

EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA

Evidenčné číslo: 101007/B/2022/36122176492048900

**ELEKTRONICKÉ BANKOVNÍCTVO - TRENDY A
BEZPEČNOSŤ**

Bakalárska práca

EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA

Evidenčné číslo: 101007/B/2022/36122176492048900

**ELEKTRONICKÉ BANKOVNÍCTVO - TRENDY A
BEZPEČNOSŤ**

Bakalárska práca

Študijný program: Financie, bankovníctvo a investovanie

Študijný odbor: Ekónómia a manažment

Školiace pracovisko: Katedra bankovníctva a medzinárodných financií

Vedúci záverečnej práce: Ing. Boris Šturc, CSc.

Bratislava 2022

Ema Recká

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú (habilitačnú) prácu som vypracoval(a) samostatne a že som uviedol (uviedla) všetku použitú literatúru.

Dátum:

(podpis študenta, resp. uchádzača o habilitačné konanie)

Pod'akovanie

Na tomto mieste by som chcela vyjadriť svoju vďaku predovšetkým vedúcemu mojej záverečnej práce Ing. Borisovi Šturcovi, CSc. za čas venovaný mentorovaniu, jeho cenné rady, trpezlivosť a inšpiráciu počas celej doby písania tejto práce. Moja vďaka taktiež patrí mojej rodine a kamarátom za podporu, ako aj všetkým, ktorí mi poskytli cenné informácie potrebné pre spracovanie mojej záverečnej práce.

ABSTRAKT

RECKÁ, Ema: *Elektronické bankovníctvo - trendy a bezpečnosť*. Ekonomická univerzita v Bratislave. Národohospodárska fakulta, Katedra bankovníctva a medzinárodných financií. Vedúci záverečnej práce: Ing. Boris Šturc, CSc. Bratislava: NHF, 2022, 41 strán.

Cieľom záverečnej bakalárskej práce je predovšetkým priblížiť čitateľovi problematiku elektronického bankovníctva, identifikovať úroveň bezpečnosti elektronického bankovníctva a posúdiť súčasné trendy v danej oblasti. Práca je rozdelená do troch hlavných kapitol a 12 podkapitol. Obsahuje 4 grafy, 5 tabuliek a 2 obrázky. Prvá kapitola sa zameriava na skúmanú problematiku v elektronickej oblasti bankovníctva na Slovensku a v zahraničí z teoretického hľadiska. V druhej časti je charakterizovaný hlavný cieľ práce, čiastkové ciele, metodika a metódy využité pri skúmaní elektronického bankovníctva a dosahovaní cieľov. Záverečná kapitola je venovaná opisu elektronického bankovníctva troch vybraných bánk pôsobiacich na Slovensku, bezpečnostnej stránke elektronických činností či procesov bánk. Identifikácií očakávaní vývoja skúmanej oblasti je venovaná posledná podkapitola. Výsledkom riešenia problematiky elektronického bankovníctva so zameraním na trendy a bezpečnosť je vytvorenie stručného prehľadu foriem bankovníctva, porovnanie elektronického bankovníctva troch bánk, formulácia zistení a očakávaní autorky práce.

Kľúčové slová:

elektronické bankovníctvo, internet banking, mobile banking, mobilná aplikácia, bezpečnostné prvky, biometria, trendy, viacfaktorová autentifikácia

ABSTRACT

RECKÁ, Ema: *Electronic banking - trends and security*. University of Economics in Bratislava. The faculty of National Economics, Department of banking and international finance. Supervisor of the final thesis: Ing. Boris Šturc, CSc. Bratislava: NHF, 2022, page count 41.

The aim of the final bachelor thesis is mainly to make the reader aware and understanding in regard to the theme of electronic banking, identify the level of the electronic banking security and evaluate contemporary trends in this sphere. The thesis is divided into 3 main sections and 12 subsections. It includes 4 graphs, 5 tables and 2 pictures. The first section focuses on the researched sphere of electronic banking in Slovakia and abroad, from the theoretical standpoint. In the second section, the principal aim of the thesis, partial aims and the methodology utilized in the research of electronic banking are all characterized. The final section is dedicated to the description of electronic banking of three chosen Slovak banks and the security of electronic activities or processes of the banks. In regard to the identification of the expectations in terms of the evolution of the researched sphere, the last subsection is dedicated to it. The results of the focus in the sphere of electronic banking with emphasis on trends and security, creation of concise overview of the banking formats, comparison of electronic banking of three banks and formulation of author's findings and expectations.

Key terms :

electronic banking, internet banking, mobile banking, phone application, security elements, biometrics, trends, multi-factor authentication

Úvod	9
1. Súčasný stav problematiky na Slovensku a v zahraničí	10
1.1 Elektronické bankovníctvo	10
1.2 Formy elektronického bankovníctva	12
1.2.1 Homebanking	12
1.2.2 Internetbanking	12
1.2.3 Mobile banking	15
1.2.4 Mail banking	17
1.2.5 Telefonické bankovníctvo	17
1.2.6 Samoobslužné zóny	18
1.2.7 Alternatívne banky/ virtuálne banky	19
1.3 E-commerce	19
1.4 Elektronické peniaze a platobné karty	21
1.4.1 Platobné karty a ich bezpečné používanie	21
1.4.2 NFC - near field communication	23
1.5 Bezpečnosť	24
1.5.1 Silná Autentifikácia Klienta	25
1.5.2 GDPR	25
1.5.3 Bankové tajomstvo	26
1.5.4 Bionické bankovníctvo	27
1.6 Hrozby elektronického bankovníctva	27
2. Cieľ práce, metódy skúmania a metodika práce	29
3. Výsledky práce a diskusia	30
3.1 Elektronické bankovníctvo Tatra banka, a.s.	30
3.1.1 Internet Banking	31
3.1.2 BusinessBanking a MultiCash	32
3.1.3 Mobilné aplikácie Tatra banky	33
3.1.4 Bezpečnosť	35
3.2 Elektronické bankovníctvo 365.bank, a.s.	37
3.2.1 Mobilná aplikácia 365.bank	38
3.2.2 Internet banking a Business banking	38
3.2.3 Bezpečnosť	39
3.3 Elektronické bankovníctvo VÚB	40
3.3.1 Nonstop banking a internetbanking	40
3.3.2 InBiz a Multicash	41

3.3.3	VÚB Mobil Banking	41
3.3.4	Bezpečnosť	43
3.4	Okamžité platby	44
3.5	Porovnanie bezpečnosti elektronického bankovníctva vybraných bánk	45
3.6	Očakávaný vývoj elektronického bankovníctva a bezpečnosti	46
	Záver	49
	Použitá literatúra	50

Úvod

Dnešný moderný svet čoraz viac upriamuje našu pozornosť na digitalizáciu bežných činností a elektronické alternatívy vo všetkých smeroch každodenného života. Bankovníctvo je sektor poskytujúci služby pre všetkých z nás. Činnosť subjektov pôsobiacich v tomto sektore sa však líši od ostatných práve vysokou formou bezpečnostných opatrení. V dobe digitalizácie je ochrana klientov a ich osobných údajov hlavnou príčinou obáv z ich strany aj zo strany banky. Elektronické bankovníctvo celosvetovo neustále napreduje, vznikajú nové produkty či funkcie a banky postupne prenášajú svoje pôsobenie do online priestoru. Vďaka konkurenčnému správaniu, pokroku v technologickej oblasti a neustálej inovácii produktov či funkcií vznikajú na trhu medzi bankami trendy. Tie môžeme pozorovať napríklad v samotnom presúvaní procesov z pobočiek do internet bankingu alebo vo využívaných technológiách, modernizácii alebo vo vývoji nových produktov a služieb.

Z uvedeného vyplýva, že táto práca je zameraná na elektronické bankovníctvo. V rámci tejto témy sa bližšie zameriava na bezpečnosť a vybrané hrozby súvisiace s elektronizáciou bankových procesov. Následne práca popisuje aktuálne trendy pomocou štyroch dôležitých pilierov, ktorými sú jednoduchosť, rýchlosť bezpečnosť a technologický pokrok reprezentovaný najmä umelou inteligenciou. Prvá kapitola tejto bakalárskej práce je určená na priblíženie problematiky z teoretického hľadiska. Opisuje jednotlivé formy elektronického bankovníctva, ich bezpečnostnú stránku a popisuje aktuálne hrozby spojené s digitalizáciou bankovníctva. Druhá kapitola obsahuje vymedzený cieľ práce a metódy využívané pri jej tvorbe. Posledná tretia kapitola poskytuje prehľad elektronického bankovníctva troch vybraných bánk, ich komparáciu z hľadiska bezpečnosti a následnú formuláciu očakávaní ďalšieho vývoja.

1. Súčasný stav problematiky na Slovensku a v zahraničí

Prvá kapitola tejto bakalárskej práce približuje teoretické východiská potrebné na vysvetlenie tematiky elektronického bankovníctva a následné využitie poznatkov pri konkrétnych príkladoch v kapitole číslo 3. Rozdelená je do šiestich základných podkapitol. V nich sa zameriavam na definovanie elektronického bankovníctva a vymedzenie jeho foriem. Ďalšie časti sú venované elektronickému obchodovaniu, tzv. e-commerce a s ním súvisiacimi elektronickými peniazmi. Nasledovné podkapitoly opisujú bezpečnostné prvky a regulácie v oblasti e-bankingu a hrozby, ku ktorým dochádza pri digitalizácií bankovníctva.

1.1 Elektronické bankovníctvo

E-bankovníctvo predstavuje formu bankovníctva, resp. poskytovania služieb banky a vykonávania platieb prostredníctvom elektronickej komunikačnej technológie ako napríklad telefón či internet. Jeho úlohou je poskytovanie rýchlej a komfortnej komunikácie bankou smerom ku klientom. Podľa S. Poloučka (2013, s. 110) „*Elektronické bankovníctvo môžeme definovať ako poskytovanie štandardizovaných bankových produktov a služieb elektronickými cestami.*“¹ Od bežného bankovníctva sa odlišuje napríklad:

- absenciou priamej komunikácie medzi klientom banky a zamestnancom banky,
- 24 hodinovou dostupnosťou bankových služieb klientom,
- rýchlosťou transakcii, služieb a komunikácie s bankou,
- jednoduchosťou práce s prostriedkami,
- efektívnosťou,
- vysokou mierou bezpečnosti a špecifickými ochrannými prvkami.

E-banking je súčasťou technologickej distribúcie bankového sektora prostredníctvom komunikačných médií. Umožňuje komerčným bankám zvyšovať kvalitu a rýchlosť služieb pre majiteľov bežných či investičných účtov a súčasne znižovať svoje náklady. Vznik elektronických financií mal veľmi veľký vplyv na bankovníctvo a hospodárenie subjektov. V knihe *Internet banking and the Law in Europe* (2006, str. 7)²

¹ POLOUČEK, Stanislav. *Bankovníctví* : 2. vyd. Praha: C. H. Beck, 2013, s. 110. ISBN 978-80-7400-491-9.

² GKOUTZINIS, Apostolos. *Internet banking and the law in Europe*: 1. vyd. New York: Cambridge University Press, 2006, s.7. ISBN 0-521-86071-7.

spomínajú, že e-bankovníctvo, ako také, sa začalo postupne rozvíjať už v 19. storočí v spojení s telegrafickou komunikáciou a malo, a stále má, veľký vplyv na ekonomickú globalizáciu.

Pre obchodné banky je typické poskytovanie bankových produktov a služieb, ktoré tvorí aktívna a pasívna časť. D. Majerčáková³(2018, str.146) uvádza, že *aktívne bankové produkty* delíme nasledovne :

- Platobné produkty - slúžia na vykonávanie platobného styku pomocou elektronického príkazu na úhradu a elektronického príkazu na inkaso.
- Depozitné produkty - umožňujú klientom vkladať voľné prostriedky do banky, pričom banka sa v tomto vzťahu nachádza na strane dlžníka.
- Finančné úverové produkty - financovanie formou úveru či inou alternatívnou formou.

Pasívne produkty bánk, ktoré klient získava aj pomocou e-bankingu, sú charakteristické poskytovaním informácií o bežnom účte či o banke. Nepochádza v nich k pohybu peňažných prostriedkov ani jedného subjektu. Do tejto kategórie zaraďujeme napríklad :

- získavanie výpisu z účtu klienta banky,
- prehľad transakcií bežného účtu,
- nastavenia účtu a platobných kariet,
- úprava informácií o klientovi ako napr. adresa trvalého bydliska,
- prehľad produktov a služieb banky,
- informácie o sadzbách banky za poskytované služby,
- prehľad devízových konverzií,
- informácie o banke.

Bežhotovostné platby sú veľkou zložkou elektronického bankovníctva. Podľa zákona č 394/2012 Z. z. o obmedzení platieb v hotovosti, ktorý Národná rada Slovenskej republiky schválila v roku 2012, sú niektoré hotovostné platby zakázané. Ministerstvo financií Slovenskej republiky oznámilo v článku *Obmedzenie platieb v hotovosti*, že zákon

³ MAJERČÁKOVÁ, Daniela. *Peniaze a bankovníctvo*: 1. vyd. Praha: Wolters Kluwer, 2018, s. 146. ISBN 978-80-7552-972-5.

bol schválený ako podpora boja proti daňovým podvodom v rámci akčného plánu, teda aby sa zabránilo vystavovaniu vymyslených dokladov bez skutočného pohybu peňazí. (MFSR, 2012)⁴

1.2 Formy elektronického bankovníctva

1.2.1 Homebanking

*„Homebanking je založený na dátovej komunikácii medzi klientom a bankou prostredníctvom osobného počítača využitím komutovaných telefónnych liniek a analógových modemov.“*⁵ Príkazy klienta boli vykonávané prevažne off-line. Banky po prijatí informácií, ktorých prenos sa konal online, spracovali a vykonali príkaz. S postupným vývojom a čoraz väčším používaním služieb internetu sa homebanking premieňal na internetbanking. Práve preto ho označujeme ako pôvodcu internetbankingu ale aj ako modernejšej verzie mobile bankingu.

Výhodou homebankingu bolo pohodlie a bezpečie domova pri vykonávaní transakcií oproti dlhšiemu osobnému procesu v pobočke banky. Z pohľadu banky, ako finančnej inštitúcie, boli najväčším pozitívom nižšie náklady na prevádzku pobočiek. Naopak, veľkou nevýhodou boli vysoké poplatky pri prenose dát banke či potreba inštalácie bankového softvéru priamo do počítača. Na zabezpečenie údajov bolo v tomto období využívané najmä šifrovanie.

1.2.2 Internetbanking

Pod pojmom internetbanking rozumieme elektronický platobný systém bánk, ktorý slúži na vykonávanie finančných transakcií a nefinančných služieb prostredníctvom webových aplikácií. Predstavuje neobmedzený virtuálny prístup klienta k jeho bežnému účtu v banke a všetkým typom bankových služieb okrem výberu hotovosti. Taktiež poskytuje novým klientom možnosť otvorenia účtu online v klasickej banke alebo virtuálnej online banke.

⁴ MFSR. *Finančný trh: Obmedzenie platieb v hotovosti*. [online] [cit. 2021-09-25]. Dostupné na : <https://www.mfsr.sk/sk/financie/financny-trh/obmedzenie-platieb-hotovosti/>

⁵ HORVÁTOVÁ, Eva. *Bankovníctvo*: 1. vyd. Žilina: GEORG Žilina, 2009, s. 263. ISBN 978-80-89401-03-1.

Internetbanking, najpoužívanejšia forma e-bankingu, vznikla už koncom minulého storočia a jeho rozvoj napredoval veľkou rýchlosťou vďaka technológiám pre vývoj webových aplikácií, rozšíreniu a väčšej dostupnosti internetu pre široké vrstvy obyvateľstva. Práve preto zastúpil miesto homebankingu. Jeho používanie sa stalo jednoduchším, nakoľko vyžaduje prítomnosť jedine internetového prehliadača. Jeho využiteľnosť sa tak rozšírila z používania počítača na používanie iných, mobilných, zariadení. Ďalšou vývojovou vetvou IB je mobile banking, opisovaný v podkapitole 1.2.3., ktorého nástup bol vyvolaný boom-om používania mobilných zariadení.

Bezpečnosť prihlásenia do internet bankingu

Veľkou nevýhodou internetbankingu je potreba zvýšenej bezpečnosti a používania ochranných prvkov pri vstupe či samotnom využívaní služieb z pohľadu klienta. Práve preto väčšina slovenských bánk využíva viacfaktorovú autentifikáciu. Zároveň však umožňuje banke neustály prístup k nahliadaniu a správe účtov jej klientov. Túto možnosť však jej zamestnanci nesmú zneužívať a informácie nachádzajúce sa v internetbankingu klienta využívajú výlučne na pracovné účely.

Pre vstup do internetovej verzie bežného účtu je potrebné poznať a použiť bezpečnostné prvky ako napríklad osobné identifikačné číslo, prihlasovacie meno a heslo. Tieto prvky predstavujú prvý stupeň overenia. Pre potreby vyššieho overenia používajú banky bezpečnostné prvky ako SMS autorizácia, fyzické čítačky kariet a elektronické podpisy na čítačkách, tokeny a iné. Aj napriek mnohým možnostiam priniesol technologický rozvoj poslednej dekády nové možnosti a banky začali využívať biometrické bezpečnostné prvky pre vstup do internetového a mobilného bankingu.

Základný prvok bezpečnosti zo strany klienta je nastavenie dostatočne silného hesla a jeho zmena po určitom čase. VÚB uvádza, že medzi aktuálne najviac využívané prvky patria nasledovné. *SMS overovanie* je jednou z najpoužívanejších a najstarších foriem viacfaktorovej autorizácie. Klientovi po zadaní telefónneho čísla príde SMS správou niekoľkomiestny kód, ktorý následne zadá na stránke internetbankingu svojej banky. Banky taktiež pri založení účtu zisťujú priamo od klienta jeho súkromný telefonický kontakt, ktorý

spárujú s jeho účtom. Tieto služby nazývame SMS banking. *Fyzické kartové čítačky* slúžia na generovanie jednorazových kódov či podpisov, pričom klient na ich získanie potrebuje čipovú kartu. *Elektronické čítačky* fungujú na princípe aplikácie, ktorú treba aktivovať v internetbankingu alebo priamo v pobočke banky na stretnutí s osobným bankárom. *Mobilné aplikácie* na potvrdzovanie prihlásenia tokenom sú novším ochranným prvkom a postupne nahrádzajú klasickú SMS autorizáciu. Po vstupe do mobilnej aplikácie banky je klientovi poskytnutý niekoľkomiestny kód slúžiaci na overovanie prihlásenia či platieb. (vub.sk, Bezpečnosť IB, Debetné karty)⁶ Pri zabezpečení a potvrdzovaní platieb na internete slúži tzv. overovanie platieb priamo v mobilnej aplikácii či *3D Secure overovanie*. Pod týmto prvkom rozumieme posielanie SMS správ s 3D Secure kódom, ktorý klient vpíše do určeného poľa alebo tento kód banka zašle do aplikácie. (Obchodné podmienky 365.bank, 2021, str.1)⁷

Bezpečnosť vykonávania operácií

Banky sa počas posledných predchádzajúcich rokov museli prispôbovať vývoju doby a medzi to patrí aj čoraz väčšie využívanie elektronických služieb. Klienti však majú strach zo zneužitia ich osobných údajov, údajov platobných kariet či prihlasovacích hesiel. Trendom pri ochrane vykonávania platobných príkazov či presúvania prostriedkov na sporiaci účet cez internetové bankovníctvo je používanie štyroch hlavných prvkov. Prvým je *ochrana biometrickými prvkami*, ktorá predstavuje najmodernejší spôsob ochrany v online priestore. Najčastejšie klienti využívajú *zabezpečenie PIN kódom* (Personal Identification Number), ktoré si klient vytvára sám. Pri niekoľkonásobnom chybnom zadaní PIN-u je prístup zamietnutý a častokrát klientovi nedovoľuje opätovne zadať heslo ani po istom čase. *GRID karta* je tretím prostriedkom, ktorá predstavuje vyššiu formu zabezpečenia vďaka využívaniu nie len číselných znakov ale aj písmen. *Elektronický osobný kľúč* náhodne generuje kód, ktorý je zaznamenaný aj na strane banky kvôli identifikácii užívateľa. (P. Štarchoň, 2017, str. 77-78)⁸

⁶ VÚB Banka. *Internet banking: Bezpečnosť IB*. [online] [cit. 2021-09-25]. Dostupné na : https://www.vub.sk/elektronicke-bankovnictvo/internet-banking/bezpecnost-ib/#tab_2

⁷ 365.Bank. *Obchodné podmienky: Obchodné podmienky pre osobné účty s prílohami*. [online]. 20.9.2021. [cit. 2021-09-29]. Dostupné na: <https://365.bank/pravne-info>

⁸ ŠTARCHOŇ, Peter. *Bankový marketing: princípy a špecifiká*: 1. vyd. Praha: Wolters Kluwer, 2017, s. 77, 78. ISBN 978-80-7552-948-0.

Výhody a nevýhody internetbankingu

Internetbanking ponúka klientom oveľa viac výhod ako len pohodlné spravovanie prostriedkov na účte z domu. Je prístupný nonstop (24 hodín denne 7 dní v týždni), s výnimkou večernej uzávierky, kedy banka klienta upozorní na spracovanie platieb po jej skončení. Uzávierka však neobmedzuje klienta vo vykonávaní transakcií či úprave nastavenia účtov. Umožňuje platby medzi rôznymi bankami rýchlo a v iných menách. Šetrí čas aj výdavky klienta na využívanie bankových služieb. Umožňuje využiť prepojenie internetbankingu s inými zariadeniami ako sú mobilné telefóny či tablety pomocou mobile bankingu. V neposlednom rade sa banky čoraz viac sústreďujú na posilňovanie bezpečnosti všetkých aspektov internetového bankovníctva. Pri používaní elektronického bankovníctva a jeho foriem, čiže aj internetbankingu, existujú riziká spojené s online priestorom. Medzi nevýhody zaradíme možné hrozby ako phishing, pharming, smshing, vishing a iné formy pokusov o získanie a zneužitie citlivých informácií. Možným mínusom je aj potreba vlastníctva aspoň jedného zariadenia, ktoré podporuje internet a internetbanking čo znevýhodňuje časť populácie, ktorá k nim prístup nemá.

1.2.3 Mobile banking

Mobile banking je modernou verziou WAP-banking, pod ktorým rozumieme využívanie internetbankingu alebo vzdialeného bankovníctva mobilným telefónom. Avšak postupným vývojom pokročilých technológií čoraz menej ľudí navštevuje internetbanking cez internetové stránky bánk a preferuje používanie mobilných aplikácií. V skratke, vlastná aplikácia banky je jednoduchým a prehľadným zobrazením internetového bankovníctva priamo v mobile. Veľkou výhodou je rýchlosť používania aplikácie pri zadávaní príkazov či potvrdzovaní platieb. V mobilnej aplikácii možno nahliadať k pohybu na účte, kontrolovať zostatok prostriedkov či komunikovať priamo s bankou. Platby prebiehajú rýchlejšie vďaka funkciám skenovania IBAN, QR kódu či EAN kódu. Klient banky má taktiež prístup ku svojim platobným kartám, ich nastaveniam a nastaveniam samotného účtu. Mobilný banking zjednodušuje základné úkony ako zmena PIN kódu plastovej platobnej karty či zadávanie príkazov na úhradu.

Súčasťou mobile bankingu je taktiež využívanie možnosti platenia digitálnymi platobnými kartami prostredníctvom služieb Apple Pay, Google Pay a inými, ktoré na potvrdenie identity majiteľa platobnej karty vyžadujú tvárovú biometriu, odtlačok prsta alebo vopred nastavené heslo. V tomto prípade je nevýhodou možné odcudzenie zariadenia.

Bezpečnosť mobile bankingu

Bankové aplikácie sú najčastejšie zabezpečené 4-8 miestnym PIN kódom, bezpečnostnou biometriou alebo ich kombináciou. Medzi najviac využívané biometrické bezpečnostné prvky od roku 2020 na slovenskom trhu podľa NBS patria ⁹:

- Hlasová biometria - overovanie totožnosti na základe hlasu.
- Tvárová biometria - využíva technológiu na rozlíšenie prítomnosti živej osoby a fotografie (FaceID).
- Odtlačok prsta - overovanie identity snímaním prsta.
- Biometrický podpis - overovanie podobnosti, rýchlosti, tlaku podpisovania a ďalších faktorov.
- Skenovanie očnej dúhovky - skúma rozloženie farieb, ich odtiene a vzory, ktoré vytvárajú.

Platby mobilom či príkazy v aplikáciách sú taktiež zabezpečené PIN kódom či biometrickými prvkami. Novinkou v oblasti internetových platieb je možnosť využitia jednorazovo generovanej digitálnej karty, ktorá zabezpečuje ochranu údajov o platobnej karte pred ich odcudzením a zneužitím. Platby sú chránené aj obmedzením výšky platenej sumy. Výška tohoto obmedzenia sa medzi bankami líši pričom klientovi dáva voľnosť zvoliť si vlastný limit v stanovenom intervale. Základným prvkom, ktorý obsahuje takmer každá aplikácia, je automatické odhlásenie používateľa z aplikácie po určitom čase nečinnosti v aplikáciách či pri opustení aplikácie. Táto funkcia je dôležitá najmä pri prechádzaní medzi aplikáciami, ktoré nie sú zabezpečené na rovnakej úrovni ako tie bankové.

Výhody a nevýhody mobile bankingu

⁹Národná banka Slovenska. *Dohľad nad finančným trhom: Biometria*. [online] [cit. 2021-09-23]. Dostupné na: <https://www.nbs.sk/sk/dohlad-nad-financnym-trhom/fintech/biometria>

Za posledných 5 rokov sa z nepoznaného mobilného bankovníctva stala neoddeliteľná súčasť každodenného života viac ako 70% ľudí. Za tento trend v rámci elektronického bankovníctva vďačíme najmä technologickému priemyslu a postupnému zlepšovaniu dostupnosti smart telefónov pre väčšinu obyvateľstva sveta. Smart-phone je dnes už bežným predmetom v rukách dospelých, tínedžerov a detí. Práve preto bankovníctvo využilo príležitosť posunúť svoje služby o krok bližšie k zákazníkom. (Pobočky sú stále dôležité, 2020, str.34)¹⁰

1.2.4 Mail banking

Služba, vďaka ktorej klient prijíma upozornenia o pohyboch na účte a banka zasiela výpis účtu na mail klienta sa nazýva mail banking. V našich podmienkach sa využíva najmä ako ekologickejšia forma získavania výpisu z bežného účtu. Tento výpis je zasielaný zväčša každý mesiac, pokiaľ klient nezvolí inak. Zabezpečuje sa heslom, ktoré pozná len klient. V USA či v Indii je využívaná služba mail bankovníctva aj na zadávanie príkazov na vklad peňazí na účet. Najčastejšie pomocou šeku.

1.2.5 Telefonické bankovníctvo

Telefonické bankovníctvo či callbanking poskytuje rovnaké služby ako internet banking či mobile banking ale ako komunikačný prvok je využívaný telefón. Jedná sa o komunikáciu majiteľa účtu s call centrom banky prostredníctvom ktorej dokáže :

- zadávať príkaz na úhradu či inkaso,
- meniť nastavenia účtu,
- blokovať kartu a nahlásiť jej odcudzenie,
- získať informácie o účte a službách banky,
- a iné.

¹⁰ Pobočky sú stále dôležité. *Obchod: marketing, retail, FMCG*. Bratislava: MAFRA, 2020, roč. 25, č. 4, 34 s. ISSN 1335-2008.

Vo väčšine bánk je klient spojený najskôr s technikou, ktorá automaticky generuje správy a informácie, až neskôr prichádza kontakt so zamestnancom banky. Telefonické služby sú do značnej miery automatizované a technológia, ako prijímateľ správy, dokáže bez zásahu človeka oznámiť napríklad zostatok na účte.

Bezpečnosť telefonického bankovníctva

Banka na overenie totožnosti osoby, ktorá do klientskeho centra volá, využíva najmä hlasovú biometriu, ktorú porovnáva s hlasovou nahrávkou urobenou klientom pri založení účtu. V prípade založenia účtu skôr, ako hlasová biometria bola bežnou súčasťou autorizácie, klient dostane možnosť nahráť hlasovú správu neskôr. Druhým overovacím prvkom je kladenie otázok, na ktoré odpoveď pozná iba klient a banka alebo zisťovanie diskretných údajov. Niektoré banky, ako napríklad Poštová banka, overuje totožnosť aj na základe vopred dohodnutého hesla. V oboch prípadoch hovoríme o diskretnej konverzácii a v prípade, že klient má záujem riešiť zložitejší problém či manipulovať s väčším množstvom prostriedkov, bankár navrhne iný prostriedok bankovníctva alebo osobné stretnutie.

1.2.6 Samoobslužné zóny

K poskytovaným službám elektronického bankovníctva patrí aj prevádzkovanie samoobslužných zón v rámci pobočky banky alebo mimo nej. Banky týmto spôsobom poskytujú niektoré služby, ktoré nie je možné vykonať inak ako osobne, 24 hodín denne len s použitím bankovej platobnej karty alebo mobilu. V týchto zónach podľa D. Bouškovej (2006, str. 216) ¹¹ banky prevádzkujú :

- bankomat kombinovaný s nočným trezorom, v ktorých klient môže vkladať alebo vyberať hotovosť,
- bankomat, ktorý poskytuje zmenárenské služby a depozity,
- automatické bezpečnostné schránky,
- informačný a transakčný terminál.

¹¹ BOUŠKOVÁ, Dagmar. *Bankové operácie*: Bratislava. Vydavateľstvo EKONÓM, 2006, s.216. ISBN 80-225-2136-1.

Všetky tieto zariadenia sú dostatočne zabezpečené napríklad kamerami aby klient nebol ohrozovaný pri využívaní služieb jeho banky. V prípade zlého zadania PIN kódu kreditnej či debetnej karty, bankomat je nastavený na jej automatické zadržanie pre prípad, že by karta bola odcudzená a zneužitá.

1.2.7 Alternatívne banky/ virtuálne banky

Skupinu bánk, ktoré konkurujú klasickým bankám s históriou v retail bankingu, s dobrým menom a dlhoročným poskytovaním služieb najmä face-to-face nazývame alternatívne banky. Väčšina z nich pochádza z modernej doby posledných pár rokov a sú založené na používanie v online priestore. Podľa P. Štarchoňa (2017, str.89)¹² do tejto skupiny zaraďujeme banky ako napríklad Revolut, N26 či slovenskú 365.bank v období jej vzniku. Revolut Bank UAB vznikol ako inštitúcia elektronických peňazí v Litve v roku 2015. Aj keď názov alternatívne banky znie zavádzajúco, aj samotný Revolut či N26 musia spĺňať podmienky licencie ECB a národnej banky, ktorá je zároveň ich regulátorom. N26 je mobilná banka založená už v roku 2013 s cieľom vytvoriť prvú mobilnú banku. Podobné koncepty ako tieto dve banky sa v našich podmienkach snažila vytvoriť 365.bank, ktorá však od roku 2021 nie je výhradne mobilnou bankou.

1.3 E-commerce

E-commerce je skratka pre electronic commerce, obchodný model nakupovania a predávania cez internet, alebo v preklade elektronický obchod. So vznikom internetu sa do online prostredia prenieslo aj nakupovanie. Je úzko spojený s elektronickým bankovníctvom. Spoločnosti tak majú možnosť rozšíriť služby o e-commerce alebo prevádzkovať samostatne internetový obchod. ECB uvádza definíciu e-commerce ako „Predaj alebo nákup tovaru alebo služieb prostredníctvom elektronických transakcií uskutočňovaných prostredníctvom internetu alebo iných počítačom sprostredkovaných sietí.“¹³ Elektronické obchodovanie má korene už v polovici minulého storočia, približne v roku 1960. S postupným rozvojom prinášajú banky na trh nové produkty a technológie na

¹² ŠTARCHOŇ, Peter. *Bankový marketing: princípy a špecifiká*: Praha. Wolters Kluwer, 2017, s.89.. ISBN 978-80-7552-948-0.

¹³ Európska centrálna banka. *Payments and markets glossary: e-commerce*. [online] [cit. 2021-10-15]. Dostupné na: <https://www.ecb.europa.eu/services/glossary/html/act7e.en.html>

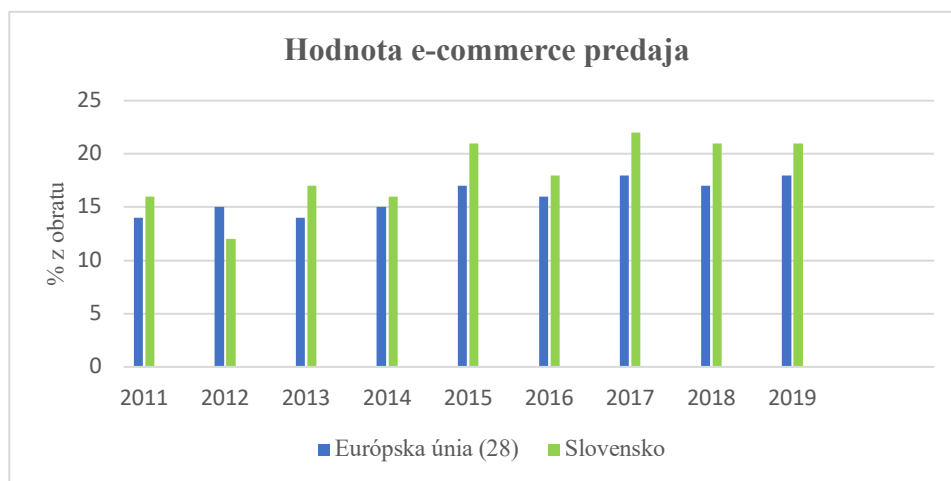
podporu tohoto segmentu. Rozlišujeme dve hlavné oblasti e-obchodu, a to práve B2B (business to business) a B2C (business to customer). Treťou oblasťou je C2C obchodovanie medzi fyzickými osobami navzájom. Bez ohľadu na to o akú oblasť sa jedná, tento spôsob obchodu prebieha pomocou elektronických platobných systémov bánk. D. Boušková (2006, str. 216)¹⁴ rozdeľuje tieto platobné systémy na:

1. Platobný systém na základe kreditných kariet - VISA, MasterCard,
2. Platobný systém na základe elektronickej hotovosti - zabezpečuje anonymné transakcie elektronickými mincami,
3. Platobný systém na základe konta - Paybox,
4. Platobný systém na základe elektronickej čipovej peňaženky - nositeľom funkcie je čipová karta.

Rast popularity e-commerce prináša nové výhody a nevýhody z pohľadu banky. Výhodou je, že banky majú vďaka online obchodu možnosť neustále napredovať a prispôbovať sa novým požiadavkám trhu. Okrem pasívnej pozície v elektronickom obchode ako sprostredkovatelia platieb môžu banky ponúkať nové alebo tradičné produkty ako aktívny subjekt na tomto trhu. Prínosom bankovníctva je napríklad elektronické platenie priamo na webe alebo v aplikácii obchodníka. Medzinárodné platby sa stali dostupnejšími a banky posilnili elektronickú bezpečnosť. Nevýhodu predstavujú novo vzniknuté riziká spojené s internetom a používanými technológiami.

Vďaka neustálemu a rýchlemu prispôbovaniu sa bankového sektora sa vykonáva stále viac elektronických obchodov. Graf 1 zobrazuje percentuálne vyjadrenie hodnoty predaja prostredníctvom e-obchodu z celkového globálneho obratu za 9 rokov na Slovensku a v Európskej únii.

¹⁴ BOUŠKOVÁ, Dagmar. *Bankové operácie*: 1. vyd. Bratislava: Vydavateľstvo EKONÓM, 2006, s.216. ISBN 80-225-2136-1.



Graf 1 Hodnota e-commerce predaja ako % z obratu. Zdroj: Eurostat. Vlastné spracovanie.

1.4 Elektronické peniaze a platobné karty

So vznikom elektronických peňazí sa postupne rozvíjalo aj elektronické bankovníctvo. Podľa Európskej centrálnej banky sú elektronické peniaze „...elektronicky uchovaná peňažná hodnota na technickom zariadení, ktoré sa môže používať na vykonávanie platieb subjektom iným ako vydavateľom elektronických peňazí.“¹⁵ Na používanie týchto peňazí je potrebný elektronický platobný prostriedok. Tieto prostriedky ECB rozdeľuje na hardware, ktoré majú podobu fyzického nositeľa elektronických peňazí, sú to napríklad plastové platobné karty a software prostriedky, ktoré fungujú pomocou internetu.

1.4.1 Platobné karty a ich bezpečné používanie

Platobné karty predstavujú jeden z najpoužívanejších bezhotovostných platobných prostriedkov. Napríklad debetné platobné karty sú súčasťou bežného účtu klienta a poskytujú mu neustály vzdialený prístup k prostriedkom nachádzajúcim sa na tomto účte. Ide o nástroj bezhotovostného platobného styku, ktorý je vydávajú ich bankové asociácie a peňažné ústavy. V Slovenskej republike prevládajú medzinárodné bankové asociácie a platobné systémy Visa a Mastercard. Platobné karty z hľadiska spôsobu zúčtovania a úhrady delíme :

¹⁵ Európska centrálna banka. *Money, credit and banking: Electronic Money*. [online] [cit. 2021-10-11]. Dostupné na: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

- *kreditné karty* - predstavujú formu revolvingového úveru, ktorý banka poskytuje klientovi opakovane počas určitej doby. Táto úverová čiastka sa obnoví po splatení. Klient tak nepoužíva vlastné zdroje ale prostriedky banky, ktoré spláca bezúročne v tzv. bezúročnom období alebo s úrokom v stanovenom percentuálnom vyjadrení zo sumy úveru. VÚB ako výhodu kreditných kariet uvádza napríklad cashback pri platbách alebo jej použitie v zahraničí. (Poznáte rozdiel medzi debetnou a kreditnou kartou?, 2021)¹⁶
- *debetné karty* - sa vydávajú k bežnému účtu v banke. Klient na nich čerpá vlastné prostriedky do vopred určeného povoleného zostatku na účte. Slúži na platenie a výber hotovosti z bankomatu.
- *charge karty* - sú podobné tým kreditným, avšak klient musí prostriedky splatiť v jednej splátke každý mesiac k stanovenému dňu.
- *pre-paid karty* alebo elektronická peňaženka - ich funkciou je obmedzenie používania hotovosti. (E. Horváthová, 2009, str.207)¹⁷

S. Polouček vo svojej knihe *Bankovníctví* (2009, str.114)¹⁸ člení karty na základe spôsobu uloženia dát a použitia na :

- karty s magnetickým prúžkom na zadnej strane karty,
- karty s elektronickým čipom, ktoré dokážu uložiť väčší objem informácií.

Bezpečnosť platenia platobnými kartami

Medzi modernejšie verzie patria čipové karty a virtuálne karty poskytujúce vyššiu mieru bezpečnosti a overovanie držiteľa karty pomocou CVM (customer verification method). Virtuálne platobné karty sú novinkou posledných pár rokov. Pomáhajú klientom ochrániť prostriedky na účte pri platení na internete. Na autorizáciu pomocou CVM slúžia tzv. CVV alebo CVC/CVC2 kódy, ktoré sa nachádzajú na prednej alebo zadnej strane karty. Fungujú náhrada k PIN kódu pri platbách na diaľku, to znamená nie platbou cez platobný terminál.

¹⁶ VÚB Banka. *Poznáte rozdiel medzi debetnou a kreditnou kartou? Dôležité fakty, ktoré by ste mali vedieť.* 2021, [online][cit. 2021-10-15]. Dostupné na: <https://www.vub.sk/jednovubky/poznate-rozdiel-medzi-debetnou-kreditnou-kartou/>

¹⁷ HORVÁTOVÁ, Eva. *Bankovníctvo*: 1. vyd. Žilina: GEORG Žilina, 2009, s. 207. ISBN 978-80-89401-03-1.

¹⁸ POLOUČEK, Stanislav. *Bankovníctví* : 2. vyd. Praha: C. H. Beck, 2013, s. 114. ISBN 978-80-7400-491-9.

„*Card Verification Code alebo v skratke CVC kód slúži na autentifikáciu držiteľa a platobnej karty pri platbách bez prítomnosti karty, hlavne pri platbách u internetových obchodníkov.*“¹⁹ Tento kód sa nachádza na zadnej strane karty a je vo forme trojčíslika. Názov CVC používa prevažne kartová asociácia VISA. CVV kód je alternatívou CVC najmä pre držiteľov karty MasterCard. CVV2, CVV1 a CVC2, CVC1 sú taktiež 3-miestne kódy, avšak rozdielom je spôsob ich generovania a druh platieb, ktorý ochraňujú. Skupina týchto kódov slúži na zabránenie zneužitia údajov karty pri internetových platbách, platbách na diaľku či fyzických platbách pomocou terminálu. Pri uniknutí informácií z prednej strany karty ako sú napr. číslo karty a dátum expirácie, súžia práve tieto 3 cifry na opačnej strane na potvrdenie platby.

1.4.2 NFC - near field communication

Near field communication (*NFC*) je technológia ktorá umožňuje poskytovať služby bezkontaktného platenia. „*Ide o súbor štandardov bezdrôtovej technológie, ktorú využíva už väčšina producentov chytrých telefónov a tabletov, ktorá slúži na vzájomnú komunikáciu medzi dvoma zariadeniami.*“²⁰ Ako aj z názvu vyplýva, prenos údajov medzi zariadeniami sa uskutočňuje na krátku vzdialenosť, pár centimetrov, ale bez fyzického kontaktu.

Zariadenia medzi ktorými sa NFC uskutočňuje sú mobilný telefón, smart hodinky a platobný terminál. Celý proces platby trvá pár sekúnd. NBS na svojej internetovej stránke uvádza, že túto technológiu podporujú služby Apple Pay, Google Pay, Garmin Pay či Samsung Pay a iné. Tieto aplikácie nazývame aj mobilné peňaženky. Okrem bezkontaktných mobilných platieb umožňujú aj platby na internete či v aplikáciách. Fungovanie tohoto systému je založené na kooperácii a dohode medzi bankou, službou mobilných platieb a poskytovateľmi platobných kariet (Visa a Mastercard). Pri používaní plastových kariet má väčšina bánk nastavený limit na bezkontaktné platby, ktorý sa líši od limitu na internetové platby. Pre väčšiu ochranu klientov je nastavený limit 50 EUR, kedysi

¹⁹ Poštová banka. *Novinky: Čo je CVC kód a kde sa na karte nachádza?*. 2016. [online] [cit. 2021-10-15]. Dostupné na: <https://www.postovabanka.sk/novinky/blog/co-je-cvc-kod-a-kde-sa-na-karte-nachadza/>

²⁰ ŠTARCHOŇ, Peter. *Bankový marketing: princípy a špecifiká*: 1. vyd. Praha: Wolters Kluwer, 2017, s. 81. ISBN 978-80-7552-948-0.

20 EUR, na platbu. Do tejto výšky sa nevyžaduje zadanie PIN-u na platobnom termináli. Pri platbách mobilom je potrebné zadať jeden z typov potvrdenia platby pri každej sume.

Veľkou *výhodou* mobilných NFC platieb je zvýšená bezpečnosť pri riziku odcudzenia oproti klasickej plastovej platobnej karte. Na autorizáciu platby je totiž potrebné zadať heslo, ktoré nemusí zodpovedať PIN kódu na plastovej karte, oskenovať tvár či prst. Nevyžaduje používanie údajov na karte či zdĺhavé vypisovanie prístupových údajov do internetbankingu. Zákazníci sa nemusia báť týchto platieb, pretože aplikácie neukladajú ani nezdieľajú číslo karty. „*Namiesto toho, pre každú platbu vytvorí jedinečné virtuálne číslo účtu a zároveň bezpečnostný kód, ktorým bezpečne spojí transakciu s konkrétnym bankovým účtom.*“²¹ Nevýhodou NFC je, že nie každý obchodník akceptuje bezkontaktné platby a má vytvorené podmienky na platenie mobilom. Tieto platby sú obmedzené aj pre tých, ktorí vlastnia staršie zariadenia nepodporujúce technológie NFC.

1.5 Bezpečnosť

Bezpečnosť elektronického bankovníctva môžeme definovať rôzne. Predstavuje napríklad ochranu údajov nachádzajúcich sa zariadeniach podporujúcich formy elektronického bankovníctva, ako napríklad počítače, tablety, mobily či platobné karty. Zahŕňame sem aj používanie autorizačných prvkov na ochranu klientov banky, ochrana pre únikom informácií z e-bankingu či informácií z platobných kariet. Veľkú hrozbu predstavuje najmä nezabezpečené internetové pripojenie. Pre čo najbezpečnejšiu formu používania IB pomocou už spomínaných zariadení odporúčajú banky používanie vlastného zaheslovaného domáceho internetového pripojenia. Vykonávanie prevodov cez internet banky častokrát podmieňujú v obchodných podmienkach používaním zariadenia s antivírusovým softvérom. S týmito podmienkami musí klient súhlasiť, pokiaľ chce využívať elektronické služby.

Druhým ohrozujúcim faktorom sú nezabezpečené internetové stránky, ktoré sa nezačínajú ako https. Toto je jeden z ochranných prvkov, ktoré má každý možnosť skontrolovať pred poskytovaním diskretných údajov. Druhým prvkom pri platení online je

²¹ Google Pay má na Slovensku rok. Čaká na konkurenciu od Apple. In *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha :4H production, 2019,roč.26, č.4., s. 46-47. ISSN 1212-4273.

system *3D secure*, ktorým disponuje obchodník a pridáva tak ochrannú vrstvu. Tento systém pri platení neposkytuje obchodníkovi informácie o platobnej karte klienta ale presmeruje ho priamo do bezpečného okna banky obchodníka. Jednotlivé platby sú následne overované SMS autorizáciou. 3D secure protokol sa týka elektronického obchodu. (Prima banka Slovensko, a.s., 2020, str. 2)²²

1.5.1 Silná Autentifikácia Klienta

Od roku 2021 sú banky povinné, na základe nariadenia Európskej únie, overovať identitu klienta pri platbách, ktoré spadajú do kategórie Silná Autentifikácia Klienta (SCA). NBS (2020) uvádza „Podľa údajov Európskej centrálnej banky je v eurozóne podvodom 23 z každých 1000 platieb kartou. Na Slovensku je to menej, podľa štatistík ide o 4 z 1000 platieb.“²³ Silná autentifikácia vyžaduje použitie minimálne jedného prvku z dvoch kategórií, ktoré sa nachádzajú v tabuľke.

Kategória/Faktor	Prvky ktoré je možné overiť pri platbách v internetovom prostredí
Vedomosť	Heslo, PIN, Odpovede na dohodnuté kontrolné otázky...
Vlastníctvo	Tokeny, Dynamické bezpečnostné kódy, Mobilné aplikácie, Mobilný telefón klienta
Charakteristické znaky držiteľa platobnej karty	Biometrické údaje: odtlačky prstov, FaceID

Obrázok 1 Zdroj: tatrabanka.sk (2020)

Tatra banka uvádza, že do kategórie silného overovania, čiže platby ktoré nemusia byť overované na základe tohoto nariadenia, nepatria elektronické platby vo výške do 30 EUR, pričom suma platieb od posledného overenia je nižšia ako 100 EUR, alebo počet týchto platieb od poslednej autorizácie nie je vyšší ako 5.

1.5.2 GDPR

²² Prima banka Slovensko. Všeobecné obchodné podmienky *Prima banka Slovensko, a.s.2020*,[online] [cit 2021-10-10]. Dostupné na: <https://www.primabanka.sk/vop/archiv>

²³ Národná banka Slovenska. *Otázky a odpovede k platbám kartami na internete*. [online] [cit 2021-10-10]. Dostupné na: https://www.nbs.sk/sk/informacie-pre-media/tlacove-spravy/spravy-vseobecne/detail-tlacovej-spravy/_otazky-a-odpovede-k-platbam-kartami-na-internete-od-1-1-2021

Európsky parlament v roku 2016 schválil nariadenie o ochrane údajov s cieľom zjednotiť podmienky v tejto oblasti v rámci celej Európskej únie. Skratka GDPR predstavuje General Data Protection Regulation, v preklade všeobecné nariadenie o ochrane údajov s vyzdvihnutím digitálnej ochrany. Celé nariadenie je zverejnené v Úradnom vestníku Európskej únie. Predmetom nariadenia je ochrana základných práv a slobôd so zameraním na ochranu osobných údajov.

Toto nariadenie je záväzné pre všetky členské štáty EÚ a každý kto pracuje s informáciami o občanoch EÚ je povinný ho dodržiavať. Sankciu za nedodržanie predstavuje pokuta do výšky 4% z ročného obratu spoločnosti alebo do výšky 200 miliónov EUR. Do tejto skupiny patrí sektor bankovníctva a v rámci neho aj online banking. S rozvojom elektronického bankovníctva sa zvyšuje množstvo informácií nachádzajúcich sa v elektronickej podobe v systémoch bánk a tým sa zvyšuje aj riziko ich úniku a zneužitia. Mbank (Ako chránime vaše osobné údaje a čo je GDPR?, 2021)²⁴ uvádza, že ich klienti majú v súlade s GDPR právo na vymazanie osobných údajov z bankových systémov, právo na prístup k nim, či právo na opravu a ich doplnenie a mnoho ďalších. Článok 7 GDPR upravuje podmienky vyjadrenia súhlasu osôb so spracovaním ich osobných údajov. Následne, po udelení súhlasu, sú tieto údaje v banke spracované a používané na príklad na marketingové účely, čiže prispôsobovanie individuálnej ponuky pre klienta a informovanie klienta o tejto ponuke. Článok 8 upravuje rovnaké podmienky pre deti mladšie ako 16 rokov, pričom v zmysle tohoto nariadenia musí súhlas vyjadriť zákonný zástupca dieťaťa. Maloletí nad 16 rokov môžu udeľovať súhlas vo svojom mene. Zmenou v oblasti udeľovania súhlasu je aj prehľadnejšie, kratšie a jednoduchšie spracovanie podmienok.

V roku 2017 schválila Slovenská republika Zákon o ochrane osobných údajov (č. 18/2018). Tento zákon upravuje problematiku ochrany údajov vo väčšej miere. Tento zákon nadobudol účinnosť 25.5.2018, v rovnaký deň ako sa začalo uplatňovať nariadenie GDPR.(P. Štarchoň, 2017, str. 91-95)²⁵

1.5.3 Bankové tajomstvo

²⁴ Mbank. Ako chránime vaše osobné údaje a čo je GDPR? [online] [cit. 2021-10-25]. Dostupné na: <https://www.mbank.sk/gdpr/#uvod>

²⁵ ŠTARCHOŇ, Peter. *Bankový marketing: princípy a špecifiká*: 1. vyd. Praha: Wolters Kluwer, 2017, s.91-95. ISBN 978-80-7552-948-0.

Zákon č. 483/2001 Z. z. o bankách a o zmene upravuje v § 91 bankové tajomstvo. Na rozdiel od vonkajších hrozieb e-bankovníctva tento zákon upravuje aj tú vnútornú, hrozbu úniku informácií priamo z prostredia banky, pochybenie na strane zamestnancov a iné. „Predmetom bankového tajomstva sú všetky informácie a doklady o záležitostiach týkajúcich sa klienta banky alebo klienta pobočky zahraničnej banky, ktoré nie sú verejne prístupné, najmä informácie o obchodoch, stavoch na účtoch a stavoch vkladov. Tieto informácie banka a pobočka zahraničnej banky sú povinné utajovať a chrániť pred vyzradením, zneužitím, poškodením, zničením, stratou alebo odcudzením....“²⁶

1.5.4 Bionické bankovníctvo

Spolu s elektronickým bankovníctvom ešte stále existujú pobočky bánk, hotovosť a klasická forma osobného bankovníctva. Tieto dve oblasti sa banky snažia spájať pomocou bionického bankovníctva aby vytvorili pre svojich zákazníkov lepší model distribúcie svojich produktov. Banky týmto spôsobom pripravujú nové typy pobočiek, ktoré by spĺňali požiadavky spojenia online a offline bankovníctva. Dôvodom sú rôzne nároky rôznych skupín klientov. Tí, ktorí využívajú prevažne digitálne služby preferujú rýchlosť a personalizáciu. Zákazníci, ktorí uprednostňujú offline cestu zase očakávajú prijateľné ceny produktov. Cieľom je zníženie nákladov, zvýšenie ziskov z výnosov a uspokojiť zákazníkov. Bionické bankovníctvo teda predstavuje niečo ako zmiešanie ľudí a digitálnej technológie s cieľom vytvoriť čo najlepšie produkty a služby pre zákazníkov pomocou bionickej banky. (Global Retail Banking, Accelerating Bionic Transformation, 2017)²⁷

1.6 Hrozby elektronického bankovníctva

Väčšina hrozieb e-bankingu prichádza z vonkajšieho prostredia a pôsobí na klientov bánk. Práve Slovenská banková asociácia pravidelne informuje občanov SR o hlavných hrozbách elektronického bankovníctva prostredníctvom publikovania článkov a správ. Je potrebné pripomenúť, že elektronické bankovníctvo nezahŕňa výlučne online banking ale aj

²⁶ Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

²⁷ DUPAS, Muriel-GREBE, Michael. *Global Retail Banking 2017: Accelerating Bionic Transformation*. [online]. 2017. [cit. 2021-10-11]. Dostupné na: <https://www.bcg.com/publications/2017/financial-institutions-global-retail-banking-2017-bionic-transformation>

phone banking či používanie platobných kariet s elektronickou formou peňazí. Sektor bankovníctva je lákadlom pre veľké množstvo útočníkov.

Phishing podľa SBA (2015)²⁸ predstavuje posielanie mailov podvodníkmi, ktorý sa vydávajú za nimi vybrané banky a snažia sa týmto spôsobom získať osobné údaje a údaje o účte, prihlasovacie heslá, číslo karty či telefónne číslo. Častokrát mail vyzerá identicky ako ten, ktorý posielala banka. Klienta presvedča o svojej pravosti napríklad priloženým odkazom na webovú stránku, ktorú nie je možné v niektorých prípadoch rozoznať od originálu. Základným rozdielom je šifrovanie stránky banky a jej internetbankingu, ktoré je štandardným ochranným prvkom systémov spravujúcich dôverné informácie. Falošné stránky toto šifrovanie pravdepodobne neobsahujú. Podvodný mail je takmer vždy zasielaný z mailovej adresy veľmi podobnej originálnej, avšak obsahuje napríklad gramatickú chybu, pridaný znak alebo iné poradie slov. Phishing neznamená len útočenie na klientov ale obeťou sa môže stať aj zamestnanec banky. Banka ako finančná inštitúcia je zabezpečená proti takýmto útokom viacerými spôsobmi ako napríklad bezpečnostné školenia zamestnancov, aktualizácia postupov a zložitejšie členenie bankovej siete.

Pod pojmom *vishing* rozumieme získavanie citlivých informácií hackermi na základe telefonátu a zasielania SMS správ. Smshing znamená lákanie osôb k poskytnutiu informácií kliknutím na odkaz v SMS správe alebo žiadanie o spätnú väzbu. Štvrtým typom podvodu je *pharming*, ktorý „...je založený na zmene DNS (Domain Name System) položiek. Užívateľ navštívi web stránky, ktoré nie sú originálnymi stránkami banky, ale sú falošné.“²⁹ V podstate ide o vytváranie falošnej stránky, ktorá je využívaná aj na účely phishingu. Hackeri sa tak snažia obchádzať zaužívané pravidlá bankového sektora..

Carding v elektronickom bankovníctve zahŕňa všetky typy podvodov spojených s platobnými kartami. Ide prevažne o kradnutie informácií a ich ponúkanie na čiernom trhu. Do tejto skupiny patrí elektronický skimming, ktorý sa postupne vyvinul z pôvodného kradnutia údajov z platobných kariet fyzicky pomocou kartových čítačiek. S elektronickou verzou krádeže týchto údajov sa banky stretávajú čoraz viac. Namiesto čítačky kariet

²⁸ Slovenská Banková Asociácia. *Ako je to naozaj. Opatrenia proti phishingu.* [online], 2015, [cit. 2021-10-11]. Dostupné na: <https://www.sbaonline.sk/novinka/ako-to-je-naozaj-opatrenia-proti-phishingu/>

²⁹ SLSP. *Bezpečnosť: Čo vám hrozí.* [online] [cit. 2021-10-12]. Dostupné na: <https://www.slsp.sk/sk/ludia/bezpecnost/co-vam-hrozi> cit[09-10-2021]

používajú zloději softvér, ktorým napádajú stránky spoločností prevádzkujúcich online obchody. (Europol, International ATM skimming network dismantled in Italy, 2016)³⁰

SBA taktiež upozorňuje, že banky nikdy od klientov nežiadajú osobné či iné citlivé údaje týmito spôsobmi. V dnešnej dobe je veľmi dôležité aby si ľudia chránili súkromie, a preto banky odporúčajú prihlasovať sa do internetového či mobilného bankovníctva iba na zabezpečenej Wi-Fi a vlastných mobilných dátach, pričom internetové bankovníctvo využívať jedine priamo na oficiálnej stránke. Pri akomkoľvek podozrení, že klient sa stal obeťou podvodu, je potrebné aby túto informáciu poskytol svojej banke. Porušenie GDPR vedie k úniku diskretných informácií zo strany banky a predstavuje porušenie práv jej klientov a zamestnancov. Banka však môže vystupovať aj ako obeť útoku.

2. Cieľ práce, metódy skúmania a metodika práce

Hlavnými cieľmi bakalárskej práce je identifikovať úroveň bezpečnosti elektronického bankovníctva a posúdiť súčasné trendy v danej oblasti. Dva hlavné ciele je možné rozdeliť na menšie čiastkové ciele. Prvým čiastkovým cieľom je poskytnúť teoretický základ problematiky elektronického bankovníctva všeobecne a z pohľadu bezpečnosti a aktuálnych trendov. Druhý cieľ je zameraný na analýzu foriem elektronického bankovníctva v troch vybraných bankách. Následne pomocou výskumu zistiť aké ochranné prvky dané banky využívajú na zabezpečenie elektronických procesov. Štvrtý čiastkový cieľ sa zameriava na komparáciu systémov elektronického bankovníctva vybraných bánk, následné identifikovanie rozdielov a formuláciu trendov.

Pri napĺňaní cieľov som vychádzala z relevantnej odbornej literatúry poskytujúcej teoretické poznatky o elektronickej podobe bankových služieb, jednotlivých formách a o bezpečnostných prvkoch využívaných bankami na Slovensku a v zahraničí. Ako doplnok pre poskytnutie aktuálnych informácií mi slúžili odborné články a oficiálne webové stránky inštitúcií bankového sektora. Tejto problematike bola venovaná kapitola číslo 1. Na základe analyzovania prvej kapitoly som sa rozhodla v kapitole číslo 3 zamerať na konkrétne tri banky pôsobiace na slovenskom trhu. Pri výbere bánk boli pre mňa dôležité ich kvalitatívne

³⁰ Europol. *International ATM Skimming Network Dismantled in Italy*. [online]. 2016. [cit. 2021-10-11]. Dostupné na: <https://www.europol.europa.eu/media-press/newsroom/news/international-atm-skimming-network-dismantled-in-italy>

stránky. Prvou vybranou bankou je Tatra banka, a.s., ktorá je všeobecne známa ako líder v oblasti bankovej digitalizácie a patrí do medzinárodnej bankovej skupiny Raiffeisen. 365.bank, a.s. vznikla ako prvá banka v Slovenskej republike, ktorá na začiatku poskytovala služby výlučne elektronicky. Tretou zvolenou bankou je VÚB, a.s., ktorá má na Slovensku a v Českej republike dlhú históriu a slúži na účely komparácie s moderným prístupom zvyšných dvoch bánk. Aktuálne informácie o vybraných bankách som čerpala z oficiálnych webových stránok a pomocou výskumu počas požuvania demo verzii internetbankingu či mobile bankingu. Vytvorila som príslušné podkapitoly kde poskytujem bližšiu analýzu ich internetového bankovníctva, mobilného bankovníctva a bezpečnostných prvkov. Pri skúmaní bezpečnostných prvkov som na základe štatistických metód a grafického znázornenia interpretovala ich vývoj za vybrané obdobie. Pri spracovávaní grafov som vychádzala z dát poskytnutých vo výročných správach a iných oficiálnych finančných dokumentoch. Pomocou komparácie systémov elektronického bankovníctva som identifikovala aktuálny stav elektronického bankovníctva na slovenskom trhu. V závere formulujem pomocou výsledkov, syntézy a dedukcie subjektívny názor na súčasný vývoj a očakávania do budúcnosti.

3. Výsledky práce a diskusia

3.1 Elektronické bankovníctvo Tatra banka, a.s.

Tatra banka, a.s. má na území Slovenskej republiky dlhú históriu, ktorú začala písať už v roku 1990 ako prvá privátna banka na našom území. Je súčasťou Raiffeisen Bank International Group a ako jediná neprebrala názov po tejto skupine. Posledná dekáda bola pre Tatra banku veľmi významná najmä v oblasti inovácii, čomu nasvedčuje aj množstvo ocenení, ktoré získala. Medzi najdôležitejšie v oblasti digitalizácie a elektronického bankovníctva zaraďujeme ocenenie časopisu Global Finance, ktorý určil TB ako „The Best Digital Bank in Slovakia“ a „The Best Mobile Banking Adaptive Site“ v roku 2020. V rámci elektronického bankovníctva je TB slovenským lídrom. Ako prvá priniesla na slovenskú scénu službu internet banking a mnohé iné produkty a služby s účelom zjednodušenia bežných činností v banke a posilnenia inovácii na slovenskom trhu. (Bankovníctví, 2018)³¹

³¹ Slovenské banky a biometria. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha: 4H production, 2018, roč. 25, č. 11, s. 46-47. ISSN 1212-4273.

V roku 2020 tak vďaka moderným službám TB bolo viac ako 99% zo všetkých transakcií banky realizovaných elektronicky. Oproti roku 2010 ide o nárast o 9 percentuálnych bodov a v porovnaní s každoročne rastúcim počtom celkových transakcií hovoríme o pomerne výraznej zmene.

Najväčšími novinkami v portfóliu Tatra banky sú predstavenie mobilnej verzie Business banking^{TB}, Chatbot Adam či Bejby Blue, osobnosť digitálneho sveta, ktorej cieľom je priblíženie bankovníctva pre mladých ľudí. *Chatbot Adam^{TB}* je náhradou za komunikáciu so zamestnancom banky, ktorou Tatra banka posúva hranice predstavy o 24-hodinovom bankingu k realite. Adama môžeme charakterizovať ako umelú inteligenciu, ktorú Tatra banka sprístupnila od leta 2019 na webe či v mobilnej aplikácii a jeho úlohou je dopĺňať ponúkané elektronické bankové služby. Od marca 2022 spúšťa jeho novú, druhú, verziu. Adam odpovedá na otázky, odkazuje na konkrétnu oblasť webu či ponúka produkty na základe informácií, ktoré dostane. Podľa vopred určených logických postupov dokáže napríklad zadávať SEPA inkaso na požiadanie, v prípade zabudnutia PIN kódu ho sprístupní klientovi po dôkladnej identifikácii a autentifikácii. Dôležitú úlohu má aj v oblasti bezpečnosti. Na základe generovania jednorazových údajov o debetnej či kreditnej karte ochraňuje používateľa pred zneužitím. Adam je neustále trénovaný zamestnancami banky a každým dňom sa učí spracovávať nové zadania, pokyny a požiadavky. V prípade, že nedokáže odpovedať na správu odosielateľa, presmeruje konverzáciu na operátora, živú osobu, ktorá požiadavku vyrieši.

3.1.1 Internet Banking

Internet banking predstavuje pre Tatra banku najdôležitejšiu časť celého systému elektronického bankovníctva. Jej široké portfólio ponúka mnoho služieb od vedenia účtu, vykonávania príkazov na úhradu, investovania do podielových fondov, aktivácie aplikácii až po moderný depozit. Klientovi ponúka prehľadné spravovanie záväzkov voči banke a majetku, ktorý však nemusí byť vedený priamo v TB. Medzi novinky zavedené v roku 2020 patrí napríklad sprístupnenie čerpania business úveru, žiadanie o odklad splátok, ukladanie dokumentov potrebných pre banku bezpečne a priamo cez internetové bankovníctvo alebo možnosť založenia účtu pre živnostníkov online. Či už sa jedná o aktívne alebo pasívne funkcie, je zrejmé, že TB sa neustále zameriava na dosahovanie efektívneho digitálneho bankovníctva pre svojich klientov.

Na kontrolu a presnú kategorizáciu výdavkov a príjmov v internetbankingu Tatra banky za 3 po sebe nasledujúce roky slúži *Spending report*. Túto funkciu banka zaviedla už v roku 2010 ako prehľadnejšiu a rýchlejšie prístupnú alternatívu k výpisu bežného účtu. V súčasnosti ju ponúka aj vo svojej mobilnej aplikácii. Prichádzajúce a odchádzajúce prostriedky vie každý klient sledovať za rôzne časové obdobie, napríklad mesiac, avšak nemusí ísť však striktne o kalendárne vymedzený časový úsek. Jednotlivé kategórie zoskupujú platby automaticky podľa toho, kam alebo odkiaľ plynuli. Medzi kategórie patrí napríklad Reštaurácie, Cestovanie či Hotovosť, ktorá uvádza v akej sume klient robil výbery hotovosti. Tento report je možné jednoducho upravovať, pridávať vlastné kategórie, do ktorých aplikácia následne triedi transakcie automaticky. Zabezpečenie realizovania platieb cez internetové bankovníctvo záleží od denných a mesačných limitov. Tatra banka ponúka varianty :

1. základná autorizácia pri prihlásení do internet bankingu pri limite 3 000 Eur/deň a 3 0000 Eur/mesiac, pričom na jednotlivé platby platí limit 500 Eur;
2. dodatočná autorizácia s použitím
 - podpisu pomocou čítačky kariet;
 - 4-8 miestneho PIN-u, v prípade ak má klient nastavené prihlasovanie do internet bankingu pomocou tohto kódu pre transakcie v hodnote nad 500 Eur do sumy 3000 Eur. (Tatra banka, a.s.)³²

3.1.2 BusinessBanking a MultiCash

V roku 2017 predstavila TB dnes už veľmi úspešný produkt *Business banking*^{TB}. Jedná sa o ekvivalent internet bankingu pre jej firemných klientov, ktorý dnes využíva už väčšina z nich. (Výročná správa, 2017)³³ V poslednej výročnej správe za rok 2021 Tatra banka uvádza, že klienti realizujú približne 8 miliónov platieb ročne. Ponúka 12 aktívnych a 16 pasívnych funkcionalít bez potreby návštevy pobočky. Ďalším systémom elektronického bankingu je aplikácia *MultiCash*, ktorú podporuje niekoľko bánk na Slovensku a Tatra banka je jednou z nich. V rámci tejto aplikácie môže klient komunikovať

³² Tatra banka, a.s.. *Internetbanking: Limity pre platby*. [online] [cit. 2022-02-23]. Dostupné na : <https://www.tatrabanka.sk/sk/personal/ucet-platby/internet-banking/>

³³ Tatra banka, a.s.. *Výročné správy: Výročná správa 2017*. [online] [cit. 2022-02-21]. Dostupné na : https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyroczne-spravy/TB_Vyrocná_správa_2017.pdf

so všetkými svojimi bankami, spravovať účty v nich vedené na jednom mieste a prepojiť s bankou svoj účtovný systém. Z troch systémov v ponuke TB je práve MultiCash ten, čo ponúka klientom najmenej online procesov.

Porovnanie IB, BBTB a MC

Hlavným znakom, v ktorom sa tieto tri systémy elektronického systému od TB líšia je cieľová skupina, pre ktorú sú určené. Bližší opis každého z nich je uvedený vyššie. Tabuľka č. 1 zobrazuje stručné porovnanie 3 systémov elektronického bankovníctva na porozumenie toho, pre koho je ktorý produkt určený a aké sú jeho charakteristiky.

	Internet Banking	Business banking^{TB}	MultiCash
Klient	Fyzické osoby	Podniky, podnikatelia	Podniky, podnikatelia
Špecifické aktívne funkcie	Trvalý príkaz	Žiadosť o úver či záruku	Príkaz na inkaso
Špecifické pasívne funkcie	Týkajúce sa súkromného účtu b-mail	Týkajúce sa firemných účtov a kariet Prevod úveru, záruky	Týkajúce sa firemných účtov
Viacfaktorové overenie	Áno	Áno	Nie

Tabuľka 1 Vlastné spracovanie. Zdroj : tatrabanka.sk

3.1.3 Mobilné aplikácie Tatra banky

Mobilná aplikácia Tatra banky je vo svojej podstate internet banking v mobile vo forme samostatnej aplikácie. Ponúka prístup k účtu za pár sekúnd a množstvo služieb bez potreby návštevy kamennej pobočky ako napríklad v prípade vytvorenia účtu v Tatra banke alebo bez potreby použitia počítača. Momentálne ponúka dve verzie Lite a Full. Lite verzia, v preklade ľahká či odľahčená, je oveľa jednoduchšia na používanie a obsahuje len základný prehľad o prostriedkoch na bežnom či sporiacom účte alebo o platobných kartách. Je určená najmä klientom vyžadujúcim základné služby od svojej banky. Do ponuky v rámci obľúbenej aplikácie Tatra banka predstavila v roku 2020 funkcie investovania do podielových fondov či založenie účtu pre živnostníkov. Medzi významné inovácie zaraďuje aj funkciu Payme, pomocou ktorej je zdieľanie platobných údajov o čosi jednoduchšie.

Takýmto spôsobom vie klient rýchlo a jednoducho vyžiadať platbu a zdieľať platobnú linku či QR kód payme s údajmi komukoľvek. (PayMe, 2022)³⁴

Okrem základnej bankovej aplikácie Mobile má TB vo svojej ponuke aj iné, ktoré uľahčujú a digitalizujú procesy. Jedná sa o MobilePay^{TB}, Čítačka^{TB}, Tatra banka POS a VIAMO. *MobilePay^{TB}* je digitálna peňaženka v podaní Tatra banky. Užívateľ do nej môže nahráť všetky karty od TB, ktoré vlastní a upravovať nastavenia limitov alebo generovať číslo pre platby na internete. Na využívanie kariet v mobile priniesla Tatra banka od roku 2019 pre svojich klientov službu Apple Pay a od 2020 aj Google Pay, pomocou ktorých funguje platobný styk na princípe NFC pre súkromné aj firemné karty. V roku 2020 týmto spôsobom realizovaných približne 12,7 mil. transakcií. Oproti roku 2019, kedy bolo realizovaných približne 5,6 milióna mobilných transakcií ide o približne 2,27-násobný nárast. Bezpečnostným prvkom je v oboch prípadoch biometria, konkrétne tvárová a skenovanie odtlačku prstu, alebo klasické zadanie PIN-u, prvky ktoré zabezpečujú e-karty pri krádeži zariadenia. Užívateľ má možnosť vybrať si prvok alebo viac prvkov jemu najviac vyhovujúcich na bežné používanie. (Výročná správa, 2019)³⁵

TB VIAMO je služba, ktorá uľahčuje posielanie prostriedkov medzi klientami Tatra banky až do hodnoty 1000 Eur denne bez potreby poznania celého čísla účtu či IBAN-u. Mesačný limit takto realizovaných platieb je na úrovni 5000 Eur s jednotlivými transakciami do 1000 Eur/platba. VIAMO je, na rozdiel od ostatných bankových aplikácií, výsledkom spolupráce VÚB banky a Tatra banky z roku 2013 a vo svojej výročnej správe z roku 2018 uvádza, že „*Poslať peniaze kamarátovi by malo byť tak jednoduché, ako mu poslať SMSku*“³⁶ Posielanie peňazí a pripomienok na zaplatenie iným klientom funguje prostredníctvom telefónneho čísla, ktoré je naviazané na účet a slúži ako identifikátor prijímateľa platby. Novinkou je zavedenie využívania tejto funkcie aj klientami iných bánk v Slovensku. V oblasti e-commerce je možné využívať funkcie VIAMO aj na platenie obchodníkom, ktorí majú priradený VIAMO QR kód. Jednotlivé platby posielané cez túto aplikáciu sú autorizované PIN-om.

³⁴ PayMe. *Platiť je rovnako jednoduché ako poslať správy*. [online] [cit. 2022-02-21]. Dostupné na : <https://www.payme.sk>

³⁵ Tatra banka, a.s.. *Výročná správa: Výročná správa 2019*. [online] [cit. 2022-02-21]. Dostupné na :

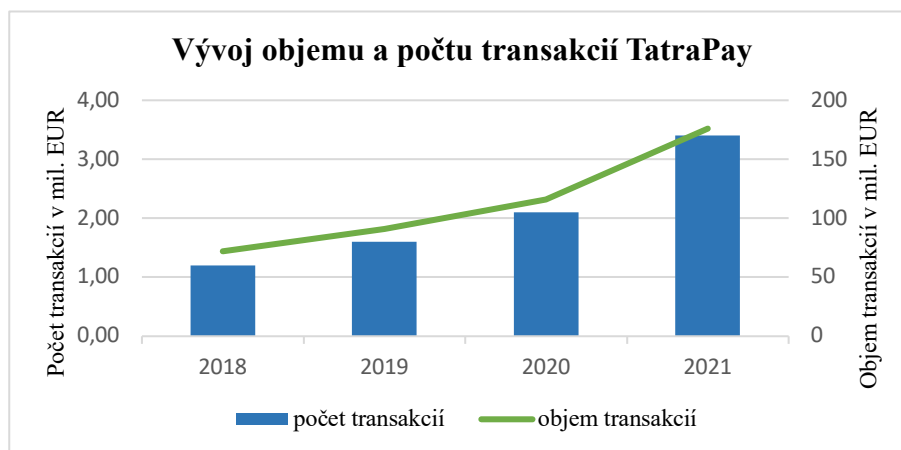
https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyročne-spravy/TB_Vyročna_sprava_2019_web.pdf

³⁶VIAMO, a.s. *Výročná správa 2018: História*. [online] [cit. 2021-09-21]. Dostupné na: <https://viamo.sk/sk/o-nas/>

3.1.4 Bezpečnosť

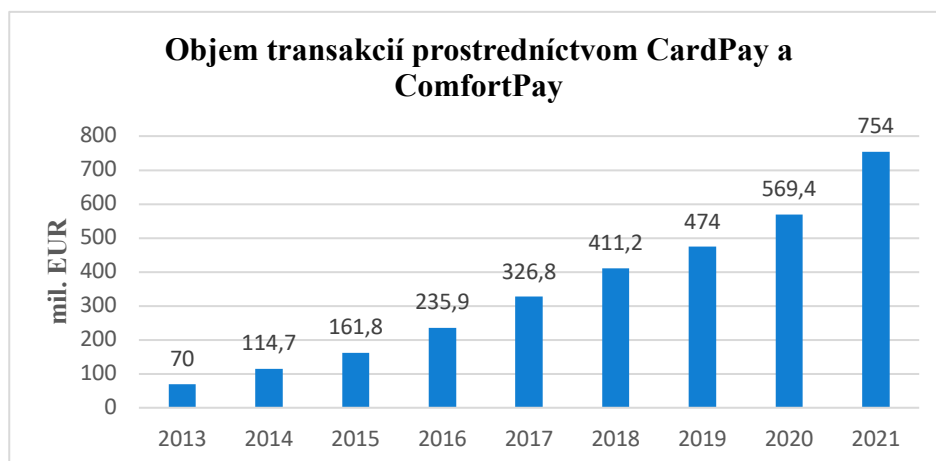
Platobné brány TatraPay, CardPay a ComfortPay

Pre firemných klientov ponúka službu TatraPay, prostredníctvom ktorej môžu zákazníci platiť za tovary či služby cez internet banking či potvrdiť platby cez aplikáciu. Jednoduchšie povedané hovoríme o platobnej bráne, ktorá umožňuje presun prostriedkov prevodom na účet. Výhodami sú rýchlosť a priame prepojenie na banku klienta bezpečným spôsobom. Takto sa zrýchľuje komunikácia medzi retailovými a firemnými klientami Tatra banky. Pre zanalyzovanie toho, či a ako intenzívne klienti využívajú túto službu slúži graf obsahujúci údaje o objeme a počte transakcií prebiehajúcich cez TatraPay za štvorročné obdobie.



Graf 2 Vývoj počtu transakcií TatraPay. Zdroj : Výročné správy Tatra banka, a.s. Vlastné spracovanie.

CardPay je platobná brána, produkt Tatra banky pre firemných klientov ponúkajúci rýchle spracovanie platieb na internete. Zákazníka presmeruje pri platení priamo na platobnú bránu TB, v rámci ktorej zadá údaje o svojej platobnej karte a v prípade potreby dvojitej autorizácie dodatočne presmeruje na 3D Secure zabezpečenie banky, v ktorej má účet. Celý proces transakcie trvá pár sekúnd. *ComfortPay*, taktiež platobná brána, vďaka ktorej zákazníci nemusia neustále zadávať číslo karty a ostatné údaje na uskutočnenia transakcie. Informácie o karte budú uložené šifrovaním bezpečne v TB. Rastúci trend vývoja objemu transakcií spracovaných prostredníctvom týchto platobných brán je zobrazený na grafe. Na základe porovnania rokov 2013 a 2021 vieme povedať, že objem vzrástol za toto obdobie niekoľkonásobne.



Graf 3 Objem transakcií CardPay a ComfortPay. Zdroj: Výročné správy Tatra banka, a.s. Vlastné spracovanie.

Obrázok 2 Platobná brána CardPay. Zdroj : platobnebranky.sk

Tatra banka na dodatočné, dvojfaktorové, zabezpečenie online platieb využíva službu *3D Secure*. 3D je skratka pre 3 domény, ktorými sú zákazník, spoločnosť alebo obchodník, ktorému platba smeruje a zabezpečenie v rámci TB dodatočným potvrdením, na ktoré slúžia SMS kódy, aplikácia, IB, čítačka. *Tvárová biometria TB* je najmodernejším bezpečnostným prvkom dostupným už od roku 2018. V začiatkoch slúžila len na overenie prístupu do aplikácie a na umožnenie otvorenia účtu online formou, od roku 2020 však klienti pomocou nej môžu žiadať online o spotrebný bezúčelový úver. Zabezpečenie telefonickú komunikáciu s DIALOG Live od roku 2013 má na starosti *Hlasová biometria TB*. Predstavuje modernú formu identifikácie klienta na základe porovnania hlasovej nahrávky zaznamenatej v banke. V 2018 roku týmto spôsobom bolo overených viac ako

50% klientov využívajúcich telefonické bankové služby.³⁷ Ako nevýhodu hlasovej biometrie vnímame vyššie riziko krádeže osobných údajov v podobe hlasového záznamu klienta cudzou osobou. Každý záznam, či už fotografie, tváre či hlasu je súčasťou šifrovanej komunikácie s bankou. Vďaka týmto inovatívnym prvkom dokázala Tatra banka zrýchliť procesy z niekoľkých dní či dokonca týždňov na pár minút v pohodlí domova a priblížiť sa tak trendom bankovníctva v Európskej únii.

Medzi hlavné bezpečnostné prvky, ktoré Tatra banka používa v rámci zabezpečenia elektronického bankovníctva patria tzv. IAAP (identifikačné, autorizačné, autentifikačné prostriedky). Prehľad bezpečnostných prvkov zobrazuje tabuľka č.2.

	Bezpečnostný prvok		
Platby	tvárová biometria, odtlačok prsta	PIN	SMS kód/overenie v aplikácií
Internet banking	PID	PIN/heslo	elektronický podpis (pomocou čítačky)
Business banking	PID	heslo	-
Mobile banking	tvárová biometria, odtlačok prsta	PIN	-
DIALOG Live	hlasová biometria	osobitné prvky (otázky)	-
VIAMO	tvárová biometria, odtlačok prsta	PIN	-

Tabuľka 2 Prehľad bezpečnostných prvkov Tatra banky. Vlastné spracovanie.

3.2 Elektronické bankovníctvo 365.bank, a.s.

365.bank, a.s je banka ktorá vznikla na konci roka 2018 ako mobilná banka (predtým odštepny závod Poštová banka a.s.) s cieľom posilňovať inovácie na trhu v rámci ekologickej udržateľnosti a prispôsobenia sa trendom medzi mladými ľuďmi. V roku 2021 sa však rozhodla okrem poskytovania výhradne elektronických služieb zamerať aj na osobnú komunikáciu s klientami a otvoriť svoje prvé pobočky. (Obchodné podmienky 365.bank,

³⁷ Slovenské banky a biometria. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha: 4H production, 2018, roč.25, č.11, 46-47 s. ISSN 1212-4273.

2021)³⁸ Pre celú skupinu Poštovej banky, a.s. išlo o výraznú zmenu, keďže všetky pobočky, okrem tých čo sa nachádzali priamo na pošte, prevzala nová značka 365.bank. Ďalším úspechom je aj získanie ocenenia „Banka roka 2021“ v rámci Slovenskej republiky od prestížneho The Banker magazine za inovácie v bankovej sfére. (365.bank, 2021)³⁹ Pýši sa aj tým, že ako prvá priniesla na slovenský trh digitálne karty a hypotéky. Vo svojom portfóliu elektronického bankingu má mobilnú aplikáciu, detskú aplikáciu Smartie a internet banking pre oblasť retailových klientov. Pre podnikateľov a firemných klientov ponúka online business banking. (365.bank, 2021)⁴⁰

3.2.1 Mobilná aplikácia 365.bank

Aplikácia s názvom 365.bank prináša klientom pohodlné spravovanie účtu v mobile. Klientovi umožňuje online otvorenie účtu či spoločného účtu s iným klientom, sporenie, posielanie žiadostí o úvery online a ďalšie výhodné funkcie. K účtu poskytuje digitálnu platobnú kartu, ktorej nastavenia vie upravovať priamo v aplikácii a využívať ju môže aj pri platení online jednorazovo pretože kartu je možné kedykoľvek zrušiť. Platobný styk sa tak uskutočňuje nie len pomocou služieb ApplePay, GooglePay ale aj Garmin či Fitbit Pay alebo fyzickou kartou, o ktorú môže požiadať priamo v mobile. Okrem bežného účtu ponúka aj založenie až 50 sporiacich účtov a produkt Syslenie, vďaka ktorému sa prostriedky ukladajú na samostatnom mieste buď zaokrúhľovaním zostatku na bežnom účte alebo zaokrúhľovaním jednotlivých vykonaných odchádzajúcich platieb. 365. bank aplikácia pre svojich klientov ponúka digitálne pôžičky až do výšky 20000 eur a hypotekárne úvery, o ktoré môžu požiadať za pár minút.

3.2.2 Internet banking a Business banking

Internet banking je služba internetového bankovníctva 365.banky ktorú poskytuje fyzickým osobám. V tejto webovej aplikácii ponúka rovnaké služby ako v jej mobilnej

³⁸ 365.Bank. *Obchodné podmienky: Obchodné podmienky pre osobné účty s prílohami.* [online]. 20.9.2021.[cit. 2021-09-29]. Dostupné na: <https://365.bank/media/ogxbvdj0/obchodne-podmienky-pre-osobne-ucty-20-9-2021.pdf>

³⁹ Andrej Zaťko. *Trišestpäťka sa stala Bankou roka na Slovensku.* . [online]. 02.12..2021.[cit. 2022-01-28]. Dostupné na: <https://365.bank/blog/moja-365/trisestpatka-sa-stala-bankou-roka-na-slovensku>

⁴⁰ Linda Valko Gáliková. *365.bank vstúpi v lete do novej éry.* [online]. 08.06.2021.[cit. 2022-01-28]. Dostupné na: <https://365.bank/blog/pre-media/365-bank-vstupi-v-lete-do-novej-ery-stane-sa-plnoformatovou-bankou-digitalnou-aj-s-pobočkami-postova-banka-bude-dalej-fungovat-ako-najdostupnejšia-banka-na-poste>

verzií. Na internetovej stránke 365.bank funguje aj online chatbot s menom Peťka, ktorá poradí klientom pri výbere produktov, prihlásení do IB alebo prepojení na operátora v banke. Ekvivalentom pre spoločnosti a podnikateľov je *Business banking*. Pre túto skupinu klientov ponúka produkty:

- *E-obchod* umožňujúci rýchle e-commerce platby na online obchode spoločnosti pre klientov 365.bank. Pri realizovaní platby odkáže klienta priamo na jeho internet banking, kde môže rýchlo a bezpečne zaplatiť svoju objednávku.
- *iTerminál* je služba virtuálneho terminálu na prijímanie online platieb od zákazníkov kartami. V rámci tejto služby funguje zabezpečenie 3D Secure, ktoré ochraňuje pred zneužitím údajov platobnej karty.
- Iné platobné terminály, vrátane mobilného.

Na rozdiel od Tatra banky, 365.bank ponúka jednu aplikáciu, v ktorej sa nachádza aj služba podobná VIAMO, teda funkcia zabezpečujúca posielanie peňazí a ich vyžiadanie v priebehu niekoľkých sekúnd len na základe telefónneho čísla. Týmto spôsobom klienti dokážu rozdeliť platbu alebo poslať žiadosť o vrátenie peňazí viacerým klientom 365.bank naraz. V oblasti elektronického bankovníctva predstavila aj samostatný produkt pre deti s názvom *SMARTIE*. Súčasťou je aplikácia pre rodiča aj pre dieťa, v ktorej spravuje účet naviazaný na účet rodiča a presúva peňažné prostriedky.

3.2.3 Bezpečnosť

Poskytovanie produktov online prináša so sebou aj vyššie nároky na zabezpečenie. Už pri samotnom zakladaní účtu cez IB či aplikáciu musí klient prejsť video hovorom so zamestnancom banky pre dôkladné overenie totožnosti. Ochrana svojich klientov pri platení online má na starosti *3D secure* zabezpečenie. Medzi bezpečnostné prvky EB, ktoré 365.bank v rámci autentifikácie ponúka, sú:

- PIN kód 4 až 6 miestny numerický kód ;
- ePIN ako dodatočný kódy pri 3D Secure;
- PIE kód (Personal Identification Emoji) kód na prihlasovanie v podobe emoji kódu, ktorý používa ako jediná banka na Slovensku;
- biometria.

3.3 Elektronické bankovníctvo VÚB

VÚB alebo Všeobecná úverová banka, je akciová spoločnosť, s veľmi dlhou históriou. Jej zakladateľom je Fond národného majetku v Bratislave. Už od 1990 funguje samostatne vďaka vyčleneniu zo Štátnej banky československej, má niekoľko dcérskych spoločností a získala mnoho prestížnych ocenení. Medzi tie najnovšie patrí ocenenie „Banka roka“ udelené magazínom Trend lebo ocenenie od Global Finance za najlepšie privátne bankovníctvo. Od roku 2001 je súčasťou Intesa Sanpaolo, bankovej skupiny, ktorá je pre VÚB z hľadiska organizačnej štruktúry materskou spoločnosťou. V rámci jej histórie bol veľmi významný rok 2008, pretože sa niesol v duchu zmien a renovácie značky VÚB, a.s.. (VÚB,a.s.)⁴¹ Od 2016 nesie titul prvej banky, ktorá priniesla na Slovensko internetový nákup kreditných kariet. Banka za posledné roky postupne rozvíjala svoje služby aby dosiahla dnešnú úroveň. Elektronické bankovníctvo a jeho rozvoj je pre VÚB veľmi dôležité od roku 2020 má viac ako 900 tisíc používateľov a za rok 2021 sa jej podarilo toto číslo zvýšiť a prekonať 1 milión. (Výročná správa, 2020, 2021)⁴²

VÚB banka ponúka svojim klientom služby IB už veľmi dlho a každým rokom, ako uvádza vo svojich finančných správach, si stanovuje nové ciele v zlepšovaní elektronického bankingu. Svedčí o tom aj počet klientov aktívne využívajúcich ich internetbanking, ktorých počet dosiahol úroveň 500 tisíc už v roku 2020, za čo vďaka vtedy ešte len začínajúcej pandémie. Klienti v dôsledku nutnosti obmedzenia osobného kontaktu začali viac využívať túto formu služieb. Práve COVID-19 a obmedzenia s ním súvisiace naštartovali v bankovom sektore EB viacerých bánk na Slovensku. Spolu s technologickým pokrokom ide o výrazne pôsobiace faktory na využívanie elektronických služieb celosvetovo a očakáva sa, že každým rokom budú banky, vrátane VÚB, presúvať svoje činnosti do online priestoru.

3.3.1 Nonstop banking a internetbanking

⁴¹ VÚB, a.s. *História VÚB banky*. [online] [cit. 2022-02-11]. Dostupné na: <https://www.vub.sk/o-banke/historia-vub/>

⁴² VÚB, a.s. *Konsolidovaná výročná správa 2021*. [online] [cit. 2022-02-11]. Dostupné na: https://www.vub.sk/files/vyročne-spravy/zalozky/ar_2021_sk_s-vyrokom-ev.pdf

VÚB, a.s. *Konsolidovaná výročná správa 2020*. [online] [cit. 2022-02-11]. Dostupné na: https://www.vub.sk/files/vyročne-spravy/zalozky/web_vub_vs-2020_sk.pdf

Vo svojom portfóliu produktov EB má internet banking, mobilnú aplikáciu VÚB, VÚB Viamo a e-platby, ktoré poskytuje v rámci *Nonstop banking* služieb. Internet banking je základnou formou EB ponúkanou vo VÚB banke. Na svojej webovej stránke ponúka priame presmerovanie na prihlasovacie okno do IB. Pre internetbanking VÚB banky je typická prehľadnosť profilu každého klienta. Úvodná stránka ponúka rýchly prehľad produktov daného používateľa či naplánovaných platobných príkazov a inkás v jednoduchom grafickom a číselnom zobrazení. Tak ako každý IB, tak aj ten od VÚB, obsahuje nastavenia profilu, účtu a všetkých kariet klienta. Okrem bežného účtu ponúka online sporenie na maximálne piatich sporiacich účtoch spravovaných v rámci IB, možnosť vykonávania transakcií či žiadanie o pôžičku. Pre tých, ktorí používajú VIAMO ponúka možnosť zadávania platobných príkazov pomocou telefónneho čísla nie len cez aplikáciu ale aj cez IB.

3.3.2 InBiz a Multicash

Fakt, že takmer každá banka má vo svojej ponuke bankovníctvo pre firmy a podnikateľov, je takmer jasný ukazovateľ rozvoja digitalizácie v bankovom sektore. Banka VÚB vytvorila pre týchto klientov internetové bankovníctvo s názvom *InBiz* a *InBiz Mobile* v sekcii firmy a podnikateľa, v rámci ktorého majú umožnené okrem klasických funkcií aj správu účtov prepojených spoločností. Táto webová aplikácia sa však pomerne výrazne líši od klasického IB najmä menej moderným vzhľadom a s tým spojenou nižšou prehľadnosťou. *Multicash* je služba, ktorú banky poskytujú pre firemných klientov vlastniacich minimálne jeden bežný VÚB účet. Táto aplikácia umožňuje jednoduchý prístup k účtom vedeným nie len vo VÚB banke ale vo všetkých, ktoré Multicash ponúkajú. (Obchodné podmienky, 2022)⁴³

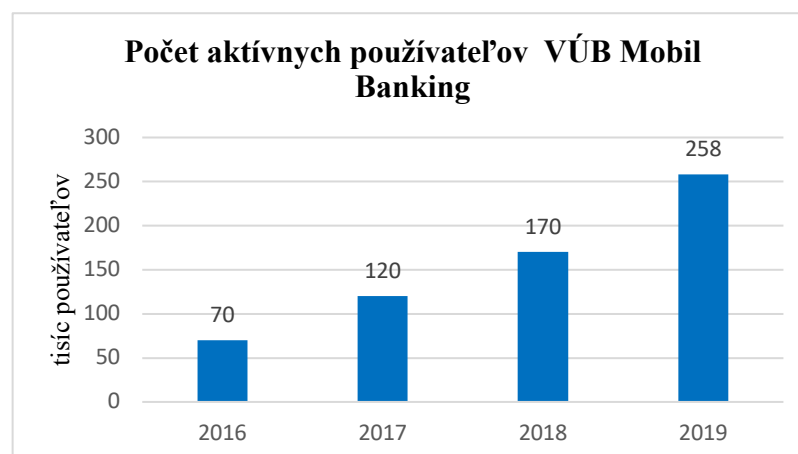
3.3.3 VÚB Mobil Banking

Internet banking aj *InBiz* majú okrem webovej aplikácie aj formu mobilnej aplikácie s rýchlejšim prístupom a praktickými funkciami na každodenné používanie ako napríklad

⁴³ VÚB, a.s. *Obchodné podmienky o zriadení a poskytovaní vybraných bankových služieb prostredníctvom systému MultiCash VÚB*. [online] [cit. 2022-02-12]. Dostupné na: <https://www.vub.sk/files/firmy-podnikatelia/elektronicke-bankovnictvo/multicash/obchodne-podmienky-k-sluzbe-multicash-platne-od-25-2-2022.pdf>

mobilná peňaženka. Platby na princípe NFC prostredníctvom Google či Apple Pay sa stali samozrejmosťou a VÚB ani v tomto trende nezaostáva. Ochrana klientov pri platení je založená na vytvorení tzv. tokenu, ktorý predstavuje vygenerované číslo karty líšiace sa od reálneho čísla na karte. Platenie mobilom taktiež umožňuje *Payme*, služba na posielanie a žiadanie platieb pomocou QR kódov či linkov. Pre urýchlenie platenia faktúr zaviedli funkciu *Scan and Pay*, vďaka ktorej stačí oskenovať QR kód obsahujúci všetky potrebné informácie pre banku na vyplnenie príkazu na úhradu alebo IBAN príjemcu. (Bankovníctví, 2020)⁴⁴VÚB VIAMO, aplikácia na rýchle platby, ktorú bližšie opisujeme v podkapitole Mobilné aplikácie Tatra banky. Rovnako ako pri Tatra banke, slúži na rýchle spracovanie platieb medzi klientami VÚB banky, ktorí majú nainštalovanú aplikáciu, pomocou telefónneho čísla. Denný limit týchto platieb je 1000 Eur pre fyzické osoby a 2000 Eur pre právnické osoby alebo fyzické osoby podnikateľov.

Okrem aktívnych funkcií obsahuje aj tie pasívne ako napríklad kontakt priamo na banku, osobného bankára, archív elektronických výpisov či bezplatné push upozornenia. O výhodách online banky v mobile svedčí aj vývoj počtu jej aktívnych používateľov, ktorý každým rokom výrazne stúpa. V roku 2016 mal Mobil Banking len okolo 70 tisíc používateľov pričom do roku 2019 sa VÚB podarilo toto číslo znásobiť na úroveň viac ako 258 tisíc. Tento vývoj znázorňuje graf č.4.



Graf 4 Počet aktívnych používateľov VÚB Mobile Banking. Zdroj: Výročné správy VÚB, a.s. Vlastné spracovanie.

⁴⁴ Slovenské P2P je tu a volá sa payme. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha: 4H production, 2020, roč. 27. č. 11, s. 46-47. ISSN 1212-4273.

Služba Kontakt je formou elektronického bankovníctva, v rámci které probíhá komunikace telefonicky přímo so zaměstnancem banky. Od roku 2020 je VÚB Mobile Banking přímo připojený s telefonickými službami a klient se tak dokáže spojit s bankou cez aplikáciu. Výhodou je oveľa rýchlejšia a bezpečnejšia komunikácia ako pri klasickom telefonáte, čo v praxi znamená, že klient sa overí vstupom do aplikácie a pri komunikácii so zamestnancom nie je potrebná dodatočná autentifikácia. Týmto spôsobom je možné realizovať rôzne operácie týkajúce sa účtu, kariet či produktov, pri ktorých je potrebné poradenstvo a pomoc.

3.3.4 Bezpečnosť

Služba VÚB pre klientov v oblasti e-commerce má názov platobná brána *eCard*. Tým, čo je to platobná brána a na čo slúži sme sa zaoberali vyššie v texte pri platobných bránach od TB. *eCard* je poskytovaná v niekoľkých jazykoch a podporuje platby v 8 menách. Poskytuje nonstop monitorovanie transakcií zo strany banky a zabezpečenie pomocou 3D Secure. Výhodnou funkciou pre zákazníkov, ktorý nakupujú online, je možnosť nastavenia opakovanej transakcie v prípade potreby.



Obrázok 3 Platobná brána *eCard*. Zdroj: platobnebrany.sk

V dnešnej dobe je čoraz dôležitejšie dbať na zabezpečenie vlastného majetku a majetku klientov. Pri peniazoch a čoraz väčšom online priestore to platí o čosi viac. Práve preto banky, medzi nimi aj VÚB, neustále zlepšujú procesy ochrany svojich klientov. Slúžia im na to ochranné prvky a momentálne aj viacfázové overovanie, ktoré kedysi nebolo bežnou súčasťou aj základných úkonov. Bezpečnostné nástroje, ktorými zabezpečuje

autorizáciu svojich klientov pri vykonávaní rôznych operácií či pri samotnom prihlasovaní, VÚB banka používa:

- SMS overovanie - 5 miestny kód vo forme SMS, ktorý je limitovaný vo VÚB na transakcie do 10 000 Eur na jeden deň;
- token - malé zariadenie slúžiace na generovanie kódov potrebných pre potvrdzovanie operácií, má podobnú funkciu ako čítačka kariet;
- mobilný token - aplikácia určená na overovanie internetových platieb;
- PIN a jednorazový PIN- využíva sa najmä pri potvrdzovaní operácií vo Viamo, MB;
- mPIN - mobilný PIN kód využívaný v aplikácii, IB, overenie pre službu Kontakt, autorizáciu elektronických platieb;
- OTC Token - zariadenie, ktoré slúži na prihlasovanie do InBizu, nahradil donedávna používaný OTP, generuje OTC kód;
- ID (identifikačné číslo);
- biometria - využíva sa najmä pri platbách mobilom, hodinkami, tabletom alebo prihlasovaní do IB či MB.

Stručný prehľad bezpečnostných prvkov využívaných pri vybraných formách EB zobrazuje tabuľka č. 3.

	Bezpečnostný prvok			
Platby	PIN	token/mobilný token	SMS kód	biometria
Internet banking	PIN	token/mobilný token	SMS kód	biometria
InBiz	PIN	OTC token	-	-
Mobile banking	PIN	-	-	biometria
VIAMO	PIN	-	-	biometria

Tabuľka 3 Prehľad bezpečnostných prvkov VÚB, a.s. Vlastné spracovanie.

3.4 Okamžité platby

Aktuálnou novinkou na slovenskom trhu sú tzv. *instant payments* (okamžité platby), ktoré prebiehajú medzi bankami. Konkrétne ide o okamžitú formu platby medzi dvoma účtami, pričom každý z nich je vedený v inej banke. Sú spracované a vyrovnané systémom Target Instant Payment Service v priebehu len niekoľkých sekúnd a je možné ich realizovať každý deň v týždni. Tento systém má aj nadnárodnú úroveň s názvom SEPA Instant Credit Transfer a jeho úlohou je poskytovanie okamžitých platieb medzi 36 krajinami a tým

dosiahnuť rovnaké podmienky pre klientov aj pri platbách do zahraničia. (ECB, 2022)⁴⁵ Okamžité platby sú pomerne nová služba a jej spustenie 4 bankami (VÚB, Slovenská sporiteľňa, Raiffeisen banka a Tatra banka) datujeme k 1. februáru tohoto roka (2022) na základe Národného plánu pre zavedenie okamžitých platieb na Slovensku z roku 2019. Všeobecne nastavený limit na platbu je vo výške až 100 000 Eur no skupina Raiffeisen (Tatra banka a Raiffeisen banka) nastavila svoje limity na 3000 Eur, VÚB a Slovenská sporiteľňa na 5000 Eur. Toto zavedenie má pre klientov týchto bánk veľké výhody a je len otázkou času, kedy ostatné banky na Slovensku začnú nasledovať tento medzinárodný trend a okamžité platby sa stanú bežnou súčasťou každodenného bankovníctva. (NBS, 2019)⁴⁶

3.5 Porovnanie bezpečnosti elektronického bankovníctva vybraných bánk

V rámci tejto bakalárskej práce orientujeme podkapitolu E. porovnaniu bezpečnosti elektronického bankovníctva vybraných troch bánk. Stručné porovnanie zobrazuje tabuľka č. 4.

Tatra banka, a.s.	<ul style="list-style-type: none"> • biometrické bezpečnostné prvky • viacfaktorová autentifikácia platieb a vstupu do elektronického bankovníctva (neobsahuje MlutiCash) • ponúka aj klasické bezpečnostné prvky ako PIN, SMS kód, čítačka kariet • priame upozorňovanie klientov na výskyt hrozieb ako napr. phishing • 3D Secure • vlastné platobné brány • internetová jednorazová platobná karta
365.bank, a.s.	<ul style="list-style-type: none"> • biometrické bezpečnostné prvky • viacfaktorová autentifikácia platieb a vstupu do elektronického bankovníctva • moderné prvky - PIE kód • 3D Secure • bezpečná digitálna platobná karta (možno kedykoľvek zrušiť v aplikácií) • jednorazová platobná karta
VÚB, a.s.	<ul style="list-style-type: none"> • biometrické bezpečnostné prvky

⁴⁵ Európska centrálna banka. *Instant payments: What are instant payments?*. [online] [cit. 2022-02-114]. Dostupné na: https://www.ecb.europa.eu/paym/integration/retail/instant_payments/html/index.sk.html

⁴⁶ Národná banka Slovenska. *Národný plán zavedenia okamžitých platieb v Slovenskej republike*. [online] [cit. 2022-02-114]. Dostupné na: https://www.nbs.sk/img/Documents/PlatobneSystemy/SEPA/Narodny_plan_zavedenia_okamzitych_platieb_v_SR.pdf

	<ul style="list-style-type: none"> • moderný token (generovanie aj v režime offline) • klasické bezpečnostné prvky ako PIN • viacfaktorová autentifikácia platieb a vstupu do elektronického bankovníctva • 3D Secure • vlastná platobná brána • jednorazová internetová platobná karta
--	---

Tabuľka 4 Stručné porovnanie bezpečnostných prvkov vybraných bánk. Vlastné spracovanie.

Z tabuľky vyplýva, že bezpečnostné hľadisko vo vybraných troch bankách na Slovensku sa nachádza približne na rovnakej úrovni. Ak zohľadníme to v akom prostredí tieto banky pôsobia, akú majú históriu a aké je ich zameranie, zistíme jednu veľmi pozitívnu informáciu. Či už v prípade Tatra banky a VÚB ako členov medzinárodných bankových skupín alebo 365.bank ako modernej novej banky na Slovensku, podmienky kladené na bezpečnostné hľadisko vnímajú ako prioritu všetky tri. Vďaka za to najmä technologickému pokroku, ktorý poháňa konkurenciu a banky sú motivované prinášať svojim klientom čo najlepšie a najmodernejšie služby a s nimi spojenú ochranu.

Najviac kreatívnou bankou z hľadiska zavádzania originálnych ochranných prvkov je 365.bank a jej PIE kódu, ktorý oslovuje najmä mladšiu generáciu klientov. Na základe hlbšej analýzy a získania údajov z výročných správ vieme však povedať, že Tatra banka si drží prvenstvo na stupni lídrov v oblasti inovácií v bankovníctve. Aj napriek tomu, že z tabuľky nie je zrejmé, v akom období boli prvky zavedené, na základe bližších údajov z výročných správ vieme posúdiť, že vo väčšine prípadov to bola práve Tatra banka, ktorá priniesla na trh nový trend a zvyšné banky ju nasledovali. V prípade VÚB banky internetbanking aj mobilný banking úspešne konkurujú inovatívnym verziám od Tatra banky a 365.bank. Na druhej strane, internetové bankovníctvo pre firemných klientov pôsobí nemoderne čo môže pôsobiť ako negatívum pre jej klientov.

3.6 Očakávaný vývoj elektronického bankovníctva a bezpečnosti

Elektronické bankovníctvo je oblasť, ktorá neustále napreduje. Vývoj je spôsobený viacerými faktormi ako napríklad technologický pokrok či čoraz viac spomínaná digitalizácia. Začiatky bankového pokroku spájame s ponúkaním bankových služieb mimo pobočiek bánk v pohodlí domova. Dnes je bankový trh zameraný na zlepšovanie a

zrýchľovanie týchto služieb, rozširovanie ponuky a postupné presúvanie bankovej činnosti do online priestoru. V posledných dvoch rokoch vo veľkej miere k vývoju prispela celosvetová pandémia ochorenia Covid-19, ktorá výrazne obmedzila socializáciu a bežný život ľudí. Tak ako každý sektor, tak aj ten bankový bol nútený sa tejto situácií prispôbiť.

Na základe zhodnotenia situácie na bankovom trhu pomocou troch vybraných bánk je možné posúdiť akým smerom sa vývoj uberá a aké trendy nás čakajú. Svoju úvahu by som rozdelila do štyroch pilierov, ktoré sú reprezentované pojmami jednoduchosť, rýchlosť, bezpečnosť a umelá inteligencia. Na tieto vlastnosti berú z môjho pohľadu banky ohľad pri posudzovaní jednotlivých krokov, ktoré ovplyvnia jej budúci vývoj. *Prvým pilierom* je jednoduchosť. Pri pohľade na už existujúce produkty možno zhodnotiť, že procesy budú čoraz viac pozostávať z menšieho množstva krokov a potrebných znalostí na ich vykonanie. Platí to napríklad pri vykonávaní platieb či samotnej obsluhy jednotlivých elektronických foriem bankovníctva. Takmer každá banka sa zameriava na vylepšovanie internet bankingu, mobilného bankingu a ostatných aplikácií z hľadiska prehľadného a intuitívneho použitia. Rovnako môžeme hovoriť o postupnom vylučovaní hotovostných prostriedkov z obehu a ich výmene za elektronickú formu. *Druhým pilierom* je rýchlosť, ktorú vnímam ako veľmi dôležitý faktor ovplyvňujúci postavenie banky na trhu či spokojnosť jej zákazníkov. Vhodným príkladom sú už spomínané okamžité platby, ktoré sú síce dnes už realitou ale zatiaľ v obmedzenom režime. Poskytujú ich len niektoré banky a jedine v mene euro, čo pravdepodobne nie je konečný cieľ Slovenskej republiky, NBS a ECB. Ďalšími príkladmi sú neobmedzené bezkontaktné platby, služby VIAMO alebo komunikácia s bankárom cez aplikáciu, ktoré za posledné roky nesmierne zrýchľujú procesy. Zameraním inovačných projektov práve na tieto oblasti môžu banky znížiť čas klientov strávený vykonávaním bankových procesov a idú ruka v ruke so znižovaním náročnosti ich vykonania. Nachádzame sa v roku 2022, v dobe kedy čas predstavuje veľmi hodnotnú komoditu, a pre uspokojenie potrieb klientov banky musia prichádzať s rýchlejšími ale kvalitnejšími možnosťami. *Tretím pilierom* je nesmierne dôležité bezpečnostné hľadisko každej činnosti vykonávanej online. Napriek neustálemu napredovaniu ochranných prvkov je hrozba zneužitia citlivých informácií stále vysoká. Banky prechádzajú na využívanie modernejších prvkov, viacfaktorové overenia a zložitejšie bezpečnostné systémy. Momentálnym bezpečnostným trendom je biometria, ktorá sa vo veľkej miere používaná pri prihlasovaní do bankovníctva, potvrdzovaní transakcií alebo pri zakladaní účtu cez internet. Je to prvok, ktorý má veľký potenciál z hľadiska nižšej schopnosti zneužitia informácií, a preto si

myslím, že tieto prvky budú využívané a časom nahradia staršie pôvodné PIN kódy či SMS overovacie kódy. Všetko to však závisí od vývoja technológie a zvykov na trhu. Ako *posledný pilier* som vybrala umelú inteligenciu, do ktorej patrí aj spomínaná biometria. Zo všeobecného hľadiska má umelá inteligencia v bankovníctve veľký potenciál najmä z hľadiska zvyšovania efektívnosti bankových procesov, úspory času a šetrenia nákladov z dlhodobého pohľadu. Je pravdepodobné, že tak ako momentálne banky testujú komunikáciu umelej inteligencie s klientami prostredníctvom chatbotov budú jej prvky využívať intenzívnejšie a postupne sa vďaka nej presunú aj zvyšné aktivity zamestnancov do internet bankingu či aplikácii.

Záver

V bakalárskej práci som sa zamerala na tému elektronického bankovníctva z pohľadu jeho bezpečnosti a aktuálnych trendov na Slovenskom trhu. Mojim cieľom bolo spracovanie výsledkov analýzy, identifikácia rozdielov v elektronickom bankovníctve troch bánk reprezentujúcich bankový trh, porovnanie bezpečnostnej stránky elektronických bankových procesov a formulovanie očakávaného vývoja Slovenského bankovníctva na základe trendov. Pri jeho dosahovaní som sa orientovala na prehľadné poskytnutie informácií o jednotlivých elektronických systémoch a spôsoby autentifikácie klientov.

Z hľadiska šírky ponuky jednotlivých bánk je zrejmé, že konkurencia ich motivuje k poskytovaniu čo najlepšieho internetbankingu, mobile bankingu a ostatných foriem elektronického bankovníctva. Bankovníctvo je vo všeobecnosti neustále vyvíjajúci sa sektor, v ktorom sa kladie veľký dôraz práve na bezpečnostnú stránku, čo sa prejavuje najmä pokročilejšími technológiami zabezpečujúcimi overovanie totožnosti a viacfaktorovými autorizáciami. V roku 2019 sa k bežným hrozbám (napr. phishing, carding) pridala pandémia COVID-19, ktorá pôsobila ako katalyzátor v ére digitalizácie a banky tak urýchlili presun svojich služieb do online priestoru. Aj práve preto sú bezpečnostné opatrenia pre banky veľmi dôležité.

Trendy vo svete nevznikajú podľa vopred určených pravidiel a inak tomu nie je ani vo svete bankovníctva, a preto som moju činnosť orientovala na posúdenie aktuálnej situácie so zámerom identifikovať prebiehajúce trendy a očakávania. Pre potreby získania informácií o trhu bankovníctva v podmienkach Slovenskej republiky je práca z veľkej časti venovaná analýze systémov elektronického bankovníctva Tatra banky, 365.bank a VÚB banky a ich následnému porovnaniu. Bezpečnostné hľadisko procesov prebiehajúcich online je v digitálnej dobe veľmi dôležité a mnou vybrané banky ho vnímajú ako prioritu. Aj napriek ich rozdielnosti sa všetky zameriavajú na zlepšovanie a skvalitňovanie svojho elektronického bankovníctva podľa aktuálnych trendov. U klientov sledovaných bánk je čoraz populárnejšia forma mobilného bankingu. Tento fakt sa následne odráža vo vysokej miere poskytovaného zabezpečenia a pokročilej ochrane voči hrozbám v podobe biometrických prvkov v slovenskom bankovníctve.

Služby elektronického bankovníctva sa budú aj naďalej rozvíjať. Ich úroveň bude daná dostupnosťou vyspelých technológií u klientov a zároveň ochotou a motiváciou poskytovať jednoduchý prístup k službám pri zohľadnení rizík spojených s IT technológiami.

Použitá literatúra

BELÁS, Jaroslav. *Manažment komerčnej banky*: 1. vyd. Trenčín: GC-TECH Ing. Peter Gerši, 2007, 315 s. ISBN 978-80-969189-7-3.

BOUŠKOVÁ, Dagmar. *Bankové operácie*: 1. vyd. Bratislava: Vydavateľstvo EKONÓM, 2006, 234 s. ISBN 80-225-2136-1.

CRONIN, Mary J. *Banking and Finance on the Internet*: 1. vyd. Canada: John Wiley and Sons, 1998, 156 s. ISBN 0-471-29219-2.

GKOUTZINIS, Apostolos. *Internet banking and the law in Europe*: 1. vyd. New York: Cambridge University Press, 2006, 404 s. ISBN 0-521-86071-7.

Google Pay má na Slovensku rok. Čaká na konkurenciu od Apple. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha :4H production, 2019, roč.26, č.4., s. 46-47. ISSN 1212-4273.

HORVÁTOVÁ, Eva. *Bankovníctvo*: 1. vyd. Žilina: GEORG Žilina, 2009, 318 s. ISBN 978-80-89401-03-1.

MAJERČÁKOVÁ, Daniela. *Peniaze a bankovníctvo*: 1. vyd. Praha: Wolters Kluwer, 2018, 192 s. ISBN 978-80-7552-972-5.

POLOUČEK, Stanislav. *Bankovníctví* : 2. vyd. Praha: C. H. Beck, 2013, 480 s. ISBN 978-80-7400-491-9.

Pobočky sú stále dôležité. *Obchod: marketing, retail, FMCG*. Bratislava: MAFRA, 2020, roč. 25, č. 4, 34 s. ISSN 1335-2008.

Slovenské banky a biometria. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha: 4H production, 2018, roč. 25, č. 11, s. 46-47. ISSN 1212-4273.

Slovenské P2P je tu a volá sa payme. *Bankovníctví: odborný měsíčník pro profesionální finance*. Praha: 4H production, 2020, roč. 27. č. 11, s. 46-47. ISSN 1212-4273.

ŠTARCHOŇ, Peter. *Bankový marketing: princípy a špecifiká*: 1. vyd. Praha: Wolters Kluwer, 2017, 120 s. ISBN 978-80-7552-948-0.

Internetové zdroje

Andrej Zaťko. *Trišesťpäťka sa stala Bankou roka na Slovensku*. . [online]. 02.12..2021.[cit. 2022-01-28]. Dostupné na: <https://365.bank/blog/moja-365/trisestpatka-sa-stala-bankou-roka-na-slovensku>

DUPAS, Muriel-GREBE, Michael. *Global Retail Banking 2017: Accelerating Bionic Transformation*. [online]. 2017. [cit. 2021-10-11]. Dostupné na: <https://www.bcg.com/publications/2017/financial-institutions-global-retail-banking-2017-bionic-transformation>

Europol. *International ATM Skimming Network Dismantled in Italy*. [online]. 2016. [cit.2021-10-11]. Dostupné na: <https://www.europol.europa.eu/media-press/newsroom/news/international-atm-skimming-network-dismantled-in-italy>

Európska centrálna banka. *Instant payments: What are instant payments?*. [online] [cit.2022-02-114]. Dostupné na: https://www.ecb.europa.eu/paym/integration/retail/instant_payments/html/index.sk.html

Európska centrálna banka. *Money, credit and banking: Electronic Money*. [online] [cit.2021-10-11]. Dostupné na: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

Európska centrálna banka. *Payments and markets glossary: e-commerce*. [online] [cit.2021-10-15]. Dostupné na: <https://www.ecb.europa.eu/services/glossary/html/act7e.en.html>

Linda Valko Gáliková. *365.bank vstúpi v lete do novej éry*. [online]. 08.06.2021. [cit. 2022-01-28]. Dostupné na: <https://365.bank/blog/pre-media/365-bank-vstupi-v-lete-do-novej-ery-stane-sa-plnoformatovou-bankou-digitalnou-aj-s-pobockami-postova-banka-bude-dalej-fungovat-ako-najdostupnejšia-banka-na-poste>

Mbank. *Ako chránime vaše osobné údaje a čo je GDPR?* [online] [cit. 2021-10-25]. Dostupné na: <https://www.mbank.sk/gdpr/#uvod>

MFSR. *Finančný trh: Obmedzenie platieb v hotovosti*. [online] [cit. 2021-09-25]. Dostupné na : <https://www.mfsr.sk/sk/financie/financny-trh/obmedzenie-platieb-hotovosti/>

Národná banka Slovenska. *Dohľad nad finančným trhom: Biometria*. [online] [cit. 2021-09-23]. Dostupné na: <https://www.nbs.sk/sk/dohlad-nad-financnym-trhom/fintech/biometria>

Národná banka Slovenska. *Národný plán zavedenia okamžitých platieb v Slovenskej republike*. [online] [cit. 2022-02-114]. Dostupné na: https://www.nbs.sk/_img/Documents/_PlatobneSystemy/SEPA/Narodny_plan_zavedenia_o_kamzitych_platieb_v_SR.pdf

Národná banka Slovenska. *Otázky a odpovede k platbám kartami na internete*. [online] [cit. 2021-10-10]. Dostupné na: https://www.nbs.sk/sk/informacie-pre-media/tlacove-spravy/spravy-vseobecne/detail-tlacovej-spravy/_otazky-a-odpovede-k-platbam-kartami-na-internete-od-1-1-2021

PayMe. *Platiť je rovnako jednoduché ako posilať správy*. [online] [cit. 2022-02-21]. Dostupné na : <https://www.payme.sk>

Poštová banka. *Novinky: Čo je CVC kód a kde sa na karte nachádza?*. 2016. [online] [cit. 2021-10-15]. Dostupné na: <https://www.postovabanka.sk/novinky/blog/co-je-cvc-kod-a-kde-sa-na-karte-nachadza/>

Slovenská Banková Asociácia. *Ako je to naozaj. Opatrenia proti phishingu.* [online], 2015, [cit. 2021-10-11]. Dostupné na: <https://www.sbaonline.sk/novinka/ako-to-je-naozaj-opatrenia-proti-phishingu/>

SLSP. *Bezpečnosť: Čo vám hrozí.* [online] [cit. 2021-10-12]. Dostupné na: <https://www.slsk.sk/sk/ludia/bezpecnost/co-vam-hrozi> cit[09-10-2021]

Tatra banka, a.s.. *Internetbanking: Limity pre platby.* [online] [cit. 2022-02-23]. Dostupné na : <https://www.tatrabanka.sk/sk/personal/ucet-platby/internet-banking/>

Tatra banka, a.s.. *Výročné správy: Výročná správa 2017.* [online] [cit. 2022-02-21]. Dostupné na : https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyrocnne-spravy/TB_Vyrocnna_sprava_2017.pdf

Tatra banka, a.s.. *Výročné správy: Výročná správa 2018.* [online] [cit. 2022-02-21]. Dostupné na : https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyrocnne-spravy/TB_Vyrocnna_sprava_2018_SK_web.pdf

Tatra banka, a.s.. *Výročné správy: Výročná správa 2019.* [online] [cit. 2022-02-21]. Dostupné na : https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyrocnne-spravy/TB_Vyrocnna_sprava_2019_web.pdf

Tatra banka, a.s.. *Výročné správy: Výročná správa 2020.* [online] [cit. 2022-02-27]. Dostupné na : https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyrocnne-spravy/TB_Vyrocnna_sprava_2020_SK_web.pdf

Tatra banka, a.s.. *Výročné správy: Výročná správa 2021.* [online] [cit. 2022-03-27]. Dostupné na : <https://www.tatrabanka.sk/files/archiv/financne-ukazovatele/vyrocnne-spravy/VyrocnaspravaTatrabanky2021.pdf>

VÚB, a.s. *História VÚB banky.* [online] [cit. 2022-02-11]. Dostupné na: <https://www.vub.sk/o-banke/historia-vub/>

VÚB Banka. *Internet banking: Bezpečnosť IB.* [online] [cit. 2021-09-25]. Dostupné na : https://www.vub.sk/elektronicke-bankovnictvo/internet-banking/bezpecnost-ib/#tab_2

VIAMO, a.s. *Konsolidovaná výročná správa 2018.* [online] [cit. 2021-09-21]. Dostupné na: https://www.vub.sk/files/ludia/sekundarna-navigacia/financne-ukazovatele/vyrocnne-spravy/najnovsie-vyrocnne-spravy/vs_vub_2018_sk_web.pdf

VÚB, a.s. *Konsolidovaná výročná správa 2020.* [online] [cit. 2022-02-11]. Dostupné na: https://www.vub.sk/files/vyrocnne-spravy/zalozky/web_vub_vs-2020_sk.pdf

VÚB, a.s. *Konsolidovaná výročná správa 2021.* [online] [cit. 2022-02-11]. Dostupné na: https://www.vub.sk/files/vyrocnne-spravy/zalozky/ar_2021_sk_s-vyrokom-ey.pdf

VÚB, a.s. *Obchodné podmienky o zriadení a poskytovaní vybraných bankových služieb prostredníctvom systému MultiCash VÚB.* [online] [cit. 2022-02-12]. Dostupné na:

<https://www.vub.sk/files/firmy-podnikatelia/elektronicke-bankovnictvo/multicash/obchodne-podmienky-k-sluzbe-multicash-platne-od-25-2-2022.pdf>

VÚB Banka. *Poznáte rozdiel medzi debetnou a kreditnou kartou? Dôležité fakty, ktoré by ste mali vedieť.* 2021, [online][cit. 2021-10-15]. Dostupné na: <https://www.vub.sk/jednovubky/poznate-rozdiel-medzi-debetnou-kreditnou-kartou/>

365.Bank. *Obchodné podmienky: Obchodné podmienky pre osobné účty s prílohami.* [online]. 20.9.2021.[cit. 2021-09-29]. Dostupné na: <https://365.bank/media/ogxbvdj0/obchodne-podmienky-pre-osobne-ucty-20-9-2021.pdf>

Právne normy

Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 z 27.4.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov

Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 272/2016 Z. z. Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov