je notebook, ktorý uviedlo až 71,8% respondentov. Značné zastúpenie má aj stolný počítač (47,6%) a tretí v poradí mobil/smartphone (36,7%). Na poslednom mieste je tablet, ktorý používa iba 8,8% respondentov.

Tab. 5. Zoznam zariadení pre prístup do elektronického bankovníctva [zdroj vlastný]

Zariadenie	**Percento respondentov**	**Počet respondentov**
mobil/smartphone	36,7%	108
tablet	8,8%	26
notebook	71,8%	211
stolný počítač	47,6%	140

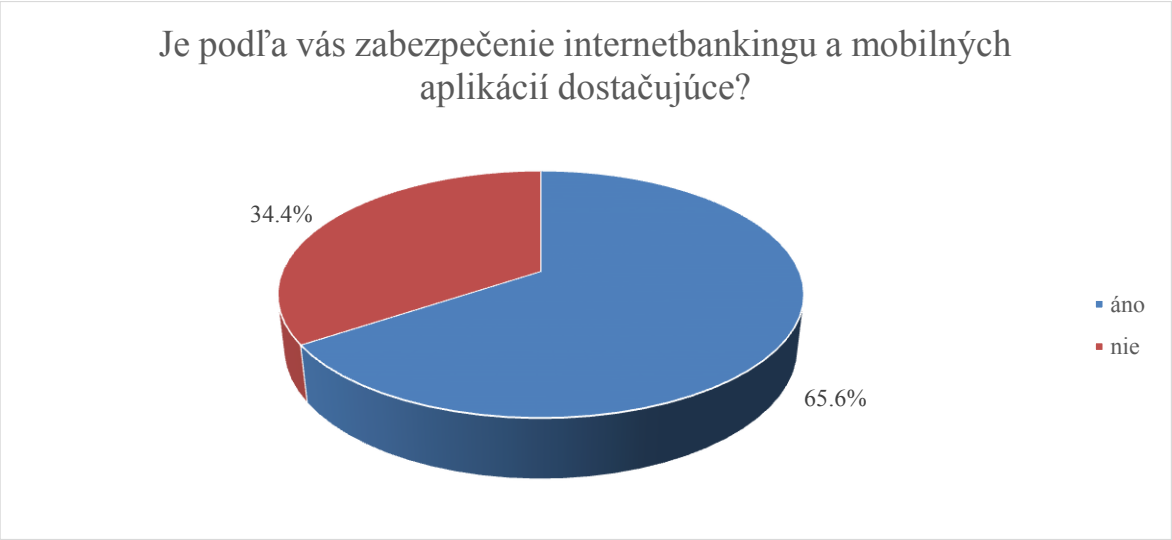
Otázka: Obávate sa rizika zneužitia prihlasovacích údajov k svojmu bankovému účtu?

Cieľom otázky bolo zistiť, či sa respondenti obávajú rizika zneužitia prihlasovacích údajov k svojmu bankovému účtu. Z 294 respondentov, ktorí sa vyjadrili k tejto otázke sa až 46,9% z nich obáva zneužitia svojich prihlasovacích údajov k bankovému účtu a naopak 53,1% respondentov sa tohto rizika neobáva.

Obr. 22. Obava zneužitia prihlasovacích údajov [zdroj vlastný]

Otázka: Je podľa vás zabezpečenie internetbankingu a mobilných aplikácií dostačujúce?

Cieľom otázky bolo zistiť, čo si myslia respondenti ohľadne zabezpečenia internetbankingu a mobilných aplikácií, ktoré používajú. Výrazná väčšina 65,6% respondentov si myslí, že zabezpečenia internetbankingu a mobilných aplikácií je dostačujúce a naopak 34,4% respondentov sa domnieva, že zabezpečenie nie je na dostačujúcej úrovni.



Obr. 23. Zabezpečenie internetbankingu a mobilných aplikácií [zdroj vlastný]

Otázka: Aké autentizačné prvky prístupu na svoj bankový účet využívate?

Otázka mapovala, ktoré autentizačné prvky a metódy prístupu na svoj bankový účet používajú respondenti najčastejšie, pričom jeden respondent mohol uviesť aj viacero autentizačných techník. Na výber bola široká škála autentizačných nástrojov, ktoré sú uvedené v priloženej tabuľke.

Tab. 6. Autentizačné prvky [zdroj vlastný]

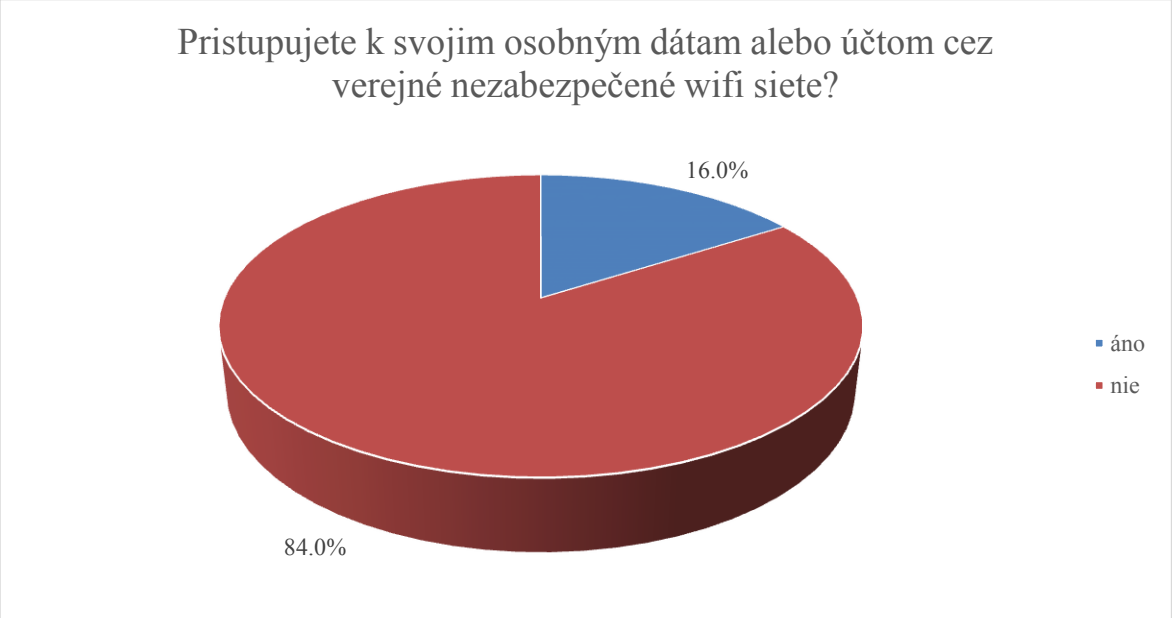
Autentizačný prvok	Percento respondentov
prihlasovacie meno a heslo	93,5%
SMS kľúč	56,8%
GRID karta	25,2%
certifikát	6,1%
čipová karta	6,8%
autorizačná kalkulačka	16,0%
biometrické prvky (otlačok prsta)	4,4%
generátor kódu pomocou mobilnej aplikácie	11,9%
iné	2,7%

Skoro všetci respondenti uviedli, že ako základný autentizačný prvok pre prístup na svoj bankový účet používajú prihlasovacie meno a heslo (93,5%). Na druhom mieste je autentizácia pomocou SMS kľúča (56,8%), ktorá slúži ako ďalšia úroveň overenia. Tretí najčastejšie používaný autentizačný prvok je GRID karta (25,2%), štvrtým je autorizačná kalkulačka (16,0%) a piatym generátor kódu pomocou mobilnej aplikácie (11,9%). V menšej miere sa používajú autentizačné prvky čipová karta (6,8%), certifikát (6,1%), biometrické prvky (4,4%) a prípadne iné (2,7%).

Zároveň sa ukázalo, že až 19,5% respondentov používa iba jeden autentizačný prvok, pričom najčastejšie sa jedná o prihlasovacie meno a heslo. Práve dva autentizačné prvky používa najväčšia skupina 52,6% respondentov, pričom ide o rôzne kombinácie, ale najviac používanou dvojicou autentizačných prvkov sú prihlasovacie meno a heslo a SMS kľúč. Posledná významná skupina 20,1% respondentov používa až tri autentizačné prvky, pričom ide opäť o rôzne kombinácie. Najviac používanou trojicou autentizačných prvkov sú prihlasovacie meno a heslo, SMS kľúč a GRID karta. Zvyšok opýtaných dokonca uviedlo, že využívajú aspoň štyri rôzne autentizačné prvky.

Otázka: Pristupujete k svojim osobným dátam alebo účtom cez verejné nezabezpečené wifi siete?

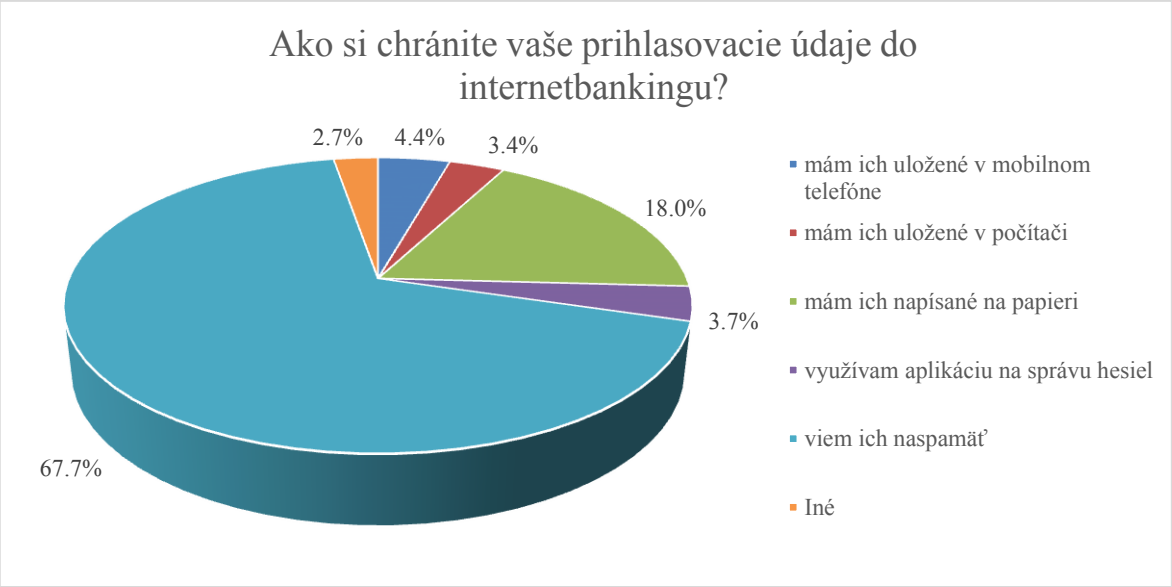
Cieľom otázky bolo zistiť, či respondenti pristupujú k svojim osobným dátam alebo účtom cez verejné nezabezpečené wifi siete. Ukázalo sa, že až 84,0% respondentov nevyužíva verejné nezabezpečené wifi siete na tento účel. Naopak 16,0% respondentov s nezabezpečeným pripojením problém nemá.



Obr. 24. Verejné nezabezpečené wifi siete [zdroj vlastný]

Otázka: Ako si chránite vaše prihlasovacie údaje do internetbankingu?

Otázka o ochrane prihlasovacích údajov má odhaliť nedostatky pri zabezpečení týchto citlivých informácií. Až 67,7% respondentov vie svoje prihlasovacie údaje do internetbankingu naspamäť. Rizikovou skupinou je 18,0% respondentov, ktorí majú svoje prihlasovacie údaje napísané na papieri, ďalej 4,4% respondentov s uloženými údajmi vo svojom mobilnom telefóne a 3,4% s uložením v počítači. Potenciál aplikácie na správu hesiel využíva len 3,7% respondentov. Zvyšných 2,7% respondentov uviedlo iné možnosti, ako si chránia svoje prihlasovacie údaje do internetbankingu.



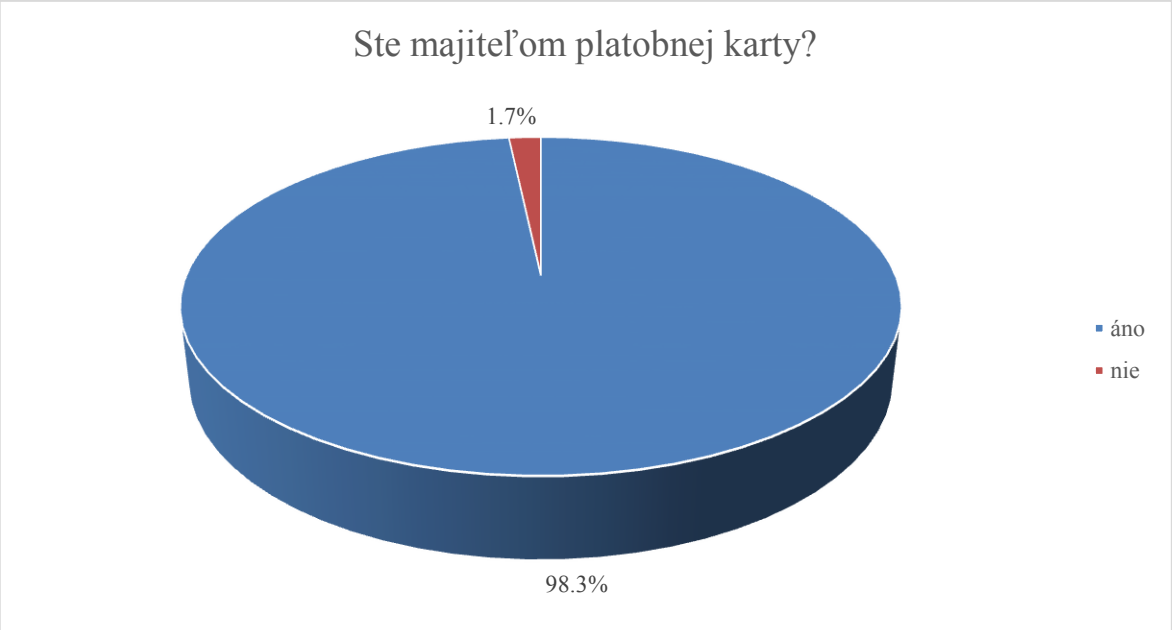
Obr. 25. Ochrana prihlasovacích údajov [zdroj vlastný]

Časť IV – Platobné karty

Táto časť prieskumu je zameraná na otázky týkajúce sa platobných kariet, t.j. či respondenti sú majiteľmi platobnej karty alebo nie. Nasledujúce štyri otázky zisťujú rôzne aspekty spojené s využívaním platobných kariet. Respondenti, ktorí nie sú majiteľmi platobnej karty, sú presmerovaní na sekciu Bezpečnostné prvky a riziká a neodpovedajú na otázky týkajúce sa platobných kariet.

Otázka: Ste majiteľom platobnej karty?

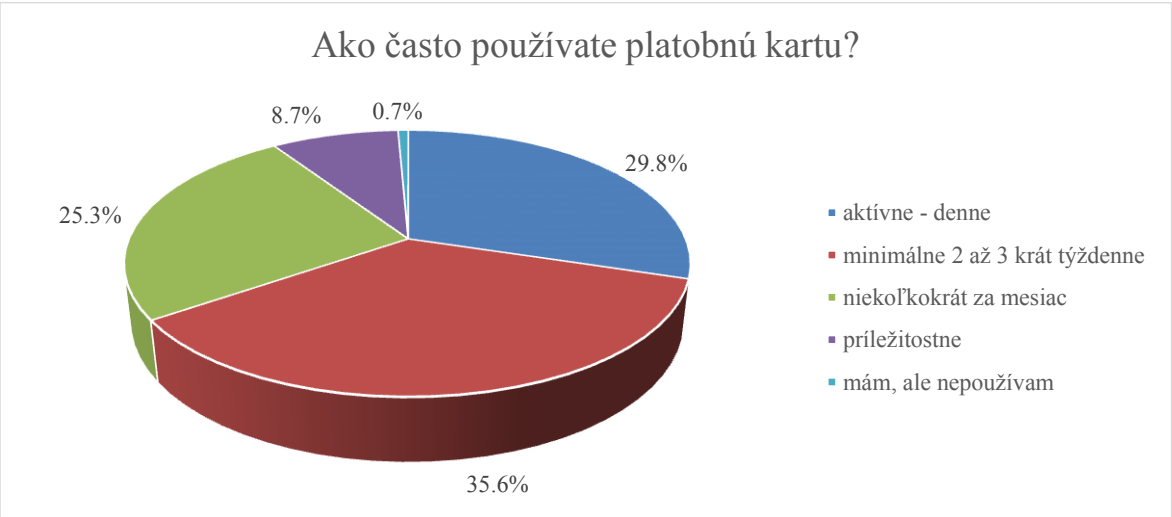
Z 294 opýtaných je až 98,3% respondentov majiteľom platobnej karty a iba 1,7% respondentov uviedlo, že platobnú kartu nevlastní.



Obr. 26. Platobné karty [zdroj vlastný]

Otázka: Ako často používate platobnú kartu?

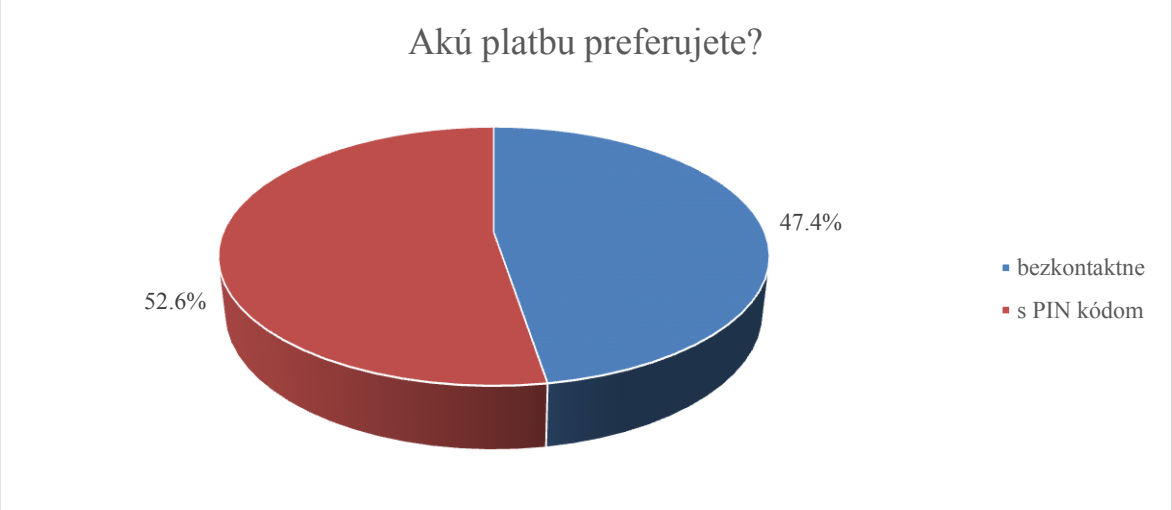
Táto otázka mala za cieľ zistiť, ako často respondenti používajú svoju platobnú kartu. Z výsledkov je zjavné, že platobná karta je obľúbený a často využívaný prostriedok platenia. Minimálne 2 až 3-krát týždenne ju používa 35,6% respondentov. Veľmi aktívnych je 29,8% respondentov, ktorí ju používajú dokonca každý deň. Frekvenciu používania niekoľkokrát za mesiac uviedlo 25,3% respondentov a príležitostne 8,7% respondentov.



Obr. 27. Frekvencia používania platobnej karty [zdroj vlastný]

Otázka: Akú platbu preferujete?

S nástupom bezkontaktných technológií je zaujímavé zistiť preferencie respondentov pri platení platobnou kartou. Pri bezkontaktnej platbe nie je nutné do čiastky 500 Kč zadávať PIN, čo môže byť odradzujúcim faktorom, kvôli riziku zneužitia.



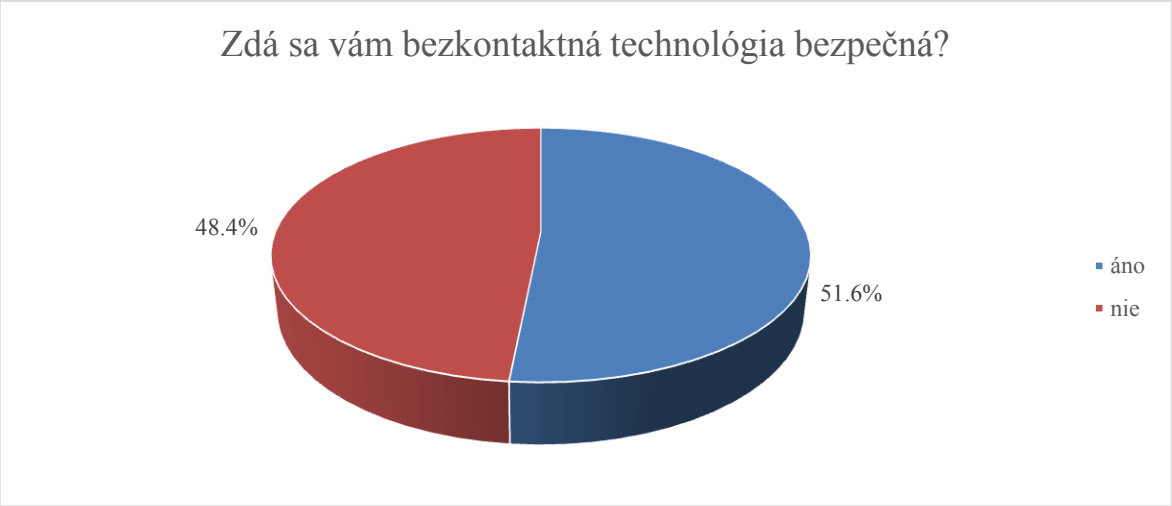
Obr. 28. Frekvencia platby s platobnou kartou [zdroj vlastný]

Ukázalo sa, že respondenti preferujú približne v rovnakom pomere platbu s použitím PIN kódu (52,6%) i bezkontaktnú platbu (47,4%) a to bez ohľadu na vekovú skupinu, sociálny status alebo najvyššie ukončené vzdelanie.

Otázka: Zdá sa Vám bezkontaktná technológia bezpečná?

Cieľom otázky bolo zistiť, či respondenti považujú bezkontaktnú technológiu používanú v platobných kartách za bezpečnú, alebo nie.

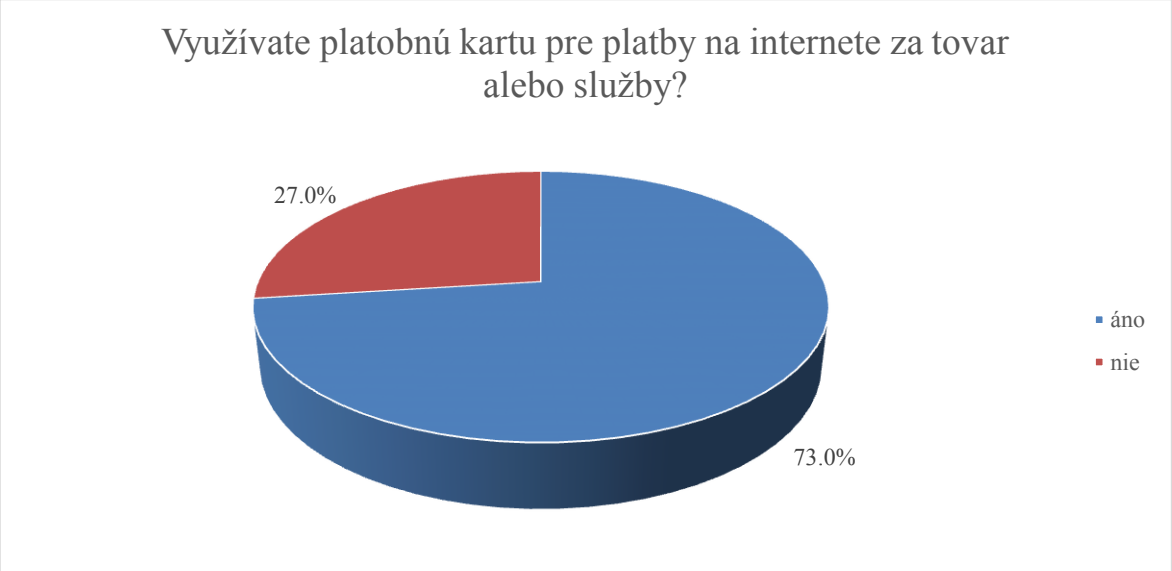
Odpovede ukázali názorové rozdelenie respondentov skoro presne na polovicu. 51,6% respondentov pokladá bezkontaktnú technológiu za bezpečnú a zvyšných 48,4% respondentov má na túto problematiku opačný názor.



Obr. 29. Bezpečnosť bezkontaktnej technológie [zdroj vlastný]

Otázka: Využívate platobnú kartu pre platby na internete za tovar alebo služby?

Cieľom otázky bolo zistiť, či respondenti využívajú platobnú kartu aj pre platby na internete za tovar alebo služby, kde je potrebné uvádzať číslo karty, dátum ukončenia platnosti a CVC/CVV kód. Až 73,0% respondentov sa vyjadrilo, že využíva platobnú kartu pre platby na internete za tovar alebo služby. Zvyšných 27,0% respondentov túto možnosť nevyužíva, prípadne môže mať svoju kartu pre platby na internete blokovanú.



Obr. 30. Platby na internete [zdroj vlastný]

Časť V – Bezpečnostné prvky a riziká

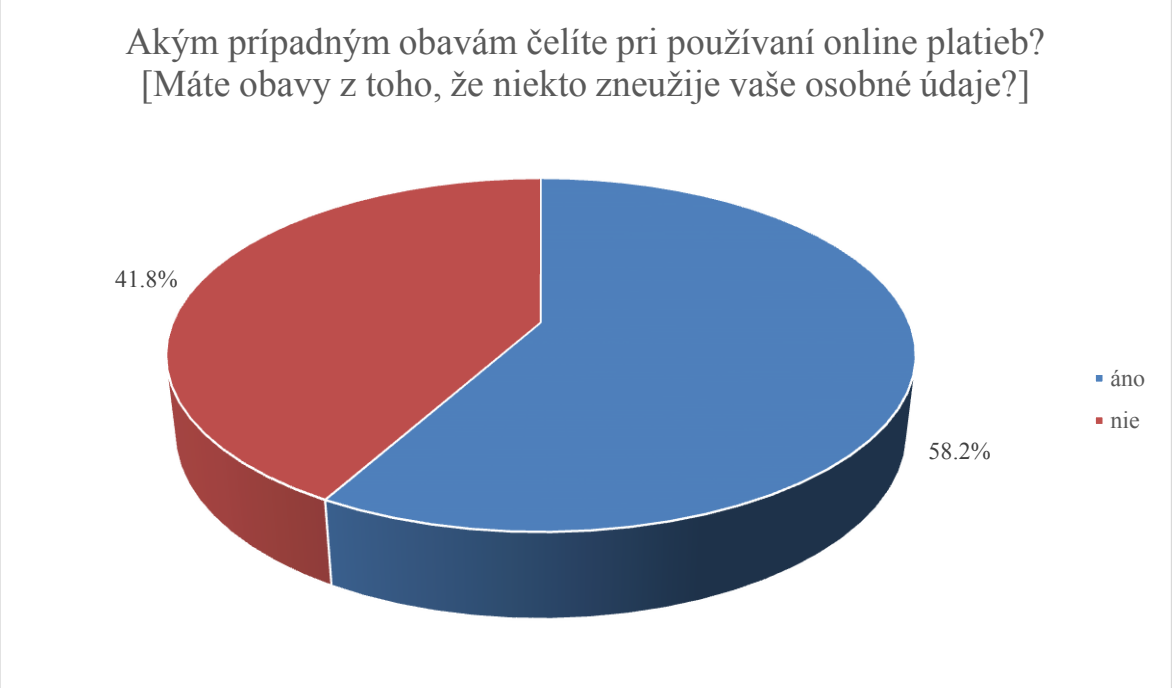
Cieľom tejto časti prieskumu je zistiť, či respondenti vnímajú riziká spojené s online platbami, či sa obávajú zneužitia, resp. odcudzenia osobných údajov alebo finančných prostriedkov. Aké rôzne možnosti ochrany používajú, či sa už osobne alebo vo svojom blízkom okolí stretli s nejakými internetovými hrozbami a či by šírenie osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch nemalo byť väčšie a intenzívnejšie.

Otázka: Akým prípadným obavám čelíte pri používaní online platieb?

Táto otázka obsahuje 3 podotázky:

- Máte obavy z toho, že niekto zneužije vaše osobné údaje?
- Máte obavy z bezpečnosti a rizika odcudzenia vašich finančných prostriedkov?
- Máte obavy, že nedostanete službu/tovar, ktoré si kúpite online?

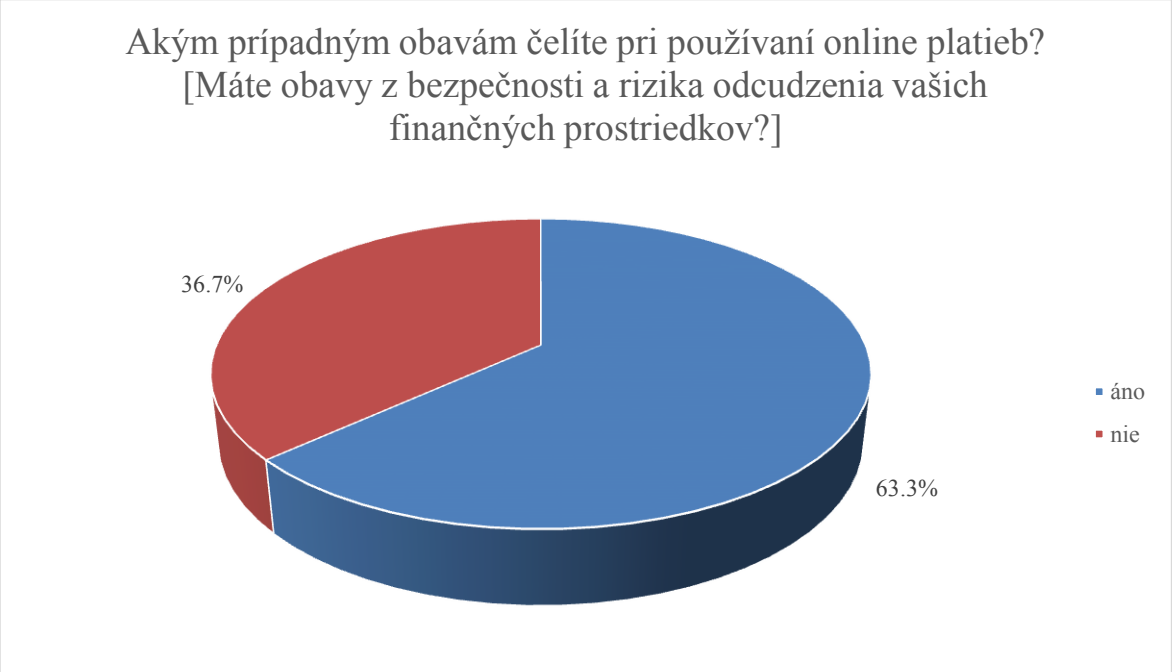
Cieľom prvej podotázky bolo zistiť, či respondenti majú obavy z toho, že niekto zneužije ich osobné údaje.



Obr. 31. Obavy zo zneužitia údajov [zdroj vlastný]

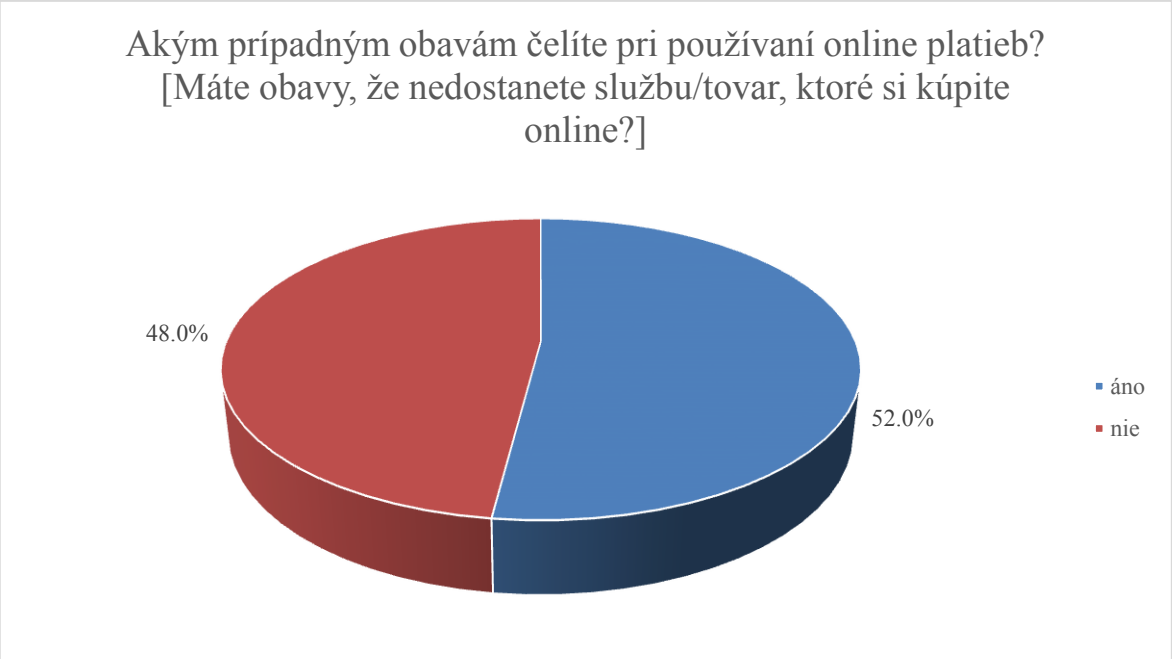
Pomerne prekvapivo až 58,2% respondentov má obavy zo zneužitia svojich osobných údajov a naopak 41,8% respondentov sa tohto rizika neobáva.

Druhá podotázka sa zamerala na obavy respondentov z bezpečnosti a rizika odcudzenia ich finančných prostriedkov. V tomto prípade sa počet ľudí, ktorí majú obavy z bezpečnosti a rizika straty finančných prostriedkov ešte zvýšil. Až 63,3% respondentov považuje toto riziko sa opodstatnené. Naopak 36,7% opýtaných sa s týmito obavami nestotožňuje.



Obr. 32. Obavy z odcudzenia finančných prostriedkov [zdroj vlastný]

Posledná podotázka zisťuje obavy respondentov z toho, že nedostanú službu alebo tovar, ktoré si zakúpia online. Takéto prípady sa bohužiaľ vyskytujú, a preto sa odporúča nakupovať primárne vo veľkých a overených internetových obchodoch, kde je toto riziko minimálne. Pri prvom nákupe v neznámom internetovom obchode je rozumné si prečítať recenzie ľudí, ktorí v ňom už nakúpili a zároveň sa vyhnúť platbe dopredu. Týmto prístupom sa dá pomerne jednoducho vyvarovať nežiaducim následkom.

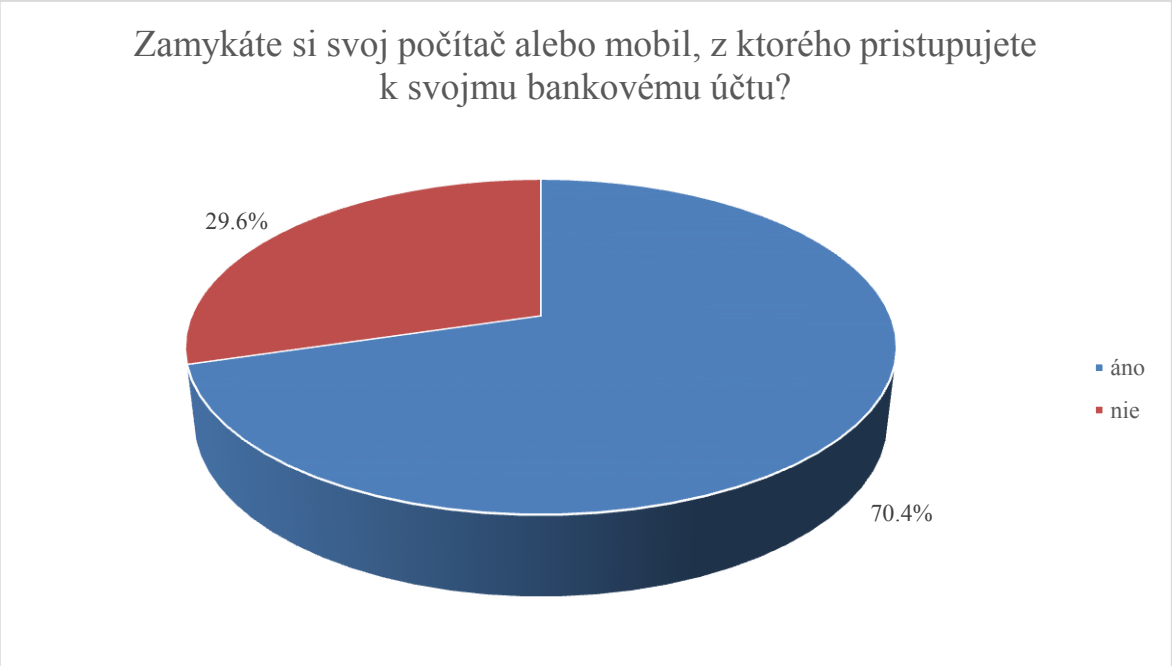


Obr. 33. Obavy z nedodania tovaru alebo služieb [zdroj vlastný]

Opäť viac ako polovica respondentov (52,0%) má obavy z rizika, že nedostanú zakúpenú službu alebo tovar. Zvyšných 48,0% respondentov tieto obavy nepovažuje za opodstatnené.

Otázka: Zamykáte si svoj počítač alebo mobil, z ktorého pristupujete k svojmu bankovému účtu?

Cieľom otázky bolo zistiť, či si respondenti chránia svoj počítač alebo mobil, z ktorého pristupujú k svojmu bankovému účtu tým, že si ho zamykajú. Ukázalo sa, že 70,4% respondentov si zamyká svoj počítač alebo mobil, z ktorého pristupujú k svojmu bankovému účtu. Ale stále je veľká skupina 29,6% respondentov, ktorí zanedbávajú túto základnú ochranu a svoj počítač alebo mobil si nezamykajú.



Obr. 34. Zamykanie počítača a mobilu [zdroj vlastný]

Vzťah respondentov, ktorí si zamykajú, resp. nezamykajú svoj počítač alebo mobil, z ktorého pristupujú k svojmu bankovému účtu vzhľadom na vekovú skupinu a sociálny status zobrazujú v prehľadnom porovnaní nasledujúce dve tabuľky.

Tab. 7. Zamykanie počítača a mobilu podľa veku [zdroj vlastný]

Veková skupina	Zamykáte si svoj počítač alebo mobil, z ktorého pristupujete k svojmu bankovému účtu?	Percento
15 - 24 rokov	áno	19,7%
	nie	3,1%
25 - 34 rokov	áno	12,9%
	nie	2,7%
35 - 44 rokov	áno	12,9%
	nie	4,4%
45 - 54 rokov	áno	15,0%
	nie	11,2%
nad 54 rokov	áno	9,9%
	nie	8,2%

Z tabuľky je vidieť, že v mladších generáciách, vo vekových skupinách 15 – 24 rokov, 25 – 34 rokov a 35 – 44 rokov výrazne prevažujú respondenti, ktorí si svoj počítač alebo mobil zamykajú. V starších vekových skupinách 45 – 54 rokov a nad 54 rokov je tento pomer približne rovnaký.

Tab. 8. Zamykanie počítača a mobilu podľa sociálneho statusu [zdroj vlastný]

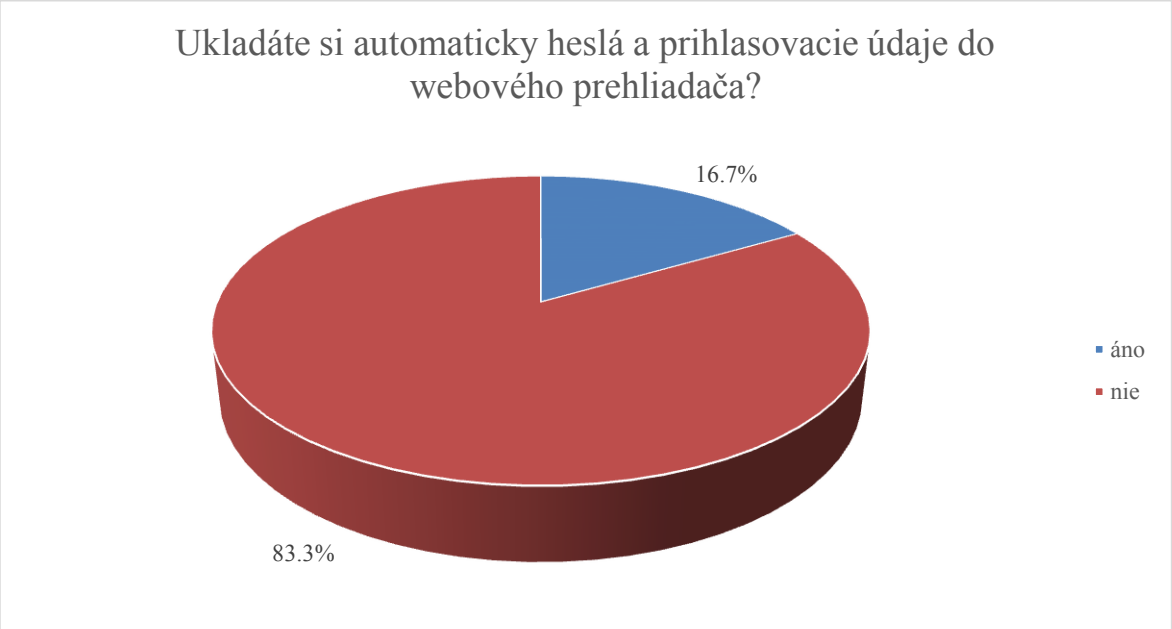
Sociálny status	Zamykáte si svoj počítač alebo mobil, z ktorého pristupujete k svojmu bankovému účtu?	Percento
študent	áno	20,4%
	nie	3,4%
zamestnaný	áno	40,8%
	nie	19,4%
nezamestnaný	áno	0,7%
	nie	0,3%
podnikateľ	áno	5,1%
	nie	2,7%
dôchodca	áno	1,7%
	nie	3,1%
materská dovolenka	áno	1,7%
	nie	0,7%

Z tabuľky je evidentné, že študenti si v najväčšej miere chránia svoje zariadenia, pretože až 6-krát viac študentov odpovedalo na položenú otázku „áno“ oproti tým, ktorí odpovedali „nie“. V skupinách zamestnaných, nezamestnaných, podnikateľov a respondentov na materskej dovolenke odpovedalo na položenú otázku „áno“ približne 2-krát viac respondentov ako tých, ktorí odpovedali „nie“. Opačný pomer je v skupine dôchodcov, kde odpovedalo na položenú otázku „nie“ približne 2-krát viac respondentov ako tých, ktorí odpovedali „áno“.

Otázka: Ukladáte si automaticky heslá a prihlasovacie údaje do webového prehliadača?

Cieľom otázky bolo zistiť, či respondenti používajú automatické ukladanie hesiel a prihlasovacích údajov do webového prehliadača, čím uľahčujú pri prípadnom odcudzení zariadenia priamy prístup k svojim účtom. Ukázalo sa, že 83,3% respondentov je obozretných a neukladá si automaticky heslá a prihlasovacie údaje do webového prehliadača. Ale

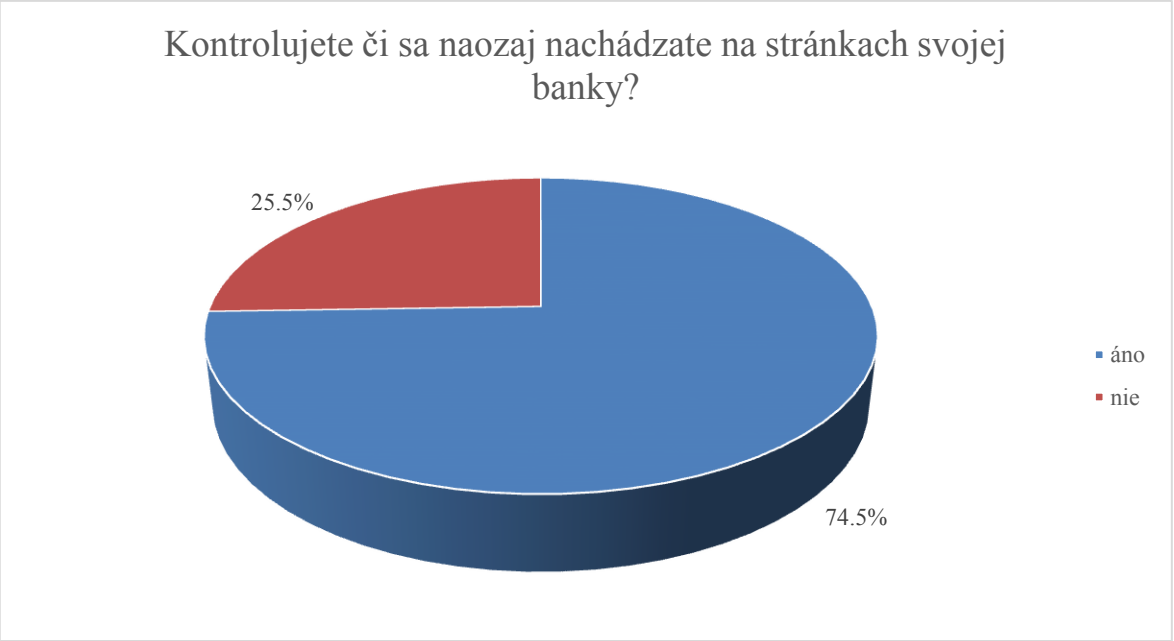
stále je tu skupina 16,7% respondentov, ktorí využívajú automatické ukladanie hesiel a prihlasovacích údajov a nepovažujú toto počínanie za rizikové.



Obr. 35. Automatické ukladanie hesiel [zdroj vlastný]

Otázka: Kontrolujete, či sa naozaj nachádzate na stránkach svojej banky?

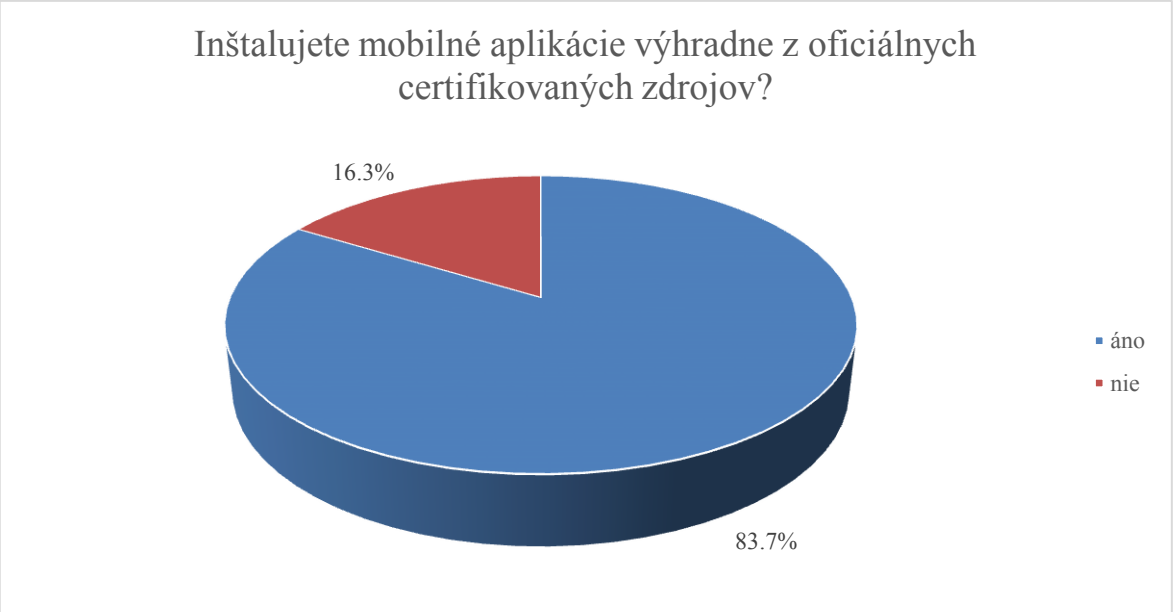
Cieľom otázky bolo zistiť, či respondenti kontrolujú, že sa naozaj nachádzajú na stránkach svojej banky, t.j. či adresa URL začína „https:“, resp. podľa symbolu visiaceho zámku. Je povzbudivé, že 74,5% respondentov si to kontroluje, čím predchádza možným hrozbám vloženia svojich prihlasovacích údajov na podvrhnutú falošnú stránku a teda ich odcudzeniu a zneužitiu. Ale stále štvrtina respondentov (25,5%) si tieto bezpečnostné prvky nekontroluje a tým môže ohroziť svoje osobné údaje a aj finančné prostriedky.



Obr. 36. Kontrola stránky banky [zdroj vlastný]

Otázka: Inštalujete mobilné aplikácie výhradne z oficiálnych certifikovaných zdrojov (Apple Store, Google Play, Windows Store)?

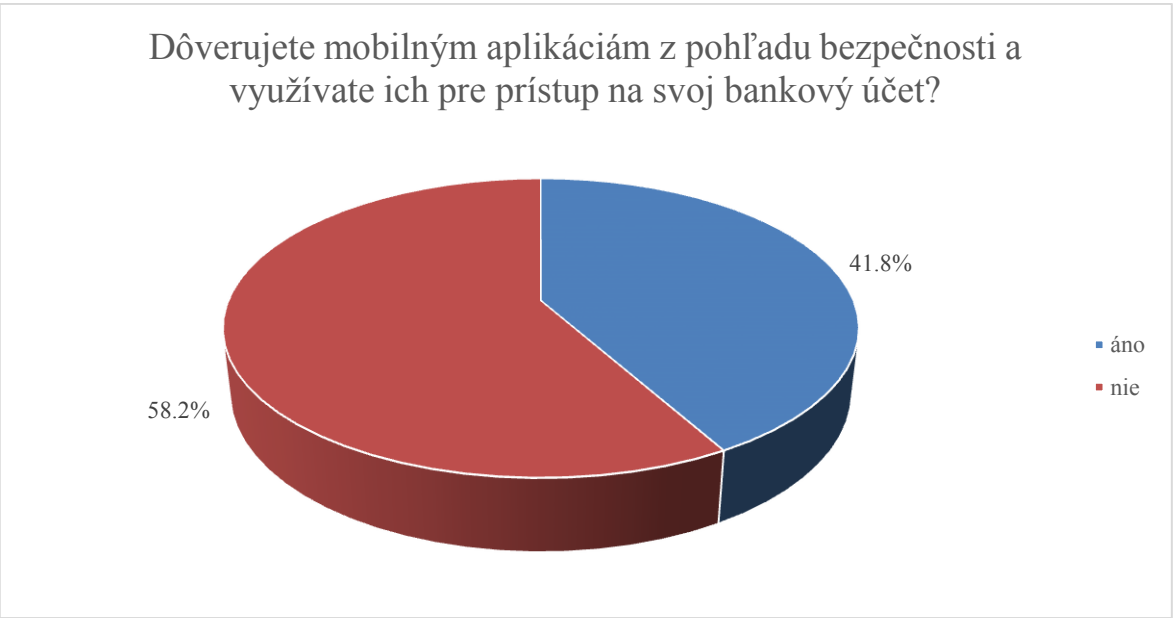
Zámerom otázky bolo vyzistiť, či si respondenti inštalujú mobilné aplikácie výhradne z oficiálnych certifikovaných zdrojov, čím sa chránia pred prípadným zavírením alebo nainštalovaním aplikácií, ktoré by mohli byť hrozbou. Je potešujúce, že až 83,7% respondentov inštaluje mobilné aplikácie výhradne z oficiálnych zdrojov a iba 16,3% respondentov používa aj aplikácie z neoverených a neoficiálnych kanálov.



Obr. 37. Inštalácia aplikácií z oficiálnych zdrojov [zdroj vlastný]

Otázka: Dôverujete mobilným aplikáciám z pohľadu bezpečnosti a využívate ich pre prístup na svoj bankový účet?

Otázka zisťovala dôveru respondentov v mobilné bankové aplikácie z pohľadu bezpečnosti. Bankové aplikácie sú najnovším trendom, ktorý sa rozšíril spolu s chytrými telefónmi.



Obr. 38. Dôvera v mobilné bankové aplikácie [zdroj vlastný]

Je zaujímavé, že iba 41,8% respondentov dôveruje mobilným aplikáciám z pohľadu bezpečnosti a využíva ich pre prístup na svoj bankový účet a až 58,2% im nedôveruje alebo ich nevyužíva.

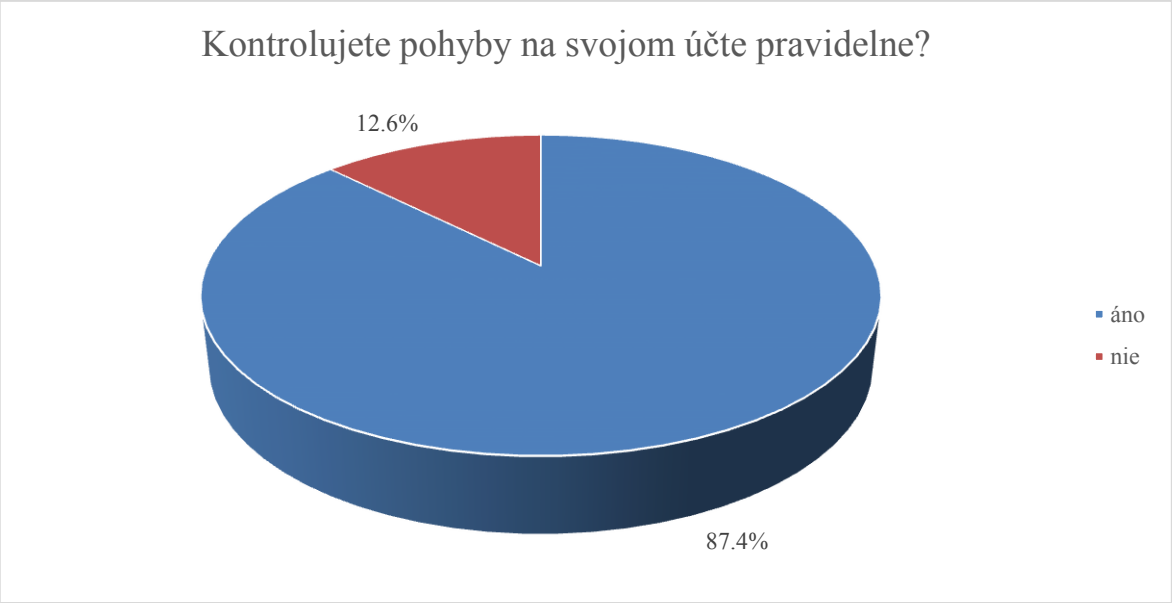
Otázka: Poskytli ste niekedy PIN alebo svoje prihlasovacie údaje tretím osobám?

Účel otázky mal za úlohu zistiť, či sa respondenti správajú bezpečne pri ochrane PIN kódu alebo svojich prihlasovacích údajov a neposkytujú tieto informácie tretím osobám. Výsledok prieskumu ukázal, že až 91,2% respondentov sa správa zodpovedne a chráni si svoje citlivé údaje. Minoritná skupina 8,8% respondentov poskytla už niekedy tieto citlivé údaje tretím osobám.

Obr. 39. Poskytnutie PINu tretím osobám [zdroj vlastný]

Otázka: Kontrolujete pohyby na svojom účte pravidelne?

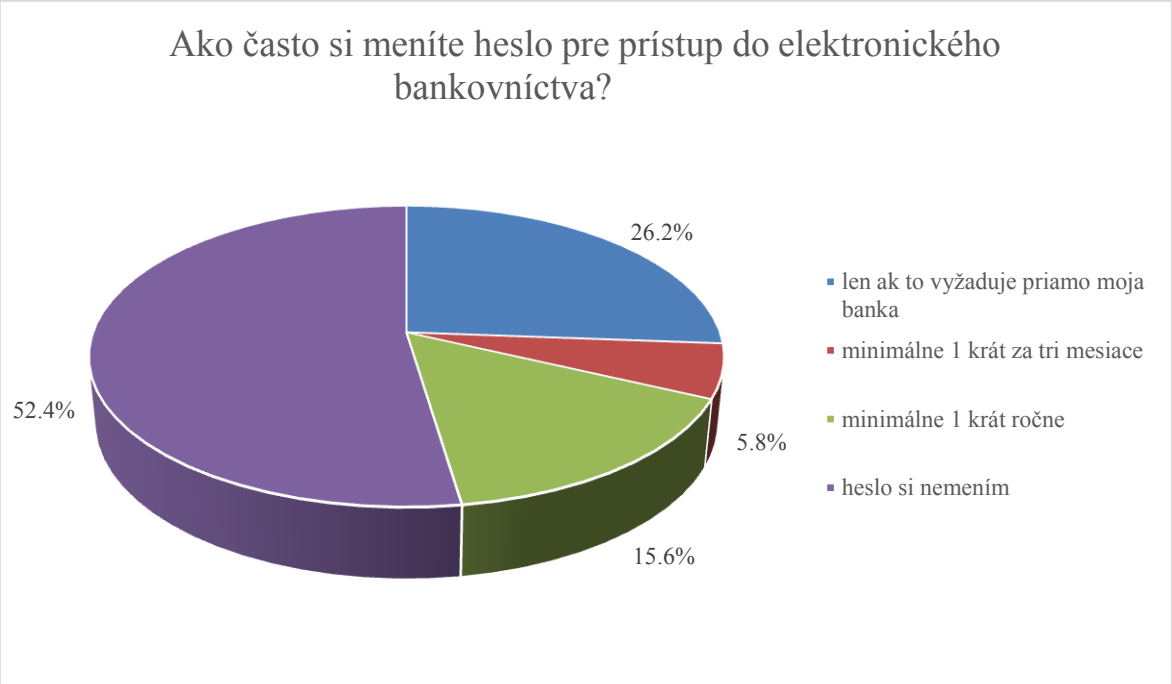
Otázka skúmala, či si respondenti kontrolujú históriu a pohyby na svojom účte pravidelne. Je povzbudivé, že až 87,4% respondentov uviedlo, že si pohyby na bankovom účte kontroluje pravidelne. Pravidelná kontrola môže pomôcť odhaliť podozrivú transakciu a zabrániť ďalšiemu zneužitiu. Zostávajúcich 12,6% respondentov si pohyby na svojom účte pravidelne nekontroluje.



Obr. 40. Kontrola pohybov na účte [zdroj vlastný]

Otázka: Ako často si meníte heslo pre prístup do elektronického bankovníctva?

Cieľom otázky bolo zistiť, či si respondenti menia svoje heslo pre prístup do elektronického bankovníctva a s akou frekvenciou. Ukázalo sa, že v tomto smere existujú veľké nedostatky, keďže až 52,4% respondentov si svoje heslo nemení vôbec a druhá najpočetnejšia skupina 26,2% respondentov ho mení len v prípade, keď to vyžaduje priamo ich banka. Ďalších 15,6% ho mení aspoň raz ročne a 5,8% minimálne raz za tri mesiace. Z pohľadu ochrany prístupu by zmena hesla mala byť v rozumnom časovom horizonte vyžadovaná priamo bankou.



Obr. 41. Frekvencia zmeny hesla [zdroj vlastný]

Otázka: S akými internetovými hrozbami ste sa už stretli osobne alebo vo svojom blízkom okolí?

Cieľom otázky bolo zistiť, či sa respondenti už niekedy stretli s uvedenými internetovými hrozbami osobne alebo vo svojom blízkom okolí.

Tab. 9. Internetové hrozby [zdroj vlastný]

Internetová hrozba	**Percento respondentov, ktorí sa stretli s danou hrozbou**
phishing (e-mailové útoky, ktorých cieľom je vylákať dôverné informácie)	42,5%
e-mail so zavírenou prílohou	55,4%
podvrhnutý falošný formulár na webe, snažiaci sa vylákať citlivé údaje	24,8%
ukradnutý účet (sociálna sieť, e-mail,...)	17,7%
útok na elektronické bankovníctvo	5,1%
zneužitie platobnej karty	18,0%
žiadna z uvedených	25,2%
iné	1,0%

Je zaujímavé, že až štvrtina opýtaných (25,2%) sa nestretla so žiadnou z uvedených internetových hrozieb. Najčastejšie prišli respondenti do kontaktu s e-mailom, ktorý obsahoval zavírenú prílohu (55,4%) a phishingovým útokom (42,5%). Až 24,8% respondentov sa stretlo s podvrhnutým falošným formulárom na webe a 17,7% s ukradnutým účtom (sociálna sieť, e-mail). Zneužitie platobnej karty uvádza 18,0% respondentov a útok na elektronické bankovníctvo iba nízky počet 5,1% respondentov. Medzi iné internetové hrozby, ktoré boli zmienené v dotazníku, patrí napríklad nebezpečný ransomware, ktorý zašifruje súbory v počítači a požaduje zaplatiť výkupné v kryptomene bitcoin.

V tejto otázke je zaujímavé aj porovnanie, s akým počtom internetových hrozieb sa jednotliví respondenti stretli. Z tabuľky nižšie vyplýva, že s práve jednou internetovou hrozbou sa stretlo 26,6% respondentov, s dvomi internetovými hrozbami prišlo už do kontaktu 22,1% respondentov a s tromi internetovými hrozbami 15,6% respondentov. Oveľa menej respondentov sa stretlo so štyrmi internetovými hrozbami (7,1%), s piatimi len 2,7% a so všetkými šiestimi 0,7% respondentov.

Tab. 10. Počet internetových hrozieb [zdroj vlastný]

Počet internetových hrozieb	Percento respondentov
žiadna z uvedených internetových hrozieb	25,2%
1 internetová hrozba	26,6%
2 internetové hrozby	22,1%
3 internetové hrozby	15,6%
4 internetové hrozby	7,1%
5 internetových hrozieb	2,7%
6 internetových hrozieb	0,7%

Otázka: Aké opatrenia proti počítačovým útokom a hrozbám využívate?

Cieľom otázky bolo vyzistiť, aké bezpečnostné prvky a preventívne opatrenia využívajú respondenti proti počítačovým útokom a hrozbám.

Z odpovedí 294 opýtaných vyplýva, že antivírový softvér patrí medzi najhlavnejšie bezpečnostné opatrenia, uviedlo ho až 87,1% respondentov. Na druhom mieste je pravidelná aktualizácia operačného systému a aplikácií, ktorú aplikuje 56,5% respondentov. Necelá polovica 49,0% zálohuje svoje dôležité dáta. Najmenej opýtaných respondentov 10,9% má svoje kritické súbory zašifrované, čo už ale vyžaduje potrebné technické znalosti. Najkri-

tickejšou skupinou sú 4,4% respondentov, ktorí žiadne opatrenie proti počítačovým útokom alebo hrozbám nepoužívajú.

Tab. 11. Využívanie preventívnych opatrení [zdroj vlastný]

Preventívne opatrenie	Percento respondentov, ktorí využívajú dané opatrenie
antivírový softvér	87,1%
pravidelná aktualizácia operačného systému a aplikácií	56,5%
zálohovanie dát	49,0%
šifrovanie kritických súborov	10,9%
žiadne opatrenie nevyužívam	4,4%

6.3 Zhodnotenie a diskusia

Z prezentovaných výsledkov prieskumu vyplýva, že využívanie elektronického bankovníctva je veľmi aktívne a určite napomáha k uľahčeniu a zjednodušeniu komunikácie medzi bankou a jej klientmi. Na pomerne slušnej úrovni je celkové povedomie o bezpečnom vystupovaní v prostredí internetu. Základné opatrenia ako nepristupovať k svojim účtom cez nezabezpečené siete, neposkytovať PIN a prístupové údaje tretím osobám, kontrolovať si históriu operácií na účte, zamykať svoj počítať a mobil, neukladať si automaticky heslá v prehliadači a inštalovať aplikácie výhradne z oficiálnych zdrojov dodržuje veľká väčšina respondentov. Stále pretrvávajú rozšírené obavy o zneužití alebo odcudzení finančných prostriedkov a zároveň o celkové zabezpečenie kanálov elektronického bankovníctva.

Priestor na zlepšenie a zvýšenie úrovne ochrany je určite v pravidelnej zmene prístupových hesiel, či už k bankovému alebo aj ďalším osobným účtom v prostredí internetu. Namiesto potreby zapamätať si všetky heslá, alebo písať si ich v otvorenej forme na papier a do telefónu, sa javí ako najschodnejšie riešenie špeciálna aplikácia na správu hesiel. V takom prípade je nutné si zapamätať jedno jediné heslo a všetky ostatné sa nachádzajú v prehľadnej zašifrovanej databáze.

Ďalší priestor pre zlepšenie je v aplikácii viacerých preventívnych opatrení. Antivírusový software a pravidelná aktualizácia operačného systému by mala byť samozrejmosťou. Zá-

lohovanie dôležitých súborov je jednoduchým a efektívnym prostriedkom ako predísť nežiaducim problémom a ušetriť si veľa starostí.

Z pohľadu autentizačných a autorizačných metód sa výrazne odporúča použitie kombinácie aspoň dvoch overovacích prvkov (dvojfaktorová autentizácia), čím sa významne zvýši úroveň zabezpečenia.

7 PROGNÓZA BUDÚCEHO VÝVOJA

Budúci vývoj technologických inovácií v elektronickom bankovníctve má široké možnosti. Pre masové rozšírenie medzi širokú verejnosť je však potrebné, aby sa stretlo viacero faktorov. V prvom rade musí byť technológia pre banku rentabilná. Zároveň je potrebné, aby ju začali klienti reálne používať, či dokonca vyžadovať. Pre tento predpoklad je nutné, aby inovácia bola jednoduchá, praktická, rýchla a v rámci možností bezpečná. S nástupom a rozšírením stále modernejších chytrých telefónov sa záujem bánk výrazne zameriava práve na možnosti využitia elektronického bankovníctva a platobného styku v tejto oblasti. V krátkej budúcnosti budeme svedkami ešte väčšieho rozvoja bezkontaktnej technológie, ktorá bude podporovaná zabezpečením pomocou biometrických údajov.

7.1 Biometria

Biometria je založená na jedinečných biologických znakoch každého jedinca a na jeho charakteristických rysoch. Biometrické prvky pre potreby identifikácie a autentizácie sú bežne rozšírené a používané napríklad v prístupových systémoch, evidencii dochádzky alebo ďalších typoch osobnej identifikácie. Výhodou tohto typu autentizácie je jednoduchosť, pohodlnosť, spoľahlivosť a predovšetkým identifikačné biometrické znaky zostávajú nemenné, nedajú sa ukradnúť alebo zabudnúť. Podstatou biometrických systémov je automatizovaná kontrola charakteristických znakov a ich porovnanie s údajmi v databáze.

Porovnávané znaky musia spĺňať určité kritériá, aby boli vhodným identifikačným a autentizačným prostriedkom. Medzi určujúce vlastnosti patrí [32]:

- Jedinečnosť – vlastnosť musí byť jedinečná u každého jedinca
- Univerzálnosť – vlastnosť musí byť merateľná u čo najväčšej skupiny ľudí
- Stálosť – vlastnosť sa nesmie meniť v čase
- Získateľnosť – vlastnosť musí byť jednoducho získateľná
- Užívateľská prijateľnosť – stupeň prijatia technológie do každodenného života

Neoddeliteľnou súčasťou automatizovaného merania je bohužiaľ výskyt náhodných a systematických elementov, ktoré ovplyvňujú výsledok merania. Z dôvodu premenlivosti výsledkov nie sú biometrické systémy schopné dať jednoznačnú odpoveď na určenie identity, ale namiesto toho stanovia mieru pravdepodobnosti, s akou ide o daného jedinca. Praktický

systém preto musí dovoľovať určitú úroveň variability a schopnosť vyrovnať sa s chybami nesprávneho prijatia (False Acceptance) a nesprávneho odmietnutia (False Rejection).

Najviac preskúmané a rozšírené biometrické vlastnosti, ktoré sa používajú pre identifikačné a autentizačné účely, sú nasledujúce [32]:

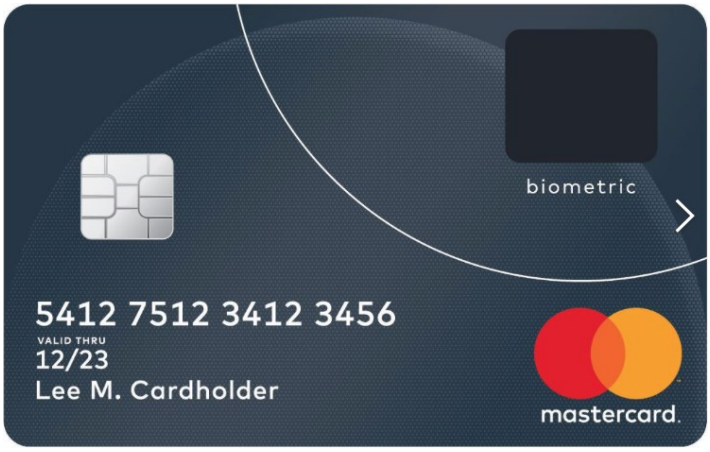
- Otlačok prsta
- Geometria ruky (rozmery dlane a prstov)
- Dúhovka oka
- Sietnica oka
- Geometria tváre
- Štruktúra žíl na prste/dlani
- Hlas
- Dynamika podpisu

V českom bankovom sektore sa začali dostávať do popredia biometrické technológie veľmi pozvoľna. Možným dôvodom je nedôvera zo strany klientov k poskytovaniu takýchto citlivých a nemenných údajov a zároveň problém bánk s ich spracovaním a bezpečným uložením. Prvým štartovacím krokom bol dynamický biometrický podpis, ktorý okrem vizuálneho prevedenia meria aj rýchlosť, smer ťahu, dynamiku a tlak podpisu. Pre tento účel sa používajú špeciálne zariadenia tzv. signpady, ktoré všetky tieto prvky zaznamenávajú. S nástupom chytrých telefónov, ktoré disponujú čítačkou odtlačkov prstov, sa tejto oblasti dostáva čoraz viac priestoru a záujmu. Väčšina tuzemských bánk už zapracovala autentizáciu a autorizáciu pomocou odtlačku prsta do svojich mobilných aplikácií. Overenie pomocou biometrických údajov má veľký potenciál nahradiť súčasné metódy využívajúce heslá a PIN kódy.

7.2 Budúcnosť platobných kariet

Aktuálny trend platobných kariet je jednoznačne daný. Česká republika je na špici v bezkontaktnom platení a podiel bezkontaktných platieb stále narastá. Predzvesť ďalšieho vývoja sa začína postupne presadzovať a do úvahy prichádzajú dva varianty. Prvou možnosťou je inovácia od spoločnosti MasterCard v podobe integrácie čítačky odtlačkov prstov do platobnej karty, ktorú budú predovšetkým presadzovať výrobcovia kreditných a debetných

kariet. Spoločnosť MasterCard technológiu vyvinula v spolupráci s nórskou firmou Zwipe, kde taktiež prebiehal pilotný projekt. Hlavnou výhodou, ktorú novinka prinesie, je bezpochyby zrušenie nutnosti zadávať alebo pamätať si PIN kód. Odtlačok prsta zaistí autorizáciu transakcie v ľubovoľnej hodnote. Výroba takejto karty je nákladnejšia a nutným predpokladom je zaistiť a zaregistrovať odtlačky prstov klientov a vytvoriť bezpečný proces ich uloženia. Táto podmienka by mohla čiastočne zabrániť väčšiemu rozšíreniu tejto technológie [33].



Obr. 42. Karta s čítačkou odtlačkov prstov [33]

Druhou, perspektívnejšou možnosťou, ktorá už je dostupná v Českej republike, je virtuálna podoba platobnej karty uložená v mobilnom telefóne s podporou NFC technológie [34]. I v tomto prípade sa transakcia autorizuje buď PIN kódom alebo pomocou čítačky odtlačkov prsta, ktorou už mobilné telefóny vo veľkej miere disponujú. Záujem užívateľov a finančných inštitúcií poukazuje na trend, ktorým sú práve mobilné platby s využitím biometrických prvkov. Z českých bánk túto službu ponúkajú ČSOB a Komerční banka, ktoré prišli s vlastným riešením a udávajú budúci smer v tejto oblasti. Pre platby využíva platformu HCE (Host Card Emulation), ktorá ukladá emulované platobné karty v zabezpečenom prostredí banky. ČSOB pre tento účel vyvinula novú aplikáciu NaNákupy, kde sa klientovi po spárovaní s internetovým bankovníctvom zobrazia všetky platobné karty, ktoré má u banky vydané [35]. Služba je dostupná pre mobilný telefón s operačným systémom Android a technológiou NFC. Nevyžaduje dokonca ani internetové pripojenie. Komerční banka sa vydala trochu odlišnou cestou, kde v spolupráci so spoločnosťou VISA implementovala bezkontaktné platby mobilným telefónom priamo do svojej mobilnej aplikácie pre smartbanking [36]. Mobilná platobná karta je v prípade Komerční banky vydá-

vaná v digitálnej podobe ako nový samostatný produkt a nevyužíva už existujúce platobné karty.

Veľkí výrobcovia a hráči na mobilnom trhu ponúkajú svoje vlastné služby pre bezkontaktné platenie mobilným telefónom. Ide predovšetkým o globálne služby Apple Pay a Android Pay, ktoré sú bohužiaľ dostupné len v niektorých krajinách a ich celosvetové rozšírenie postupuje pomalým tempom. Tieto služby ponúkajú univerzálne riešenie a možnosť využívať pre platenie platobnú kartu akejkoľvek podporovanej banky. Majitelia iPhonov si budú musieť na bezkontaktnú platbu mobilným telefónom kvôli politike spoločnosti Apple počkať až do oficiálneho spustenia služby Apple Pay v Českej republike.

7.3 Bankomaty novej generácie

Ani bankomaty neobišiel technologický pokrok a postupom času vylepšujú a dopĺňajú ďalšie funkcie. Základnou službou, ktorú bankomat ponúka, je vydávanie hotovosti. V ďalšom štádiu sa bankomat naučil hotovosť aj prijímať a vložiť na účet klienta. Táto služba je už pomerne rozšírená a počet takýchto „vkladomatov“ sa neustále zvyšuje. Okrem týchto štandardných platobných operácií bankomaty ponúkajú možnosť zmeniť PIN na platobnej karte, zistiť zostatok na účte, dobiť kredit alebo zaplatiť faktúru u mobilného operátora, získať informácie o produktoch banky, prípadne zvoliť počet a typ bankoviek pri výbere.

Bankomatom sa nevyhol ani aktuálny trend bezkontaktnej technológie, kedy už nie je potrebné kartu vkladať do bankomatu, ale postačí priblíženie karty, poprípade bezkontaktnej nálepky alebo dokonca len mobilného telefónu s technológiou NFC. Tým sa zase o niečo zjednoduší a urýchli výber hotovosti. Platobnú kartu nie je potrebné dávať preč z ruky a tým sa znižuje riziko skopírovania karty páchateľom, či zabudnutia karty v bankomate. Bezpečnostný PIN kód je potrebné aj naďalej zadať pri akejkoľvek výške výberu.

Použiť otlačok prsta alebo inú biometrickú vlastnosť namiesto PIN kódu na autentizáciu pri výbere hotovosti ponúkajú biometrické bankomaty napríklad v Japonsku, kde sa konkrétne využíva scan krvného riečiska ruky alebo prsta. Tento typ bankomatu sa presadil aj v susednom Poľsku, kde banky uviedli na trh 2000 bankomatov tohto typu. Senzor zosníma odtlačok prsta alebo jeho krvné riečisko a porovná snímok s uloženým vzorom. Ak sa snímok zhoduje, klient je oprávnený vykonať požadovanú transakciu. Predpokladom

k využívaniu týchto bankomatov je návšteva pobočky, kde si klient svoj odtlačok zaregistruje do bankového systému [37].

Obr. 43. Bankomat na krvné riečisko prsta [37]

Ďalším štádiom vývoja bankomatov by mohla byť prirodzená transformácia na samoobslužný kiosk, ktorý by sčasti nahradil širokú sieť bankových pobočiek a ušetril banke náklady. Takýto viacúčelový bankomat by mohol sprostredkovávať komunikáciu pomocou video technológie a ponúkol možnosť základných služieb vrátane uzatvárania zmlúv pomocou biometrického podpisu.

ZÁVER

Elektronické bankovníctvo a digitálna forma peňazí idú ruka v ruke s technologickým vývojom a inováciami. Dynamika tejto doby núti banky investovať čoraz viac prostriedkov do inovácií a zvýšenia kvality zabezpečenia svojich služieb. Bankovníctvo je práve tou oblasťou, kde je aplikácia moderných technológií najviac viditeľná a má dosah na široké spektrum populácie. Užívatelia si už zvykli na pohodlie a možnosť neustáleho prístupu k svojmu účtu. Príležitosti, ktoré ponúkajú moderné chytré telefóny, však idú ešte ďalej. V jednom prístroji sa dokáže skĺbiť nepretržitý komunikačný kanál s bankou a prístupom k bankovému účtu a taktiež virtuálna forma platobných kariet, ktoré plne zastúpia svoju plastovú verziu. Navyše s implementáciou biometrických techník vznikol veľmi robustný a spoľahlivý bezpečnostný prvok. Všetky tieto výhody ukazujú jednoznačný smer, kam sa elektronické bankovníctvo vydá v blízkej budúcnosti.

Práca dáva ucelený pohľad na aktuálny stav technológií vo finančnom sektore a zameriava sa najmä na problematiku zabezpečenia a ochrany pred potenciálnymi útokmi a hrozbami zo strany kybernetických zločincov. V úvodnej časti sú v teoretickej rovine popísané aktuálne technológie a možnosti ich využitia. Veľmi zaujímavé bude sledovať, ako sa ďalej bude vyvíjať situácia okolo digitálnych mien a predovšetkým bitcoinu v zmysle ich legalizácie a prijímania zo strany obchodníkov. S určitosťou však ide o oblasť, ktorá sa bude ďalej rozvíjať a ktorá ponúkne alternatívu k centralizovaným bankovým systémom. Otázka bezpečnosti, overenia a ochrany je rozobratá v ďalšej časti práce z pohľadu najbežnejších prístupových metód priameho bankovníctva. Do procesu autentizácie a autorizácie čoraz viac prehovárajú biometrické metódy, ktoré majú nespornú praktickú výhodu a nižšiu úroveň zneužitia. Posledná pasáž teoretickej časti je zameraná na aktuálne hrozby a typy útokov, ktoré využívajú páchatelia na poli kybernetickej kriminality. Dôležitým výstupom je identifikácia rizík, návrhy obranných mechanizmov a preventívnych opatrení.

Praktická časť práce obsahuje dotazníkový prieskum o povedomí internetovej bezpečnosti v súvislosti s peniazmi a jednotlivé odpovede sú prehľadne znázornené vo forme grafov a tabuliek. Z prieskumu vyplynulo, že povedomie o skúmanej oblasti je na slušnej úrovni a zásadné nedostatky sa neprejavili vo väčšej miere. Pri celkovom zhodnotení vyplynuli návrhy na zlepšenie a zvýšenie úrovne ochrany proti rizikám a hrozbám kybernetických útokov.

V závere diplomovej práce je pohľad do blízkej budúcnosti s prehľadom možností, ktorými sa bude uberať oblasť elektronického bankovníctva. Hlavnú úlohu budú hrať bezkontaktné technológie, ktoré sa ešte viac rozvinú v spojení s chytrými telefónmi a biometrické metódy identifikácie. Tie majú potenciál nahradiť nespočetné množstvo hesiel a kódov, ktoré je potrebné si pamätať a ktoré sa dajú pomerne jednoducho zneužiť. Využitie biometrických prvkov v bankovom sektore má určite svoje úskalia, predovšetkým z pohľadu ich zabezpečenia, ale ich nesporný prínos bude rozhodujúcim argumentom pre ich hromadné rozšírenie do každodenného života.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Elektronické bankovnictví. *Ceed.cz* [online]. [cit. 2017-05-22]. Dostupné z: http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm

[2] PŮLPÁNOVÁ, Stanislava. *Elektronické peníze a jejich úprava v České republice* [online]. Český finanční a účetní časopis, 2007 [cit. 2017-05-22]. Dostupné z: https://www.vse.cz/polek/download.php?jnl=cfuc&pdf=233.pdf

[3] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

[4] PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy*. Praha: Computer Press, 2000. ISBN 80-7226-328-5.

[5] Přímé bankovnictví. *Finance.cz* [online]. [cit. 2017-05-22]. Dostupné z: https://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi

[6] Platební karty a jejich druhy. *Penize.cz* [online]. [cit. 2017-05-22]. Dostupné z: http://www.penize.cz/80265-platebni-karty-a-jejich-druhy

[7] Bezkontaktní platby. *Raiffeisen Bank* [online]. [cit. 2017-05-22]. Dostupné z: https://www.rb.cz/informacni-servis/karty-raiffeisen/rady-a-tipy-ke-kartam/bezkontaktni-platby

[8] Elektronické bankovnictví - 2. část. *Učetní kavárna* [online]. 2010 [cit. 2017-05-22]. Dostupné z: http://www.ucetnikavarna.cz/archiv/dokument/doc-d9466v12332-elektronicke-bankovnictvi-2-cast

[9] Internetové peněženky. *Finanční poradenství online* [online]. [cit. 2017-05-22]. Dostupné z: https://www.financni-poradenstvi.com/internetove-penezenky

[10] Jak fungují předplacené platební karty? *Půjčko.cz* [online]. 2016 [cit. 2017-05-22]. Dostupné z: http://pujcko.cz/jak-funguji-predplacene-platebni-karty

[11] NÁDASKÝ, Adam a Peter PÉNZEŠ. *Niekoľko úvah k virtuálnej mene bitcoin* [online]. Národná banka Slovenska, 2013 [cit. 2017-05-22]. Dostupné z: http://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2013/08-2013/06_biatec13-8_nadasky.pdf

[12] Market Price (USD). *Blockchain.info* [online]. 2017 [cit. 2017-05-22]. Dostupné z: https://blockchain.info/charts/market-price?timespan=all

[13] Obchodování s bitcoiny. *Česká národní banka* [online]. 2014 [cit. 2017-05-22]. Dostupné z: https://www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf

[14] České banky jsou na špici v zabezpečení elektronických plateb. *ČESKÁ BANKOVNÍ ASOCIACE* [online]. 2016 [cit. 2017-05-22]. Dostupné z: https://www.czech-ba.cz/cs/ceske-banky-jsou-na-spici-v-zabezpeceni-elektronickych-plateb

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

[16] *Analýza zabezpečení internetového bankovnictví v České republice* [online]. Měšec.cz, 2005 [cit. 2017-05-22]. Dostupné z: https://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf

[17] Pozor na internetové podvodníky!. *MBank* [online]. 2016 [cit. 2017-05-22]. Dostupné z: https://www.mbank.cz/blog/post,675,pozor-na-internetove-podvodniky.html

[18] Jak se u českých bank přihlašujeme do internetového bankovnictví a jak potvrzujeme platby? *Finparáda* [online]. 2016 [cit. 2017-05-22]. Dostupné z: http://finparada.cz/3856-Jak-se-u-ceskych-bank-prihlasujeme-do-internetoveho-bankovnictvi-a-jak-potvrzujeme-platby.aspx

[19] Jak je chráněno mobilní bankovnictví, které používáte? *Finparáda* [online]. 2016 [cit. 2017-05-22]. Dostupné z: http://finparada.cz/4092-Jak-je-chraneno-mobilni-bankovnictvi-ktere-pouzivate.aspx

[20] Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví. *Česká národní banka* [online]. [cit. 2017-05-22]. Dostupné z: https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html

[21] Desatero bezpečnosti České bankovní asociace. *ČESKÁ BANKOVNÍ ASOCIACE* [online]. 2015 [cit. 2017-05-22]. Dostupné z: https://www.czech-ba.cz/cs/desatero-bezpecnosti-ceske-bankovni-asociace

[22] KAČMÁR, Rastislav. *ZaBEZPEČ si vedomosti: Kybernetická bezpečnosť* [online]. Slovak Security Policy Institute, 2016 [cit. 2017-05-22]. Dostupné z:

https://slovaksecurity.org/wp-content/uploads/2016/10/Kyberneticka-bezpecnost_SSPI.pdf

[23] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[24] JAMES, Lance. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

[25] V Česku řádí další phishing. Chce získat přístupové údaje k účtu ČSOB. *Cnews.cz* [online]. 2017 [cit. 2017-05-22]. Dostupné z: https://www.cnews.cz/v-cesku-radi-dalsi-phishing-chce-ziskat-pristupove-udaje-k-uctu-csob

[26] KOLOUCH, Jan. *KYBERNETICKÉ ÚTOKY* [online]. [cit. 2017-05-22]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[27] Ochrana před hrozbami na Internetu. *Avast* [online]. [cit. 2017-05-22]. Dostupné z: https://www.avast.com/cs-cz/c-online-threats

[28] Ransomware – historie, aktuální vyhlídky a možnosti ochrany. *IT Systems* [online]. 2016 [cit. 2017-05-22]. Dostupné z: https://www.systemonline.cz/clanky/ransomware-historie-aktualni-vyhlidky-a-moznosti-ochrany.htm

[29] Co je to botnet. *Timehosting.cz* [online]. 2015 [cit. 2017-05-22]. Dostupné z: http://timehosting.cz/co-je-botnet

[30] WANG, Ping, Sherri SPARKS a Cliff C. ZOU. *An Advanced Hybrid Peer-to-Peer Botnet* [online]. University of Central Florida [cit. 2017-05-22]. Dostupné z: https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html

[31] *Botnety sú všade, ale ich prevádzkovatelia zostávajú skrytí* [online]. eFocus, 2010 [cit. 2017-05-22]. Dostupné z: www.efocus.sk/images/uploads/28_32.pdf

[32] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. VŠB TU Ostrava, 2008 [cit. 2017-05-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

[33] Never forget your PIN again: Mastercard creates credit card with fingerprint scanner. *The Telegraph* [online]. 2017 [cit. 2017-05-22]. Dostupné z: http://www.telegraph.co.uk/technology/2017/04/20/mastercard-creates-credit-card-fingerprint-scanner

[34] Budoucnost platebních karet? NFC technologie. *Investujeme.cz* [online]. 2014 [cit. 2017-05-22]. Dostupné z: http://www.investujeme.cz/clanky/budoucnost-platebnich-karet-nfc-technologie

[35] ČSOB NaNákupy. *ČSOB* [online]. [cit. 2017-05-22]. Dostupné z: https://www.csob.cz/portal/lide/produkty/platebni-karty/csob-nanakupy

[36] Komerční banka spouští bezkontaktní platby přes chytrý telefon a novou generaci mobilního bankovnictví. *Komerční banka* [online]. 2016 [cit. 2017-05-22]. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/komercni-banka-spousti-bezkontaktni-platby-pres-chytry-telefon-a-novou-generaci-mobilniho-bankovnictvi-1205

[37] Forget fingerprints – banks are starting to use vein patterns for ATMs. *Theguardian.com* [online]. 2014 [cit. 2017-05-22]. Dostupné z: https://www.theguardian.com/money/2014/may/14/fingerprints-vein-pattern-scan-atm

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

[39] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[40] MÁČE, Miroslav. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. Finance (Grada Publishing). ISBN 80-247-1725-5.

[41] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

BIN	Bank Identification Number
BTC	Bitcoin
C&C	Command and Control
ČNB	Česká národní banka
ČSOB	Československá obchodní banka
CVC	Card Verification Code
CVV	Card Verification Value
DDoS	Distributed Denial of Service
DNS	Domain Name System
GSM	Global System for Mobile Communications
GPS	Global Positioning System
HCE	Host Card Emulation
HTTPS	Hypertext Transfer Protocol Secure
IRC	Internet Relay Chat
IVR	Interactive voice response
NFC	Near Field Communication
PDA	Personal Digital Assistant
PIN	Personal identification number
QR	Quick Response
SIM	Subscriber identity module
SMS	Short message service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAP	Wireless Application Protocol

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: ZOZNAM OTÁZOK V PRIESKUME

Prieskum o povedomí internetovej bezpečnosti v súvislosti s peniazmi:

https://docs.google.com/forms/d/e/1FAIpQLSebpz9vYtR-CxNAxNaZhFdItjem7OHd23JHjAxOnR6WRXvJxg/viewform

Identifikačné údaje

Pohlavie

- ○ muž
- ○ žena

Veková skupina (vyberte jednu z možností)

1. 15 – 24 rokov
2. 25 – 34 rokov
3. 35 – 44 rokov
4. 45 – 54 rokov
5. nad 54 rokov

Váš sociálny status (vyberte jednu z možností)

1. študent
2. zamestnaný
3. nezamestnaný
4. dôchodca
5. podnikateľ
6. materská dovolenka

Vaše najvyššie ukončené vzdelanie (vyberte jednu z možností)

1. základné
2. stredoškolské bez maturity
3. stredoškolské s maturitou
4. vysokoškolské

Používanie internetu

Aké zariadenia používate pre prístup na internet?

- ☐ mobil/smartphone
- ☐ tablet
- ☐ notebook
- ☐ stolný počítač
- ☐ iné

Ktoré z nasledujúcich činností robíte online?

- ☐ e-mail
- ☐ čítanie online správ

- ☐ využívanie online sociálnych sietí
- ☐ kúpa služieb a tovaru (knihy, nábytok, elektronika, dovolenka,...)
- ☐ elektronické bankovníctvo
- ☐ hranie online hier
- ☐ sledovanie televízie

Elektronické bankovníctvo

Využívate služby elektronického bankovníctva?

- ○ áno *(skok na sekciu Elektronické bankovníctvo (áno))*
- ○ nie *(skok na sekciu Elektronické bankovníctvo (nie))*

Elektronické bankovníctvo (nie)

Ak nevyužívate služby elektronického bankovníctva, aký máte dôvod? (vyznačte max 3 možnosti) *(odoslať formulár)*

- ☐ neznalosť práce s počítačom
- ☐ chýbajúce technické vybavenie (PC, internet,..)
- ☐ nezáujem o služby
- ☐ uprednostnenie návštevy pobočky
- ☐ nedôvera v zabezpečenie elektronických transakcií
- ☐ strach zo zneužitia osobných údajov a finančných prostriedkov
- ☐ nedostatok informácií o službe

Elektronické bankovníctvo (áno)

Aké služby elektronického bankovníctva využívate?

- ☐ internetbanking (webový prehliadač)
- ☐ smartbanking (banková aplikácia v mobile)
- ☐ phonebanking (zákaznícka linka, bankár na telefóne)
- ☐ homebanking (špeciálny program banky – firemná klientela)
- ☐ iné

Ako často využívate služby elektronického bankovníctva?

- ○ aktívne - denne
- ○ aktívne - 2 až 3 krát týždenne
- ○ niekoľkokrát za mesiac
- ○ príležitostne

- ○ mám, ale nepoužívam

Z akých zariadení pristupujete do svojho elektronického bankovníctva?

- ☐ mobil/smartphone
- ☐ tablet
- ☐ notebook
- ☐ stolný počítač
- ☐ iné

Obávate sa rizika zneužitia prihlasovacích údajov k svojmu bankovému účtu?

- ○ áno
- ○ nie

Je podľa vás zabezpečenie internetbankingu a mobilných aplikácií dostačujúce?

- ○ áno
- ○ nie

Aké autentizačné prvky prístupu na svoj bankový účet využívate?

- ☐ prihlasovacie meno a heslo
- ☐ SMS kľúč
- ☐ GRID karta
- ☐ certifikát
- ☐ čipová karta
- ☐ autorizačná kalkulačka
- ☐ biometrické prvky (otlačok prsta)
- ☐ generátor kódu pomocou mobilnej aplikácie
- ☐ iné

Pristupujete k svojim osobným dátam alebo účtom cez verejné nezabezpečené wifi siete?

- ○ áno
- ○ nie

Ako si chránite vaše prihlasovacie údaje do internetbankingu?

- ○ mám ich uložené v mobilnom telefóne
- ○ mám ich uložené v počítači/tablete
- ○ mám ich napísané na papieri
- ○ využívam aplikáciu na správu hesiel
- ○ viem ich naspamäť

- ○ iné

Platobné karty

Ste majiteľom platobnej karty?

- ○ áno *(skok na sekciu Platobné karty II)*
- ○ nie *(skok na sekciu Bezpečnostné prvky a riziká)*

Platobné karty II

Ako často používate platobnú kartu?

- ○ aktívne - denne
- ○ minimálne 2 až 3 krát týždenne
- ○ niekoľkokrát za mesiac
- ○ príležitostne
- ○ mám, ale nepoužívam

Akú platbu preferujete?

- ○ s PIN kódom
- ○ bezkontaktne

Zdá sa Vám bezkontaktná technológia bezpečná?

- ○ áno
- ○ nie

Využívate platobnú kartu pre platby na internete za tovar alebo služby?

- ○ áno
- ○ nie

Bezpečnostné prvky a riziká

Akým prípadným obavám čelíte pri používaní online platieb?

Máte obavy z toho, že niekto zneužije vaše osobné údaje?

- ○ áno
- ○ nie

Máte obavy z bezpečnosti a rizika odcudzenia vašich finančných prostriedkov?

- ○ áno
- ○ nie

Máte obavy, že nedostanete službu/tovar, ktoré si kúpite online?

- ○ áno

- ○ nie

Zamykáte si svoj počítač alebo mobil, z ktorého pristupujete k svojmu bankovému účtu?

- ○ áno
- ○ nie

Ukladáte si automaticky heslá a prihlasovacie údaje do webového prehliadača??

- ○ áno
- ○ nie

Kontrolujete, či sa naozaj nachádzate na stránkach svojej banky? (Poznámka: Bezpečné spojenie rozpoznáte na základe adresy URL, ktorá sa začína „https:“ alebo podľa symbolu visiaceho zámku.)

- ○ áno
- ○ nie

Inštalujete mobilné aplikácie výhradne z oficiálnych certifikovaných zdrojov (Apple Store, Google Play, Windows Store)?

- ○ áno
- ○ nie

Dôverujete mobilným aplikáciám z pohľadu bezpečnosti a využívate ich pre prístup na svoj bankový účet?

- ○ áno
- ○ nie

Poskytli ste niekedy PIN alebo svoje prihlasovacie údaje tretím osobám?

- ○ áno
- ○ nie

Kontrolujete pohyby na svojom účte pravidelne?

- ○ áno
- ○ nie

Ako často si meníte heslo pre prístup do elektronického bankovníctva?

- ○ len ak to vyžaduje priamo moja banka
- ○ minimálne 1 krát za tri mesiace
- ○ minimálne 1 krát ročne
- ○ heslo si nemením

S akými internetovými hrozbami ste sa už stretli osobne alebo vo svojom blízkom okolí?

- ☐ phishing (e-mailové útoky, ktorých cieľom je vylákať dôverné informácie)
- ☐ e-mail so zavírenou prílohou
- ☐ podvrhnutý falošný formulár na webe, snažiaci sa vylákať citlivé údaje
- ☐ ukradnutý účet (sociálna sieť, e-mail,...)
- ☐ útok na elektronické bankovníctvo
- ☐ zneužitie platobnej karty
- ☐ žiadna z uvedených
- ☐ iné

Aké opatrenia proti počítačovým útokom a hrozbám využívate?

- ☐ antivírusový softvér
- ☐ pravidelná aktualizácia operačného systému a aplikácií
- ☐ zálohovanie dát
- ☐ šifrovanie kritických súborov
- ☐ žiadne opatrenie nevyužívam

Poznámka:

Ak je pri odpovediach znak ○, ide o otázku s výberom práve jednej odpovede.

Ak je pri odpovediach znak ☐, ide o otázku s výberom viacerých odpovedí.