Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Aplikace pro mobilní bankovnictví

Petr Svoboda

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Petr Svoboda

Podnikání a administrativa

Název práce

Aplikace pro mobilní bankovnictví

Název anglicky

Mobile Banking Application

Cíle práce

Hlavním cílem bakalářské práce bude analýza a porovnání aplikací pro mobilní bankovnictví. Práce bude orientována na aplikace bank působících v České republice.

Dílčí cíle práce jsou:
- charakterizovat současné bankovní aplikace s důrazem na bezpečnostní prvky
- analyzovat a porovnat vybrané mobilní aplikace českých bank
- v praktické části pomocí vhodných metod a postupů zhodnotit aplikace pro mobilní bankovnictví na platformě Apple
- formulovat výsledky a závěrečná doporučení

Metodika

Teoretická část bude zpracována za pomoci studia odborné literatury a vhodných internetových zdrojů.

Bude provedena analýza aplikací v rámci celkového procesu používání mobilního bankovnictví.

Vlastní řešení bakalářské práce bude realizováno porovnáním aplikací českých bank dostupných v App Store pro iOS

Na závěr práce bude zajištěna syntéza získaných poznatků a budou formulovány výsledky práce a doporučení.

Doporučený rozsah práce

35

Klíčová slova

apple, iOS, mobilní, internetové, bankovnictví, aplikace, zabezpečení

Doporučené zdroje informací

ALLEN, G. *Android 4 : průvodce programováním mobilních aplikací.* Brno: Computer Press, 2013. ISBN 978-80-251-3782-6.

LASHINSKY, A. *Do nitra společnosti Apple : jak skutečné funguje nejobdivovanější firma světa = Inside Apple : how America's most admired-and secretive-company really works.* Brno: Computer Press, 2013. ISBN 978-80-251-3778-9.

MÁČE, M. *Platební styk : klasický a elektronický.* Praha: Grada, 2006. ISBN 80-247-1725-5.

POLOUČEK, S. *Bankovnictví.* V Praze: C.H. Beck, 2013. ISBN 978-80-7400-491-9.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

doc. Ing. Zdeněk Havlíček, CSc.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 21. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 07. 03. 2017

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Aplikace pro mobilní bankovnictví" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2017 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce doc. Ing. Zdeňku Havlíčkovi, CSc. za odborné vedení a cenné rady při konzultacích a zpracování bakalářské práce.

Aplikace pro mobilní bankovnictví

Souhrn

Cílem bakalářské práce je analyzovat a porovnat vybrané aplikace pro mobilní bankovnictví na platformě Apple. Teoretická část je zaměřena na vymezení základních pojmů z oblasti elektronického bankovnictví a sním spojených nových technologií, legislativní úpravy platebního styku a přehledu funkcionalit aplikací pro mobilní bankovnictví. Dále je představena mobilní platforma Apple, její vývoj, bezpečnostní prvky a hrozby.

V praktické části jsou charakterizovány čtyři vybrané aplikace českých bank pro mobilní platformu Apple. Na základě kritérií cena, optimalizace, recenze, uživatelská zkušenost a zabezpečení je sestaven model vícekriteriální analýzy variant, který pomocí metody analytického hierarchického procesu určí kompromisní variantu a pořadí vybraných aplikací.

Na základě výsledků jsou zformulována doporučení pro uživatele a určeny hlavní oblasti, ve kterých by aplikace, jež podle vyhodnocení nelze doporučit, měly vylepšit své funkcionality a vlastnosti.

Klíčová slova: bankovnictví, internetové, mobilní, smartbanking, aplikace, zabezpečení, bezpečnostní hrozby, Apple, iOS, QR

Mobile Banking Application

Summary

The aim of this bachelor thesis is to analyse and compare selected mobile banking applications on the Apple platform. The theoretical part focuses on defining the basic terms of electronic banking and accompanying new technologies. The next part is focused on electronic payments regulations and legislation and outline of mobile banking applications functionalities. The next is introduction of Apple mobile platform, its evolution, safety features and security threats.

The practical part of the thesis characterizes four selected Czech mobile banking applications suitable for apple platform. Based on the criteria: price, optimization, review, user experience and security, the applications are compared using methods of analytic hierarchy process to choose a compromise and determine the order of results.

The results are assigned to define user recommendations and to suggest improvements in functionalities and features for applications with result classification: not recommended.

Keywords: banking, internet, mobile, smartbanking, application, security, security threats, Apple, iOS, QR,

Obsah

1 Úvod

V posledních deseti letech došlo k dynamickému rozvoji v oblasti mobilních zařízení s operačními systémy, které umožňují instalaci sofware třetích stran. Zlomovým momentem ve vývoji tzv. chytrých telefonů a tabletů bylo představení mobilního telefonu Apple iPhone v roce 2007. Právě z tohoto důvodu byl v této bakalářské práci vybrán mobilní operační systém iOS, jako platforma pro mobilní bankovní aplikace.

Formy bezhotovostního platebního styku se postupem s rozvojem techniky měnily a bankovní sektor tento vývoj reflektoval. Proto banky začaly svým klientů nabízet služby přímého bankovnictví, díky kterému šetří čas a peníze uživatelům, a především vlastní náklady na provoz poboček. Uživatelům umožňuje správu bankovních účtů prostřednictvím zařízení, která jsou součástí domácností a firem, jimž dovoluje kontrolu svých peněžních prostředků kdykoliv a kdekoliv, bez nutnosti návštěvy pobočky.

Téměř každá komerční banka již v dnešní době nabízí řešení pro mobilní operační systémy, které se navzájem liší v dílčích funkcionalitách, způsobu zabezpečení, v jednoduchosti a přehlednosti uživatelského rozhraní a výši poplatků za jednotlivé služby spojených s využíváním aplikace pro mobilní bankovnictví. Za účelem výběru vhodného řešení a poskytovatele je nutné zvolit a analyzovat aplikace podle předem určených kritérií, z nichž nejdůležitější jsou zabezpečení a uživatelská zkušenost.

Podnětem pro výběr daného tématu je aktuálnost a zájem o analýzu nejvhodnější aplikace pro mobilního bankovnictví. Rychlý vývoj mobilních zařízení je trend posledních několik let, který bude pravděpodobně pokračovat i v blízké budoucnosti. Spolu se změnou uživatelských návyků klientů komerčních bank se jedná o hlavní argument, proč získávat v dané oblasti aktuální informace.

Cíl práce a metodika

1.1 Cíl práce

Hlavním cílem bakalářské práce je analyzovat a porovnat aplikace pro mobilní bankovnictví. Práce je orientována na aplikace bank působících v České republice.

Dílčí cíle práce jsou:

- charakterizovat současné bankovní aplikace s důrazem na bezpečnostní prvky
- analyzovat a porovnat vybrané mobilní aplikace českých bank
- v praktické části pomocí vhodných metod a postupů zhodnotit aplikace pro mobilní bankovnictví na platformě Apple
- formulovat výsledky a závěrečná doporučení

1.2 Metodika práce

Teoretická část bude založena na studiu odborné literatury a vhodných internetových zdrojů zaměřených na oblast elektronického bankovnictví a mobilní platformy Apple.

V praktické části bude provedena analýza aplikací pro mobilní bankovnictví českých bank dostupných v App Store pro iOS v rámci celkového procesu používání mobilního bankovnictví.

Na závěr bude provedena syntéza získaných poznatků z teoretické i praktické části, na jejichž základě budou formulovány výsledky práce a doporučení.

2 Přehled řešené problematiky

2.1 Platební styk

Platební styk je definován jako přesun hotovostních a bezhotovostních prostředků mezi plátcem a příjemcem, kterými mohou být fyzické i právnické osoby. Realizace platebního styku může probíhat v rámci jednoho státu i mezinárodně, a to prostřednictvím služeb peněžního ústavu. V případě hotovostního styku není účast peněžního ústavu podmíněna a jedná se o přesun finančních prostředků v hotovosti za použití zákonných platidel mezi plátcem a příjemcem. U bezhotovostního styku dochází k úhradě bezhotovostním převodem na účtech plátců a příjemců u bank prostřednictvím tzv. „účetních peněz“. Teritoriálně je možné platební styk rozdělit na tuzemský (subjekty uvnitř ekonomiky, zpravidla místní měna), zahraniční (tuzemské a zahraniční subjekty včetně tuzemských subjektů v zahraničí) a přeshraniční mezi subjekty tuzemskými s vazbou na zahraniční ze zemí Evropského hospodářského prostoru. (Máče, 2006)

2.1.1 Bezhotovostní platební styk

Spolu s rozvojem techniky docházelo současně k rozvoji nástrojů pro bezhotovostní platební styk, ke kterému je nezbytné vlastnit bankovní účet, jenž se skládá ze dvou částí. Prvním je identifikátor účtu klienta (číslo účtu) a druhou částí je kód platebního styku (kód banky), jedinečný kód pro každou obchodní banku působící v ČR, stanovený ČNB. Pro přeshraniční platby se používá formát IBAN, definovaný standardem ISO 13616, který je doplněný o kód země a kontrolní číslem. (Kalabis, 2012)

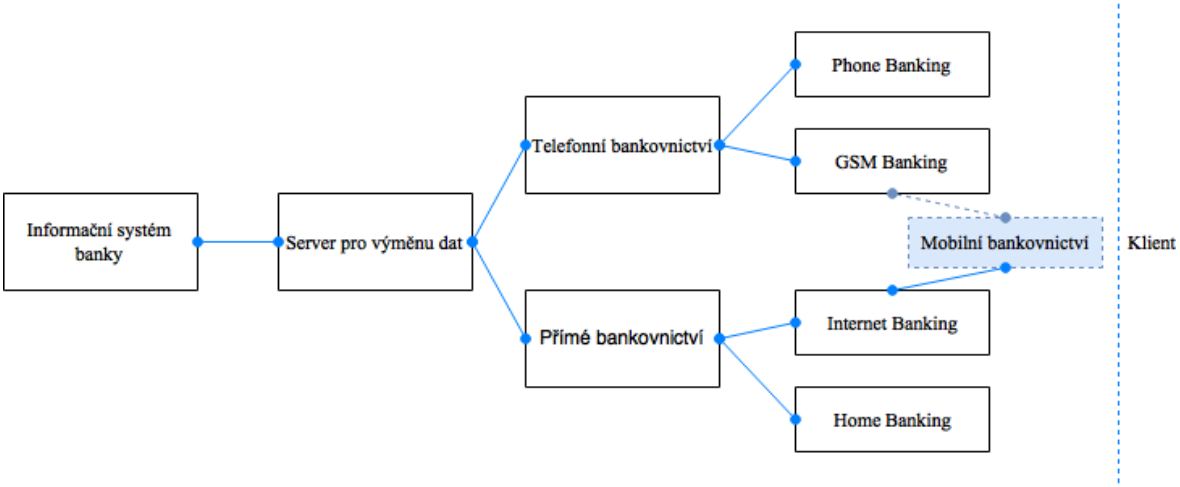
První formou vzdálené komunikace mezi bankou a klientem byl telefon. Klient se v tomto případě identifikoval pouze jménem a autentizace byla prováděna nadiktováním hesla. Poté se využíval fax, kde pro zabezpečení byly používány kódové tabulky. (Máče, 2006)

S rozvojem počítačové techniky došlo k rozšíření komunikace při platebním styku na 24 hodin denně, 7 dní v týdnu. K tomu je nutné zabezpečené připojení mezi komunikačními servery banky a uživatelských aplikací. Tato forma bankovnictví

znamená úsporu času a nákladů pro klienty a banky, která může vést ke zvýšení produktivity. (Kalabis, 2012)

Realizace vzdálené komunikace mezi klientem a bankou je v současné době uskutečňována na dvou základních způsobech ovládání účtu.

Obrázek 1 - Formy komunikace mezi bankou a klientem



Zdroj: (Máče, 2006), vlastní zpracování

2.1.1.1 Phone banking

Komunikace pomocí Phone banking probíhá prostřednictvím pevné linky a mobilního telefonu. Klient svým hlasem, nebo tlačítky komunikuje s živým telefonním bankéřem, respektive hlasovým informačním systémem. Klientovi umožní sledovat stav účtu, zadávat příkazy k úhradě a inkasu, spravovat trvalé příkazy a termínované vklady. (Kalabis, 2012)

Pro zřízení této služby je nutné navštívit pobočku, kde dojde k uzavření smlouvy a přidělení speciálního kódu, který slouží k autorizaci uživatele při každém hovoru. I vzhledem k možnosti komunikace s živým pracovníkem, je cena této formy bankovnictví zpravidla nejdražší. Dalšími nevýhodami je možnost jednoduchého zneužití s potřebou pouze jednoho identifikačního údaje a omezená nabídka služeb přes tento kanál. (Máče, 2006)

2.1.1.2 GSM banking

Jedná se o formu bankovnictví, ke které je zapotřebí mobilní telefon. První možností je využití technologie WAP, která umožní mobilnímu telefonu přístup k internetu. WAP

stránky banky jsou speciálně upravené pro zobrazení na malém displeji mobilního telefonu. Druhou možností je SIM toolkit zajišťující šifrovaní SMS zpráv, pomocí kterých klient zadává příkazy. SIM toolkit je nahrán přímo na SIM kartu v telefonu. (Máče, 2006) S nástupem chytrých telefonů se zmiňované způsoby ovládání účtu staly zastaralými.

2.1.1.3 Home banking

Forma založená na propojení osobního počítače klienta s bankovními servery za pomoci internetového připojení. Na počítači klienta je nainstalován speciální software, který umožňuje bezpečné a spolehlivé zadávání operací pro platební styk a kontrolu nad peněžními prostředky. Bezpečnost je založena na základě přihlašovacích údajů a elektronického podpisu. Hlavní nevýhodou služeb home banking je skutečnost, že software je vázaný na konkrétní počítač. Alternativou, která nabízí podobné služby a není vázána na konkrétní hardware je internet banking. (Máče, 2006)

2.1.1.4 Internet banking

Internetové bankovnictví představuje pro klienta jednoduchou formu obsluhy svého účtu pouze s počítačem, internetovým připojením a prohlížečem. Umožňuje přístup a provádění operací nepřetržitě v průběhu dne z libovolného počítače. Nabízí obdobné služby jako ostatní formy, velkou výhodou je získávání výpisů z účtu v elektronické podobě bez nutnosti nákladného zasílání poštou a v kratších časových intervalech. K přihlášení do služby internet banking je zapotřebí kombinace dvou až tří přístupových údajů a k potvrzení operace například autentizační kód zaslaný pomocí SMS, nebo například podpisový certifikát. (Kalabis, 2012)

2.1.1.5 Smart banking

Předchůdcemi internetového bankovnictví pro chytré telefony, dnes označovaného jako Smart banking, jsou jednoznačně PDA banking a Java banking. První zmíněná forma využívá mobilní zařízení PDA (Personal Digital Asistent) připojené k internetu pomocí datové připojení GPRS v GSM sítí, která je předchůdcem v dnešní době rozšířených 4G LTE sítí, nebo klasické připojení Wi-Fi. Java banking využívá aplikace typu Java nahranou do klasického mobilního telefonu s připojením k mobilní datové síti. (Kalabis, 2012)

Obě výše zmíněné formy jsou v dnešní době překonány díky rozšíření chytrých mobilních telefonů a dalších zařízení s mobilním operačním systémem, pro které jsou vyvíjeny mobilní aplikace. Rozsah služeb a funkcionalit je analogický ostatním formám přímého bankovnictví.

2.1.2 **Legislativní úprava elektronického bankovnictví**

Vzhledem k prudkému nárůstu významu elektronického bankovnictví je daná oblast právně upravena na úrovni evropského práva. Existují tři základní směrnice a jedno doporučení, které lze považovat za nezbytné pro tuto oblast.

1) Směrnice č. 2000/46/ES o přístupu k činnosti institucí elektronických peněz, která má za cíl zvýšit důvěru a právní jistotu klientů k elektronickým platebním prostředků a jejím hlavním úkolem je kontrola emise elektronických peněz.
2) Směrnice č. 2002/65/ES zvyšující ochranu spotřebitele před poskytovateli finančních služeb. Ukládá povinnost poskytnout spotřebiteli komplexní informace před uzavřením smlouvy a možnost do 14 dnů odstoupit. Dále zakazuje nekalé marketingové a jiné praktiky, jako například telefonní hovory, které by přiměly spotřebitele ke koupi nevyžádané služby
3) Směrnice č. 97/7/ES upravující ochranu spotřebitele v případě smluv uzavřených na dálku a postup v případě zneužití platební karty
4) Doporučení č. 97/489/ES vyjasňující vztah mezi vydavatelem a držitelem v případě provádění operací elektronickou cestou
   (Máče, 2006)

V České republice neexistuje norma, která by přímo upravovala samotné formy elektronického bankovnictví, avšak platební styk, pod který spadá klasická i elektronická podoba, upravuje Zákon o platebním styku č. 284/2009 Sb. Ten byl naposled novelizován Zákonem č.452/2016 Sb., jenž je účinný od 1.3.2017. Předmětem úpravy Zákonu o platebním styku je:

1) Činnost některých osob oprávněných poskytovat platební službu a vydávat elektronické peníze
2) Účast v platebních systémech a vznik a provozování platebních systémů

3) Práva a povinnosti poskytovatelů a uživatelů platebních služeb
4) Práva a povinnosti vydavatelů a držitelů elektronických Zákon také zapracovává směrnice a nařízení Evropské unie, například Nařízení Evropského parlamentu a Rady č. 924/2009 o přeshraničních platbách ve Společenství.

(Zákon č.284/2009 Sb., 2017, citování online 3.3.2017)

Dalším zákonem je Zákon o bankách č.21/1992 Sb., který v oblasti elektronického bankovnictví upravuje činnost bank na českém území.
(Zákon č.21/1992 Sb., 2017, citováno online 14.1.2017)

V případě zřízení služeb elektronického bankovnictví uzavírá klient s finanční institucí smlouvu, jejíž součástí jsou všeobecné obchodní podmínky, které obsahují práva a povinnosti obou smluvních stran. Podpisem smlouvy s těmito podmínkami klient souhlasí, proto je nutné se s nimi seznámit, vzhledem k tomu, že se u jednotlivých finančních institucí můžou lišit.
(Schlossberger, 2005)

2.2 Mobilní bankovnictví

Mobilní platforma má schopnost transformovat vztahy finančních institucí s jejich klienty. Vzhledem k tomu, že služby mobilního bankovnictví pracují mimo tradiční infrastrukturu, jako jsou například bankomaty a pobočky, měly by banky uvažovat o budoucnosti mobilních aplikacích jako o náhradě této infrastruktury, a proto do jejich inovace vložit maximum.
Vývoj mobilních zařízení nutí banky vyvíjet své služby, aby splnily očekávání svých klientů a jejich rostoucí požadavky. Vývoj by se měl zaměřit zejména na oblast vylepšení funkcionalit pro spokojenost klienta, poskytování co možná nejlepšího zabezpečení a vylepšování stávajících řešení.
Mnoho klientů velkých bank používá internetové bankovnictví, ale pouze zlomek používá mobilní bankovnictví. Tento podíl však neustále roste, proto se banky na tuto oblast s rozvojem mobilních zařízení soustředí čím dál tím více.
(Nicoletti, 2014)

2.2.1 **Aplikace pro mobilní bankovnictví**

V roce 2015 se prostřednictvím mobilní zařízení k internetu připojovalo přes 40 % obyvatel ČR, oproti roku 2012 se jedná o více než čtyřnásobný nárůst hodnot. (Český statistický úřad, 2016, citováno online 29.12.2016)

Z toho důvodu už téměř každá česká banka nabízí aplikaci pro smartbanking, která jim umožňuje správu účtu přes chytrý telefon nebo tablet. Zpravidla se uživatelům nabízí verze pro mobilní operační systémy Android OS a iOS. Některé banky nabízejí variantu pro Windows 10 Mobile a starší verzi mobilního OS od Microsoft – Windows Phone 8. Prostředí aplikace pro různé OS je obdobné, liší se pouze v některých ovládacích prvcích specifické pro danou platformu a rozdíly lze nalézt také u některých funkcionalit.

Česká spořitelna nabízí více než jednu aplikaci pro mobilní bankovnictví. Kromě aplikace, která nabízí pouze pasivní pohled na zůstatky, je novinkou aplikace Friends 24, která umožňuje realizovat platby do 10 000 Kč bez znalosti čísla účtu adresáta, postačí libovolný kontakt – telefon, e-mail nebo Facebook Messenger. Tyto aplikace nad rámec standardního mobilního bankovnictví fungují na stejném principu – jen mají omezenou možnost využití nebo lákají na moderní řešení.

(Česká spořitelna 2, 2016, citováno online 20.1.2017)

Následující tabulka zobrazuje dostupnost aplikace pro mobilní bankovnictví pro různé platformy a datum jejich uvedení do elektronických distribučních kanálů.

Tabulka 1- Aplikace pro mobilní bankovnictví v ČR

Název		Termín dostupnosti aplikace		
Banka	Aplikace	iOS	Android	Windows Phone (10 Mobile)
Air Bank	Mobilní bankovnictví	4/2013	7/2013	3/2015
Česká spořitelna	Servis 24 - Mobilní banka	2/2012	7/2012	12/2014
ČSOB	ČSOB SmartBanking	1/2012	1/2012	3/2013
Equa Bank	Equa bank	10/2011	10/2011	X
Era / Poštovní spořitelna	Era Smartbanking	1/2012	1/2012	3/2013
Fio Banka	Fio banka Smartbanking	5/2011	8/2011	10/2013
ING Bank	ING Bank CZ	12/2012	12/2013	X
Komerční Banka	Mobilní Banka	11/2012	11/2012	11/2013
mBank	mBank CZ	10/2011	3/2012	X
Moneta (GE Money Bank)	Smart Banka - mobilní bankovnictví	12/2011	12/2011	X
Raiffeisenbank	Raiffeisenbank CZ - Mobilní eKonto	11/2012	11/2012	X
Sperbank	Smart Banking	11/2013	11/2013	X
UniCredit Bank	Smart Banking	10/2011	10/2011	4/2012
Waldviertel Sparkasse Bank	WSPK Smartbanking	3/2015	3/2015	3/2015
ZUNO Bank	ZUNO CZ Mobile Banking	11/2012	11/2012	12/2014

Zdroj: (Bubák, 2015, citováno online 29.12.2016), vlastní zpracování

2.2.2 **Aktivace mobilního bankovnictví**

Pro uživatele elektronického bankovnictví existuje zpravidla jediná hlavní možnost, jakým způsobem aktivovat aplikaci pro správu osobního účtu v jejich mobilním zařízení. V prostředí pro elektronické bankovnictví v internetovém prohlížeči lze aplikaci pro mobilní bankovnictví aktivovat. Proces se u rozdílných poskytovatelů liší. U některých mohou být k aktivaci nutné údaje zaslané uživateli klasickou poštou. K aktivaci je nutná spolupráce mezi mobilním zařízení a internetovým prohlížečem. Aktivační kód je nutné zadat či naskenovat pomocí QR kódu. Aktivace je platná vždy pouze pro jedno zařízení a je vázána na sériové číslo zařízení. (Nicoletti, 2014)

V některých případech je nutné aplikaci znovu aktivovat i v případě aktualizace operačního systému zařízení (eKonto – Raiffeisenbank). Přístupové heslo do mobilní aplikace je nutné navolit v prostřední internetového prohlížeče (Servis 24 – Česká spořitelna), nebo přímo v aplikaci (eKonto – Raiffeisenbank). V případě ztráty nebo odcizení zařízení je možné deaktivovat propojení účtu s aplikací v internetovém bankovnictví nebo zavoláním na zákaznickou linku.

2.2.3 **Funkcionality bankovní aplikace**

Kromě správy účtu nabízí bankovní aplikace mnoho dalších funkcí, z nichž některé nejsou na bankovní účet klienta vázány. Z toho důvodu, k některým z nich, není nutné mít aplikaci aktivovanou. Jedná se například o kurzovní lístek nebo informace o nových produktech. Funkcionality aplikací lze rozdělit mezi veřejnou část, ke které má uživatel přístup po stažení aplikace, a uzavřenou ke správě účtu.

1) Veřejná část – uživatel nemusí mít zřízen účet

    - *„seznam nebo mapa poboček, navigace k nejbližší pobočce*
    - *seznam nebo mapa bankomatů, navigace k nejbližšímu bankomatu*
    - *kontaktní údaje banky a poboček – emaily, telefony*
    - *kurzovní lístek cizích měn*
    - *slevy v rámci věrnostního programu, který banka podporuje*
    - *možnost zažádat o produkty banky (účet, cestovní pojištění, ...)*
    - *veřejné zprávy od banky“*

2) Uzavřená část – uživatel musí mít zřízen účet a aktivováno mobilní bankovnictví

    - *„aktuální dostupný zůstatek na běžném účtu*
    - *historie účtu s možností zobrazení detailních informací ke každé položce (platbě, výběru apod.)*
    - *stavy a historie ostatních produktů (kontokorent, úvěr, spoření, ...)*
    - *informace o platebních kartách, někdy i s možností deaktivace, změny PIN apod.*

- *provedení platby (příkazu k úhradě)*
- *skenování platby či načtení platby ze složenky nebo z faktury pomocí QR kódu (nabízejí jen některé banky)*
- *nastavení šablon plateb, které můžete při platbách využít*
- *žádosti o produkty, ke kterým potřebujete mít založený běžný účet, sledování a nastavení jejich parametrů apod. (kontokorent, úvěr, spořicí účet, investice do podílových fondů)*
- *nastavení mobilního bankovnictví jako takového"*

(Bubák, 2015, citováno online 20.01.2017)

Další užitečnou funkcionalitou aplikací je možnost vyzkoušení uzavřené části před aktivací mobilního bankovnictví. Určitou formu demo verze nabízí většina českých bank, ne všechny pak umožňují plné vyzkoušení všech funkcí v aplikaci. Pokud uživatel ještě před výběrem banky předpokládá, že bude aktivně využívat mobilní aplikaci, je tento nástroj schopen pomoci s rozhodováním mezi bankovními produkty.

2.3 NFC (Near Field Chip)

V souvislosti s mobilním bankovnictvím je nutné zmínit NFC, v překladu čip pro komunikaci v blízké oblasti. V posledních deseti letech došlo k rozmachu a uplatnění v mnoha oborech lidské činnost, především v souvislosti s rozvojem mobilních zařízení.

NFC je vysokofrekvenční technologie s malou šířkou pásma, která slouží ke komunikaci dvou zařízení s touto technologií na krátkou vzdálenost. Funguje na frekvenci 13,56 MHz, která se dříve používala pro identifikaci na radiové frekvenci (RFID) navazující na systém čárových kódů pro identifikace zboží. NFC tuto technologii dále vylepšuje.

NFC technologie umožňuje komunikace formou přenosu dat na vzdálenost maximálně 4 cm mezi dvěma zařízeními aktivními (2 mobilní telefony vybaveny NFC) nebo zařízením aktivním a pasivním (Platební karta a terminál). NFC nalézá uplatnění v mnoha případech. Může sloužit pro osobní identifikaci, pro odemčení zámků hotelových pokojů, automobilů nebo pro bezkontaktní platby.

(Coskun, 2011)

Mobilní platba uskutečněná pomocí NFC umožňuje v jednom zařízení kombinaci několika platebních karet, věrnostních karet a dalších funkcí. Mobilní telefon vybaven NFC může být náhradou za všechny tyto nástroje.
Také pomáhá společnostem využít mobilní zařízení jako marketingový nástroj, skrz nějž je schopna komunikovat se zákazníky například promo akce nebo novinky. (Nicoletti, 2014)
Platby pomocí NFC v mobilním zařízení umožnují v České republice pouze ČSOB a Komerční banka. První zmíněná používá samostatnou aplikaci pro Android OS. Komerční banka tuto možnost implementovala přímo do verze aplikace Mobilní banka pro stejný operační systém. Obě aplikace vyžadují zařízení s NFC a verzí Android OS 4.4 a vyšší, v případě Komerční banky je nutné zřídit speciální službu.

Komplexní řešení bezkontaktního placení bez nutnosti platební karty včetně autorizace platby pomocí otisku prstu nebo synchronizace mezi telefonem a chytrými hodinkami nabízí Apple, Google a Samsung. Vzhledem k velikosti trhu v České republice nejsou služby v tuzemsku prozatím dostupné. České banky proto vyvíjejí vlastní řešení. Otázkou zůstává, jak budou postupovat v případě zájmu globálních služeb o vstup na český trh. Investice bank do vývoje vlastního řešení a rozšířenost bezkontaktních platebních karet mohou způsobit, že velcí výrobci nebudou mít zájem zavádět vlastní technologie. (Láska, 2016, citováno online 20.1.2017)

2.4 QR kód

Quick Response kód je druh čtvercového čárového kódu původně vyvinutý v Japonsku v roce 1994 pro automobilový průmysl ke zjednodušení sledování procesu výroby. QR kód používá čtyři standardizované kódovací módy (numerický, alfanumerický, binární a japonské písmo Kanji) k efektivnímu uložení dat. (QR code 1, citováno online 20.1.2017)
QR kód se stal populární mimo oblast automobilového průmyslu hlavně díky větší kapacitě uložených dat a menším nárokům na čtecí zařízení. QR kód se skládá z černých čtverců uspořádaných na mřížce s bílým pozadí. Získaná data jsou extrahována z horizontální i vertikální struktury obrazce.
(Denso ADC, 2011, citováno online 21.1.2017)

Vytvoření QR je dostupné díky mnoha placeným i bezplatným aplikacím a internetových stránek. Uživateli je umožněno vytvoření a další sdílení kódů, které jsou v současné době jedním z nejpoužívanějším typem a ve srovnání se standardními čárovými kódy typu UPC nebo EAN mohou obsahovat mnohem více informací. (QR code 2, citováno online 21.1.2017)

2.4.1 **Použití**

Typickým čtecím zařízením QR kódu jsou v dnešní době fotoaparáty chytrých mobilních telefonů, které naskenovaný kód konvertují do užitečné formy například odkazu na internetové stránky značky, která použije kód jako marketingový nástroj z důvodu rychlejšího dosažení stránky než manuální zadání do prohlížeče.
(Lee, 2012, citováno online 21.1.2017)
Většina způsobů použití QR kódů v běžném životě cílí na uživatele mobilních zařízení. Naskenovat lze například vizitku ve formátu vCard, již zmiňovaný odkaz na internetové stránky, vytvoření e-mailu nebo textové zprávy. Aplikace pro skenování i generování QR kódů lze nalézt na většině mobilních operačních systémech jako vestavěné řešení, nebo ke stažení v distribučních kanálech pro aplikace.
(Edwards, 2010, citováno online 22.1.2017)

2.4.2 **QR platby**

Quick response kód může být užiteční pro elektronický platební styk díky tomu, že může obsahovat informace o bankovním účtu, platební kartě a také mohou obsahovat formát pro sdílení platebních údajů v aplikacích pro mobilní bankovnictví.
(Van Grove, 2011, citováno online 22.1.2017)
Česká republika byla první, kde v roce 2012 došlo k masovějšímu použití plateb pomocí skenování QR kódů. Formát pro sdílení platebních údajů elektronickou cestou byl vyvinutý v rámci tvorby aplikace pro mobilní bankovnictví a je použitelný v rámci EU a několika dalších zemí díky standardu ISO 13616, který upravuje použití mezinárodního čísla bankovního účtu (IBAN) umožňující mezinárodní platby. (ISO 13616, 2007, citováno online 3.2.2017)
Na vývoji a rozšíření formátu pro sdílení platebních údajů se nejvíce podílely Raiffeisenbank a.s., technologická společnost Inmite s.r.o. a ČSOB a.s.. Obecně

uznávaným se tento formát stal standardizací Českou bankovní asociací na konci roku 2012. (Šmídová, 2015, citováno online 3.2.2017)

„Praktické využití formátu spočívá především v přenosu platebních údajů bez zásahu lidského faktoru. Tím se jednak zvýší komfort pro klienty, ale také sníží počet špatně zadaných plateb a nákladů na jejich dohledávání, případně vymáhání. Typickým příkladem použití je uvedení QR kódu s platebními údaji na faktuře pro iniciaci platby. Klient v takovém případě spustí na chytrém telefonu/tabletu bankovní aplikaci a QR kód načte. Tím se mu předvyplní příslušná pole platebního příkazu v mobilní aplikaci. Klient údaje zkontroluje, platební příkaz autorizuje a odešle. Vše se obejde bez ručního zadávání čísla účtu, variabilního symbolu atd. Tím nejen roste uživatelská spokojenost, ale také klesá chybovost zadání a nutnost řešit reklamace.“
Formát lze použít pro jednorázový i trvalý příkaz k úhradě a svolení k inkasu. Poslední dva zmíněné byly spolu s možností přidání pole „zpráva pro mne“ doplněny ke standardu v květnu roku 2015.
(Česká bankovní asociace, 2015, citováno online 3.2.2017)

QR platba není produkt jedné banky a v aplikacích pro mobilní bankovnictví tento standard využívá celkem deset bank působících v České republice. Generování platebních údajů implementovala do svých produktů většina výrobců ekonomického software. K rozšíření QR plateb pomohli například poskytovatelé telekomunikačních služeb, kteří tuto platební metodu zahrnují do vystavených faktur. Bezplatně lze vygenerovat platební QR kód například na internetových stránkách qr-platba.cz
(Hovorka, 2014, citováno online 6.2.2017)

V případě doplnění specifického symbolu by takto vygenerované platební údaje mohly sloužit k úhradě poplatku za přihlášku ke studiu.

Obrázek 2 - Formulář a Platební QR kód

Zdroj: (QR Platba, 2017), vlastní zpracování

QR jsou často využívány v oblasti kryptografických měn včetně Bitcoin. Šifrované klíče a informace pro provedení transakce jsou sdíleny mezi digitálními peněženkami právě za pomoci Quick response kódů.

(Blockchain, citováno online 6.2.2017)

2.5 Mobilní platforma Apple

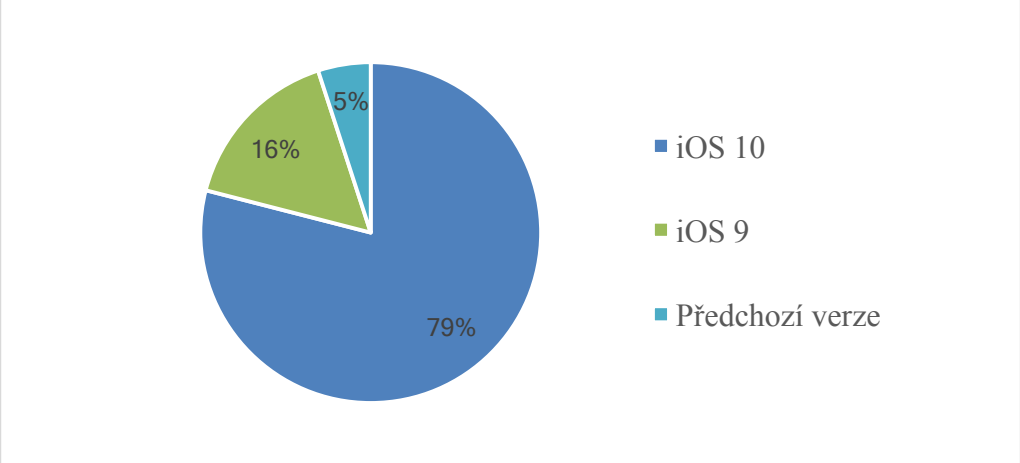
Mobilní platforma Apple byla poprvé představena v roce 2007 spolu s první generací mobilního telefonu stejného výrobce pod názvem iPhone OS. Jedná se o mobilní operační systém, jehož prostředí využívá k přímé komunikaci s uživatelem dotyková gesta a hardwarová tlačítka. V současné době se jedná o druhý nejpoužívanější mobilní operační systém vedle Android OS. Mobilní platformu Apple dnes kromě chytrých telefonů využívají tablety, chytré hodinky, hudební přehrávače a digitální mediální centrum Apple TV. Jedná se o uzavřený systém, který je distribuován pro hardware společnosti Apple.

(Lashinsky, 2012)

2.5.1 **iOS**

iOS je označení pro mobilní operační systém určený pro mobilní telefony iPhone a tablety iPad. Při představení byl prezentován jako iPhone OS, mobilní verze operačního systému pro osobní počítače Mac OS X.
(Apple 4, 2007, citováno online 6.2.2017)
Součástí druhé verze iPhone OS byl App Store, elektronický distribuční kanál pro aplikace třetích stran, a také SDK, který vývojářům poskytl soubor nástrojů pro vývoj vlastního software.
Se čtvrtou verzí uvolněnou v roce 2010 došlo k přejmenování na iOS. Hlavní aktualizace se systému dostane každý rok společně s představením nové generace mobilních telefonů.
(Chartier, 2010, citováno online 6.2.2017)
Současná verze iOS 10 byla představena v roce 2016 a je kompatibilní se všemi mobilními telefony iPhone představenými od roku 2012 a tablety od roku 2013. Celosvětově je nainstalovaná verze iOS 10 na téměř 80 % aktivních zařízení.
(Apple, 2017, citováno online 25.2.2017)

Graf 1 - Nainstalovaná verze operačního systému



Zdroj: (Apple 1, 2017), vlastní zpracování

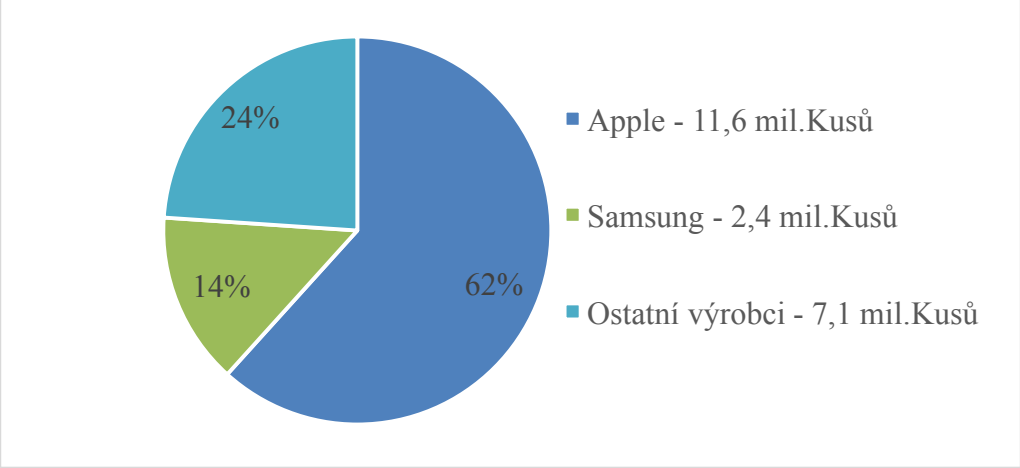
Tuto skutečnost je nutné zmínit vzhledem k tomu, že aplikace pro mobilní bankovnictví českých bank vyžadují verzi iOS 7, některé dokonce iOS 8 či iOS 9. Je proto možné, že na některých starších aktivních zařízení, není možné služeb mobilního bankovnictví využívat. Nekompatibilita je způsobena nutností

optimalizovat aplikace pro nové verze operačního systému a také skutečností, že pro verzi iOS 7 vyšla poslední bezpečnostní aktualizace v březnu roku 2014.
(Clover, 2014, citováno online 18.2.2017)

2.5.2 **WatchOS**

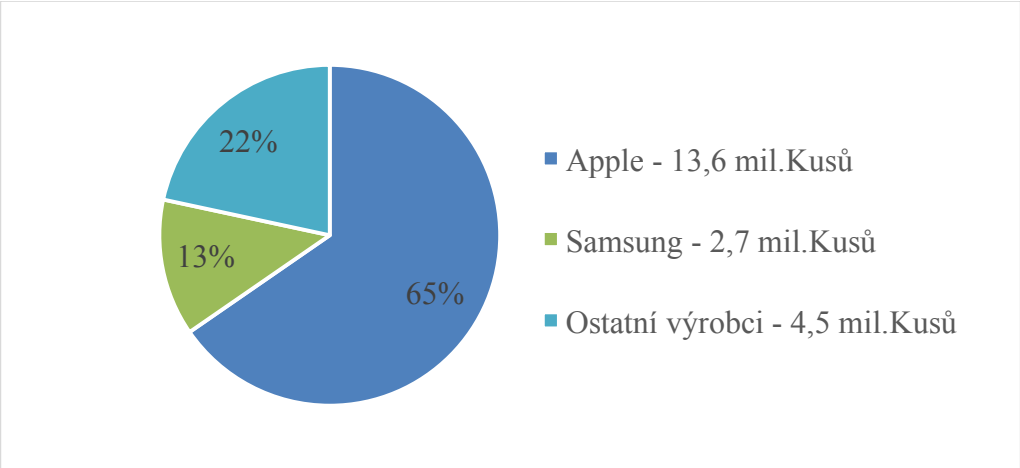
WatchOS je operační systém chytrých hodinek Apple Watch poprvé představený s jejich první generací v dubnu roku 2015. Operační systém vychází z iOS pro telefony a tablety, z jejichž prostředí lze také do Apple Watch instalovat aplikace a provádět další nastavení. Nyní je pro chytré hodinky dostupná třetí verze operačního systému, která upravuje vzhled a přináší některé nové funkce. Vzhledem ke stáří operačního systému a celkovému rozšíření nositelné elektroniky se aplikace pro mobilní bankovnictví dostávají do této platformy velmi pomalu a v následujících letech je očekáván vývoj a výrazné vylepšení použitelnosti bankovních aplikací pro nositelnou elektroniku v čele s chytrými hodinkami.
(Rossignol, 2017, citováno online 18.2.2017)
Následující grafy zobrazují tržní podíl a celkové prodeje chytrých hodinek Apple Watch a konkurence v letech 2015 a 2016

Graf 2 - Celkové prodeje a podíl na trhu (2015)



Zdroj: (Strategy Analytics, 2017), vlastní zpracování

Graf 3 - Celkové prodeje a podíl na trhu (2016)



Zdroj: (Strategy Analytics, 2017), vlastní zpracování

Jako první na českém trhu představila verzi aplikace pro chytré hodinky Komerční banka. Nabízí však pouze pasivní sledování zůstatku a pohybů na účtu a není k dispozici pro konkurenční operační systém pro nositelnou elektroniku Android Wear. (Systém Online, 2016, citováno online 18.2.2017)

Druhou bankou působící v České republice, která nabízí verzi aplikace pro chytré hodinky je skupina ČSOB, do která patří Era a Československá obchodní banka. Obě banky pro své klienty nabízí aplikace ve verzi WatchOS i Android Wear. Nabízí obdobné funkce jako aplikace Komerční banky.
(Bubák, 2017, citováno online 20.2.2017)

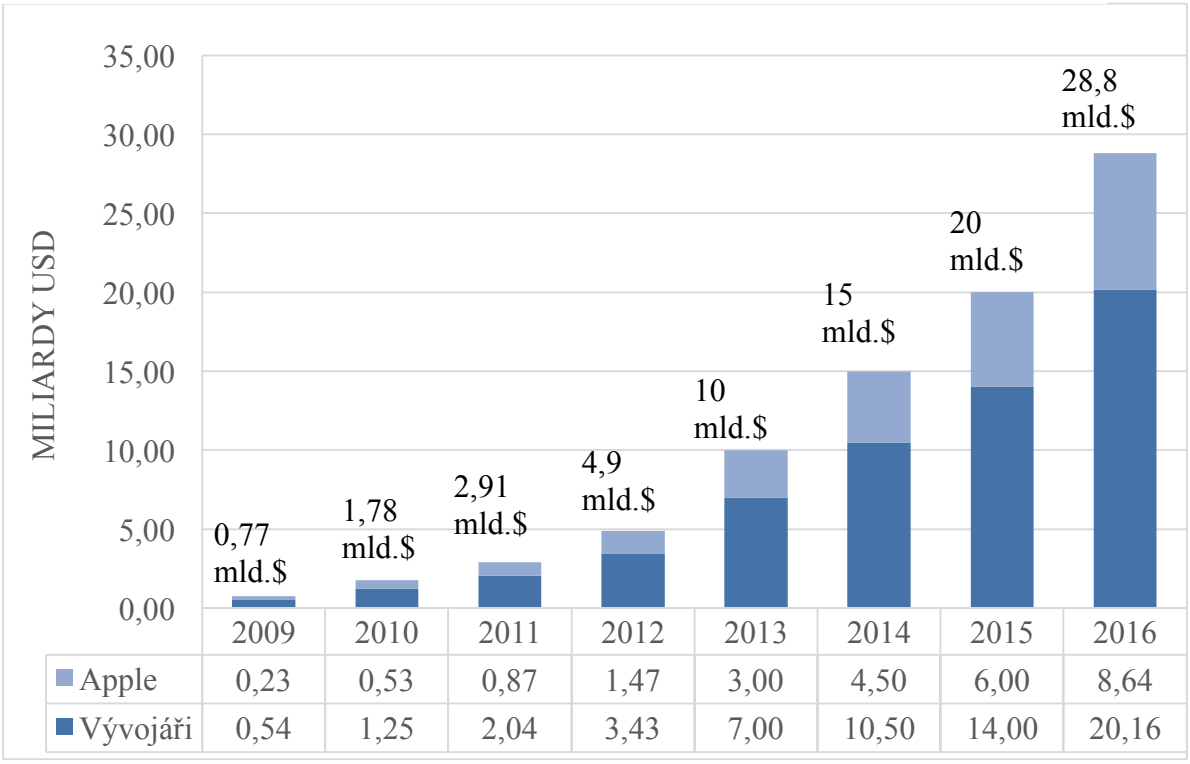
2.5.3 **App Store**

Po více než roce od vydání prvního zařízení s mobilním operačním systémem Apple byla spuštěna digitální distribuční platforma pro stahování aplikací třetích stran.
V App store se nachází aplikace pro chytré telefony, hodinky a televizi, tablety a na stejném principu funguje také Mac App Store, s aplikacemi pouze pro osobní počítače Apple, spuštěný v roce 2010. Koncept App Store vychází ze staršího iTunes Music Store online obchodu s hudbou a dalším audiovizuálním materiálem.
V roce 2016 nastala změna v rozdělení příjmů z prodeje aplikací mezi Apple a vývojáři. Stávající model rozdělení příjmů v poměru 70:30 procent ve prospěch

vývojářů byl změněn na poměr 85:15 po prvním roce, kdy uživatelé aplikaci aktivně používají. (Goode, 2016, citováno online 21.2.2017)

Následující graf zachycuje vývoj příjmů z prodeje aplikací v čase mezi roky 2009 a 2016.

Graf 4 - Příjmy z prodejů App Store (2009-2016)



	2009	2010	2011	2012	2013	2014	2015	2016
Apple	0,23	0,53	0,87	1,47	3,00	4,50	6,00	8,64
Vývojáři	0,54	1,25	2,04	3,43	7,00	10,50	14,00	20,16

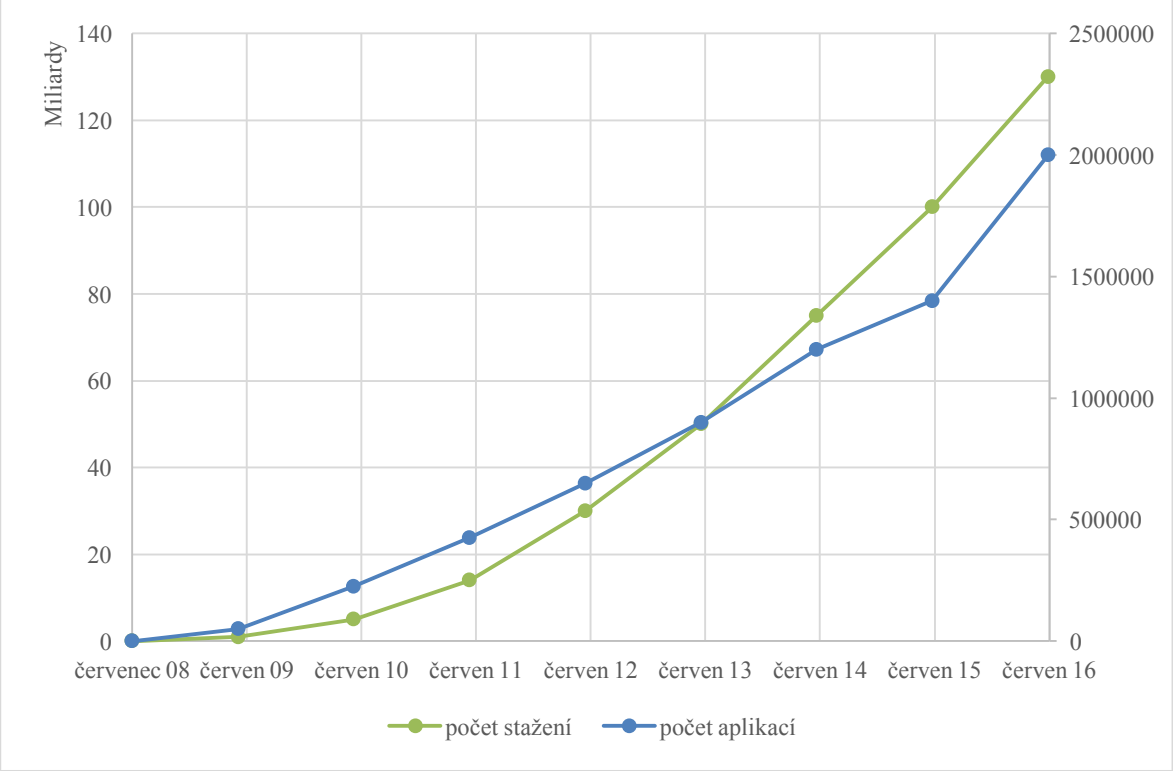
Zdroj: (Statista 1, 2016, citováno online 21.2.2017), (Whitney, 2011, citováno online 18.2.2017), (Keizer, 2013, citováno online 18.2.2017), vlastní zpracování

V době uvedení App Store na trh, v červenci 2008, bylo obsaženo 500 aplikací různého zaměření. V lednu roku 2017 bylo k dispozici 2,2 milionu různých aplikací.

V září roku 2016 bylo rozhodnuto o stažení nestabilních aplikací nepodporující některá zařízení. Jen v říjnu 2016 bylo tímto způsobem odstraněno téměř 50 tisíc aplikací. (Perez, 2016, citováno online 29.12.2016)

Následující graf zobrazuje vývoj počtu dostupných aplikací (vedlejší osa) a přibližný počet stažení (hlavní osa) v čase mezi uvedením platformy App Store a koncem roku 2016.

Graf 5 - Počet aplikací dostupných v App Store a přibližný počet stažení



Zdroj: (Statista 3, 2017, citováno 19.2.2017), vlastní zpracování

Do dnešního dne vzniklo mnoho dalších služeb pro získání aplikací do mobilních zařízeních, z nichž některé z nich se přejmenovaly, zanikly, nebo byly sloučeny s novější službou. Až v roce 2011 se do distribučních platforem Apple App Store, Google Play a Windows Store začaly dostávat aplikace pro mobilní bankovnictví bank působících v České republice. V následující tabulce se nachází přehled současných distribučních platforem pro mobilní aplikace včetně data uvedení na trh a přibližného počtu dostupných aplikací k určitému datu.

Graf 6 - Přehled elektronických distribučních platforem

Název	Datum spuštění	Počet aplikací	K datu
Amazon AppStore	3/2011	600 tis.	4/2016
Windows (Phone) Store	10/2010	669 tis.	7/2016
Google Play (Android market)	10/2008	2200 tis.	7/2016
Apple App Store	7/2008	2200 tis.	1/2017
BlackBerry World	4/2009	234,5 tis.	4/3014
Ubuntu (Touch) App Store	10/2013	2,798 tis.	1/2017
Firefox market place	9/2013	6,1 tis.	1/2017

Zdroj: (Statista 2, 2016, citováno online 19.2.2017), (UApp Explorer, 2017, citováno online 19.2.2017), (Firefox MarketPlace, 2017, citováno online 19.2.2017), vlastní zpracování

2.5.4 **Touch ID**

Touch ID je systém rozpoznávající otisky prstů umožňující rychlý a bezpečný způsob přístupu do zařízení. Funguje na principu přikládání prstu na senzor v různých úhlech. Je to systém podřazený zámku obrazovky. Díky tomu může uživatel nastavit složitější kód pro zámek obrazovky, a přesto mu senzor Touch ID umožní rychlý přístup do zařízení. Samotný senzor se aktivuje díky kroužku z oceli okolo něj, který rozpozná přiložení. Uživatel má možnost naskenovat celkem pět otisků a šance, že by otisk prstu někoho jiného byl rozpoznán jako naskenovaný otisk uživatele je 1:50000. Od verze iOS 9 jsou schopni vývojáři aplikací schopni využít Touch ID k přístupu do aplikací. Naskenované otisky zůstávají uloženy v zašifrované paměti v rámci Secure Enclave a nejsou kamkoliv odesílány a uchovávány. (Apple 3, 2016, citováno online 21.2.2017)

V případě poškození senzoru lze pro opětovnou funkčnost systému vyměnit pouze společně se základní deskou v autorizovaném servisu. Při výměně pouze senzorového obvodu zůstává funkční jen jako domovské tlačítko. V minulosti při nové verzi systému iOS 8.3 došlo u zařízení iPhone 6 a iPhone 6 Plus s takto vyměněným senzorem Touch ID při pokusu o aktualizace k zablokování celého

zařízení. Po nátlaku uživatelů bylo toto bezpečností opatření v další aktualizaci odstraněno.
(Brignall, 2016, citováno online 22.2.2017)

2.5.5 **Apple Pay**

Služba společnosti Apple Inc. představená v září roku 2014. Jedná se o alternativu k bezkontaktní platební kartě využívající primárně NFC, ale může být využívána pouze jako elektronická platební karta v kompatibilních aplikacích. NFC je součástí řady mobilních telefonů Apple iPhone 6/6 Plus a novějších, dále tento čip nalezneme v chytrých hodinkách Apple Watch. Přidání platební karty do telefonu probíhá dvěma způsoby. Prvním je přidání platební karty, kterou již uživatel používá při nákupech v App Store, kde stačí pouze zadat bezpečnostní kód platební karty, druhou je její naskenování do aplikace Wallet a potvrzení bankou. Při každé platbě je nutné potvrdit transakci použitím čtečky Touch ID. Veškeré údaje o kartě jsou uchovány pouze v hardwarové komponentně tzv. secure element čipu na základní desce zařízení a v aplikace Wallet není u platební karty uvedeno jméno držitele a pouze část čísla karty.
(Holzman, 2014, citováno 29.12.2016)
Apple Pay je v současné době dostupné ve 13 zemích světa, v nejbližší době by mělo následovat Německo a Polsko. Pokud má však uživatel účet vedený v některé z 13 zemí, je možné využívat Apple Pay u jakéhokoliv bezkontaktního terminálu. Konkurenčními službami jsou Samsung Pay, Android Pay a Microsoft Wallet.
(Apple 2, 2017, citováno online 8.3.2017)

2.5.6 **Možnosti zabezpečení**

Mobilní platforma Apple je obecně považována za bezpečnější než konkurence. Jedním z hlavních důvodů je fakt, že instalace aplikací z neověřených zdrojů je uživatelsky náročnější než v případě Android OS. Na oficiálních kanálech ke stažení aplikací v případě Google Play pro Android i App Store pro iOS dochází ke schvalovacímu procesu ze strany výrobce. (Dormehl, 2016, citováno 10.12.2016)
Na uzavřené platformě iOS je možná instalace neoficiálních aplikací, na rozdíl od Open Source povaze Android OS, možná jen za pomoci tzv. „Jailbreak“.

Všeobecné povědomí o zabezpečení zařízeních pracujících na platformě Apple pramení dle názoru autora z doby, kdy se na počítačích Mac téměř neobjevoval škodlivý software, a to zejména z důvodu nízkého podílu na trhu oproti počítačům s operačním systémem Windows od Microsoft. Za desetiletou historii mobilního operačního systému iOS se objevilo několik stovek více či méně závažných bezpečnostních chyb, které byly ve většině případů eliminovány bezpečnostní aktualizací instalovanou uživatelem. Přesto však tento systém komplikuje šíření klasických hrozeb, ale také instalaci bezpečnostního software třetích stran, jako například antivirové programy.

Zabezpečení iOS zařízení můžeme rozdělit na 4 části:

1) Zabezpečení zařízení

   Tímto pojmem se rozumí bezpečností opatření, které znemožní přístup do systému. První možností je kódový zámek. Uživateli umožňuje nastavit délku, složitost a čas, za který je po nečinnosti zařízení požadován. Lze tak omezit některé funkce před odemčením a nastavit smazání dat po několika špatných pokusech. Konkurence s Android OS nabízí navíc možnost nastavení gesta k odemčení zařízení. Dalším bezpečnostním prvkem je Touch ID skener otisků prstů, který slouží k odemčení zařízení, ale i k přístupu do aplikací třetích stran a urychluje samotnou autorizaci oproti kódovému zámku. Do zařízení lze naskenovat několik otisků, které jsou uloženy pouze v paměti na základní desce zařízení. Tento prvek je podřazený kódovému zámku, z toho důvodu lze zadáním správného kódu Touch ID obejít.

2) Zabezpečení Dat

   iOS má jako základní prvek datové bezpečnosti uložiště šifrované pomocí 256bitového AES algoritmu. Smazaní dat na dálku pomocí iCloud aplikace funguje právě na principu smazání klíče, který je potřeba k přístupu k datům. Šifrovat lze tímto způsobem i zálohu dat z mobilního zařízení. Vývojáři mají také možnost šifrovat soubory aplikací.

3) Zabezpečení Aplikací

   App Store i konkurenční řešení nabízí stovky tisíc aplikací všech kategorií. V iOS jsou aplikace navzájem izolované, pouze uživatel může aplikaci poskytnout přístup k další. To se děje například při synchronizaci kancelářských aplikací na cloudové

uložiště nebo při umožnění aplikace sociální sítě k fotografiím. Bankovní aplikace může mít přístup do adresáře, nebo k fotoaparátu k naskenování QR kódu, nikdy by však uživatel neměl dovolit přístup jiného software k aplikaci mobilního bankovnictví. V případě, kdy by došlo ke škodlivému chování software, je u schválených aplikací možnost dohledání vývojáře aplikace snadná za pomoci certifikátu.

4) Zabezpečení síťové komunikace

„*Síťová komunikace je pro každé chytré mobilní zařízení zásadní. Velice často se tato zařízení připojují k firemním sítím, a proto je důležité, aby jejich komunikace byla dostatečně zabezpečená. iOS nabízí hned několik možných zabezpečených komunikací pro realizaci VPN spojení, ať už je to IPsec, L2TP, PPTP nebo SSL-VPN. K dispozici je i ověřování pomocí x.509 certifikátů nebo hardwarových či softwarových tokenů různých výrobců. V případě komunikace s Microsoft Exchange pro přístup k e-mailu a kalendáři je možné konfigurovat použití 128bitového šifrovaného SSL spojení*“
(Meduna, 2013)

Komunikace mezi zařízeními Apple může probíhat přes iMessage. Aplikace pro sdílení textových a hlasových zpráv s možností sdílení fotografií a videí je součástí systému iOS pro mobilní zařízení i MacOS pro osobní počítače. Také u iMessage je komunikace šifrována pomocí asymetrické kryptografii s veřejným a soukromým klíčem. Zprávy zaslané pomocí této aplikace jsou uloženy v zařízení uživatele, ale i na serverech iCloud. V začátku roku 2016 byla vydána bezpečnostní aktualizace, která eliminovala možnou hrozbu útoku na komunikaci přes iMessage z důvodu časového intervalu obnovení dešifrovacích klíčů. (Storm, 2016, citováno 29.12.2016)

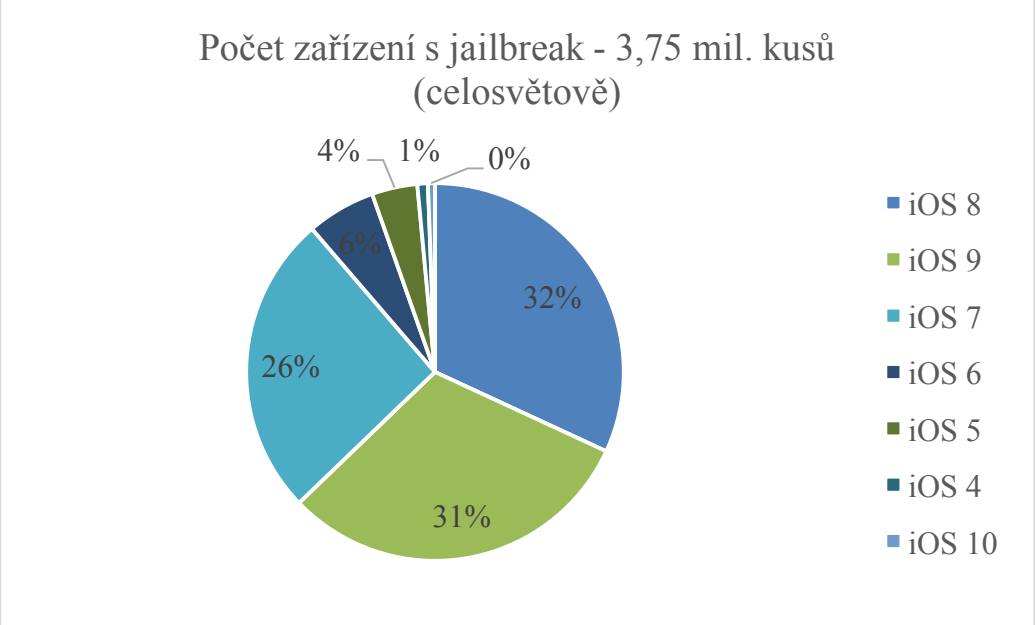
2.5.7 **Jailbreaking**

Jailbreaking softwarová úprava, která mění operační systém na iOS zařízení, odstraňuje omezení a umožňuje uživatelům instalovat aplikace a další obsah z jiných zdrojů, než jen z oficiálního App Store. Jailbreak je často zaměňován s procesem odblokování zařízení pro poskytovatele telefonních služeb mimo zemi původu.
Tato úprava s sebou nese možnost výskytu některých rizik. Tím hlavním může být nevratné zničení software zařízení, které může v určitých případech nastat, s tím souvisejí ztráta záruční lhůty na zařízení, nemožnost upgrade systému a problém

s oficiální podporou. Dalším nevýhodou jailbreak je bezpečnost. S instalací aplikací a dalšího obsahu z neověřených zdrojů uživatel významně zvyšuje možnost napadení dat svých i dat uložených v aplikacích. V neposlední řadě se uživatel může setkat s nestabilním chodem systému a celkovým zpomalením.

Výhodami instalace jailbreak je vyšší míra přizpůsobení prostředí systému, instalace neoficiálních programů, nebo získání placeného software bez poplatku. Celá tato software úprava je vratná přehráním systému do továrního nastavení v případě, že nedojde ke komplikaci. (Costello, 2017, citováno online 13.2.2017)

Graf 7 - Zařízení s Jailbreak



Zdroj: (Quora, 2017, citováno online 16.2.2017), vlastní zpracování

2.6 Bezpečnostní hrozby

V této kapitole budou charakterizovány typy bezpečnostních hrozeb, které umožňují útočníkovi získat přístup k citlivým údajům, například přístupová data k internetovému bankovnictví.

2.6.1 Phishing

Jedná se o jednu z nejčastějších forem útoku na internetové bankovnictví za účelem získání citlivých uživatelských dat. Phishing využívá e-mailové schránky, s jejichž pomocí se snaží od klientů bank získat přihlašovací údaje, k napadení bankovního

účtu. Podstatou této metody je zaslání e-mailu, který na první pohled vypadá, jako oficiální forma komunikace banky. Vzhled, způsob vyjadřování, v některých případech i doména e-mailové adresy souhlasící s bankovní institucí může klienty oklamat. Ve většině případů zpráva obsahuje odkaz na falešné stránky internetového bankovnictví.
(Rouse, 2015, citováno online 29.12.2016)
Účinnou metodou obrany je na tyto podvodné zprávy nereagovat. Banky na tuto hrozbu často upozorňují a informují uživatele, že nikdy nepožadují citlivá data klientů na základě e-mailů a zpráv.
(Česká spořitelna 3, citováno online 29.12.2016)
Hrozbou, která reaguje na přechod uživatelů z klasického internetového bankovnictví na mobilní bankovnictví je tzv. „spear phishing“. Funguje na podobném principu jako phishing, ale namísto falešného hypertextového odkazu obsahuje přílohu s aktualizací dané aplikace například ve formě souboru „.apk“ pro Android OS, ze které se citlivé údaje dostanou k útočníkovi. V případě systému iOS je možné útok realizovat pouze na zařízeních s „Jailbreak“.
(Zetter, 2015, citováno online 29.12.2016)

2.6.2 **Vishing**

Pojmenování této metody vzniklo spojením slov voice a phishing. Jak už název napovídá, jedná se o obdobnou techniku útoku, kde formou není e-mail, ale telefonická komunikace. Útočník předstírá operátora dané bankovní instituce a snaží se od oběti získat citlivé informace. Ve většině případu se nesnaží získat všechna data najednou, ale ve více fázích s odstupem času s pomocí více telefonních hovorů, aby oběť nepojala podezření z zneužití informací. Pravděpodobnost rizika napadení aplikací pro mobilní bankovnictví přes Vishing je nízká, vzhledem k faktu že útočník by po získání údajů potřeboval fyzicky získat také mobilní zařízení oběti. Jedinou možností by bylo přes internetové bankovnictví aktivovat mobilní aplikaci v jiném zařízení.
(Keyworth, 2016, citováno 29.12.2016)

2.6.3 **SMiShing**

V případě této hrozby zasílá potenciální oběti SMS zprávu, která může obsahovat výzvu k zaslání přihlašovacích údajů (Kalabis, 2012)
Zpráva může podobně jako e-mail obsahovat odkaz ke stažení aplikace, nebo její aktualizace.

2.6.4 **Pharming**

Pharming oproti předchozím patří mezi propracovanější bezpečnostní hrozby. Napadá DNS, kde přepisuje IP adresu a uživatel je tak z původních stránek své banky přesměrován na jejich věrnou napodobeninu vytvořenou útočníkem, ze kterých získá po uživatelově přihlášení potřebná data pro identifikaci. Tento způsob přináší hrozbu v případě internetové bankovnictví, při používání aplikace pro mobilní bankovnictví nezpůsobuje vznik rizika. (Matyáš, 2008)

2.6.5 **Distributed DOS**

Tento typ hrozby není směřován cíleně na uživatele, ale na vzájemnou komunikace mezi klientem a bankou či přímo bankovní servery. Samotný útok má za cíl přehltit server požadavky a tím způsobit zpomalení běžného chodu, nebo dokonce pád celého systému. Útok je zpravidla veden v jeden časový okamžik, aby byl účinek co možná nejefektivnější. Distrubuted Denial Of Service je sofistikovanější typ útoku typu DOS, kdy na rozdíl od něj dochází k vyslání falešných požadavků s cílem přetížit hardware přes ovládnutí více míst současně.
(Imperva 1, citováno online 28.12.2016)
Typ útoku Distributed DOS je schopný ohrozit i chod aplikací pro mobilní bankovnictví v případě, že přímo napadne servery, na kterých běží komunikace mezi aplikací a bankou. Ve většině případu nedojde ke ztrátě finančních prostředků klientů bank, ale útok je schopen vyřadit služby elektronického bankovnictví i na několik dní.
(Collinson, 2017, citováno online 24.1.2017)

2.6.6 **Man in the Middle**

Jedná se o útok na uživatele, který napadá hashovací funkci. Používá falešný SSL certifikát, kterým oklame uživatele i server a bez jejich svolení získává informace

z jejich komunikace. Cílem je získat informace, jako například uživatelská jména, detaily o účtu, nebo čísla kreditních karet, které dále mohou sloužit například ke krádeži finančních prostředků. Typickým cílem těchto útoků jsou uživatelé elektronického bankovnictví a dalších služeb, kde jsou nezbytné přihlašovací údaje. Pro ochranu před tímto typem útek je vhodné vyhnout se používání Wi-Fi na veřejných místech, nebo bez důkladného zabezpečení, dále odhlašování z aplikací, kde hrozí ztráta citlivých dat. Uživatel by také měl sledovat upozornění na nezabezpečené stránky u webových prohlížečů.
(Imperva 2, citováno online 29.12.2016)
Na konci roku 2015 došlo ke stažení některých aplikací dostupných z distribučního kanálu App Store pro iOS na základě možnosti úniku dat právě pomocí Man in the Middle. Aplikace sloužící k blokování marketingových sdělení instalovaly certifikát, který umožňoval přerušit cestu šifrovaných dat. K tomuto problému byla vydána pouze krátká tisková zpráva. Zpětně se však riziku útoku mohou uživatelé vyhnout odstraněním certifikátu v menu nastavení zařízení. Tato cesta ovšem pro běžné uživatele není příliš známá.
(Dočekal, 2015, citováno online 29.12.2016)

3 Vlastní práce

V praktické části budou srovnány bankovní aplikace čtyřech bank působících na území České republiky. Srovnání proběhne pomocí vícekriteriální analýzy variant, konkrétně metodou analytického hierarchického procesu.
První vybranou aplikací pro mobilní bankovnictví ke srovnání bude SERVIS 24 od České spořitelny, a to z důvodu dlouhodobě nejvyššího počtu klientů.
Druhou aplikací bude mobilní řešení od Equa bank. Banka funguje na českém od září roku 2011 a v současnosti má více než 250 tisíc klientů. Equa bank byla vybrána jako zástupce moderní nízkonákladové banky, která při splnění několika podmínek nabízí vedení účtu kompletně zdarma, včetně výběrů z bankomatů ostatních bank.
Jako třetí aplikace byla vybrána Era SmartBanking od Era – Poštovní spořitelna, především z důvodu, že banka patří do skupiny ČSOB, tudíž se aplikace ČSOB SmartBanking a Era SmartBanking liší pouze grafickou úpravou. Co se týče funkcionalit, jsou na tom obě aplikace stejně, proto srovnání do určité míry budou moci využít i klienti ČSOB. Aplikace Era byla upřednostněna oproti ČSOB z důvodu rozsáhlé marketingové kampaně z roku 2014 zaměřenou na používání mobilní aplikace.
Poslední aplikací bude Mobilní eKonto od Raiffeisenbank, která získala ocenění Nejlepší banka roku a Klientsky nejpřívětivější banka roku za rok 2016 v osmém ročníku udělování cen Hospodářských novin s názvem Nejlepší banka. Název aplikace Mobilní eKonto pochází z doby před prodejem eBanky (Expandia Banky) finanční skupině Raiffeinsen International.

3.1 Kritéria hodnocení

Po představení jednotlivých bankovních aplikací bude provedeno jejich srovnání pomocí metody analytického hierarchického procesu (dále jen AHP). K hodnocení budou sloužit jednotlivá kritéria představená v této kapitole, kde budou také určeny jejich váhy, a to Saatyho metodou, které se provádí párovým porovnávání důležitosti objektů.

3.1.1 Cena

Pro aktivní používání aplikace pro mobilní bankovnictví musí mít uživatel zřízen účet u finanční instituce, u kterého platí za jednotlivé služby poplatky dle ceníku. Z toho důvodu

je kritérium cena zahrnuto do porovnání jednotlivých bankovních aplikací. Z ceníku bank budou vybrány jednotlivé úkony, které v průběhu měsíce průměrný klient využívá. Konkrétně se jedná o zadání jednorázového a trvalého příkazu k úhradě přes mobilní aplikaci, poplatek za vedení účtu, příchozí platbu, měsíční výpis elektronickou formou a výběr z bankomatu vlastní a cizí banky. Ke srovnání bude využita následující tabulka, která uvažuje aktivního uživatele mobilního bankovnictví. Celková suma za poplatky poté poslouží při výběru kompromisní varianty pomocí metody AHP.

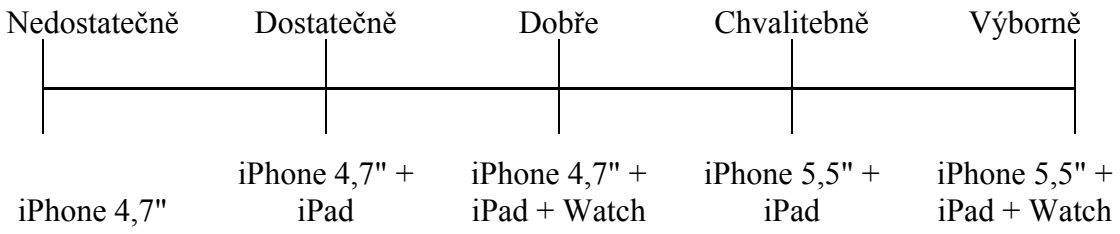
Tabulka 2 - Přehled využití služeb

Služba	Četnost (měsíčně)
Poplatek za vedení běžného účtu v CZK	1x
Odchozí platba	5x
Zadání trvalého příkazu k úhradě	1x
Příchozí platba	3x
Výběr z bankomatu vlastní banky	2x
Výběr z bankomatu cizí banky	1x

Zdroj: vlastní zpracování

3.1.2 **Optimalizace**

Kritérium optimalizace bude hodnotit, zda jsou jednotlivé aplikaci uzpůsobeny pro různá zařízení pracující na mobilní platformě Apple. Prvním předpokladem je, aby prostředí aplikace bylo optimalizováno pro všechny verze mobilních telefonů iPhone včetně verzí Plus s 5,5“ displejem s rozlišením 1920x1080 pixelů. Dále bude hodnoceno, zda je aplikace dostupná ve verzi pro tablety, které jsou v dnešní době pro některé uživatele schopné nahradit stolní počítač, či notebook. Jako poslední bude kritérium optimalizace uvažovat přítomnost verze pro chytré hodinky Apple Watch, která prozatím umožňuje pouze pasivní kontrolu účtu. Jelikož toto kritérium nelze kvantifikovat, bude u jednotlivých variant upraveno pomocí hodnotící škály.



3.1.3 **Recenze**

Dalším kritériem, které je nutné zahrnout do celkového hodnocení jsou uživatelské recenze. Pro potřeby srovnání budou použita hodnocení jednotlivých aplikací v elektronickém distribučním kanálu pro aplikace App Store. Recenzenti z řad uživatelů mohou aplikaci přiřadit hodnocení od jedné do pěti hvězdiček a slovní komentář. Průměrné hodnocení bude zahrnuto při výběru kompromisní varianty.

3.1.4 **Uživatelská zkušenost**

Uživatelská zkušenost je jediným kritériem, které je hodnoceno subjektivně na základě poznatků autora z testování jednotlivých aplikací. Do tohoto kritéria je zahrnut design aplikace, uživatelská přívětivost, celková orientace uvnitř aplikace a použitelnost. Důležitou součástí kritéria je také samotná aktivace bankovní aplikace a propojení s účtem, jelikož banky u tohoto kroku nabízí odlišné postupy. Vzhledem k faktu, že se jedná o subjektivní hodnocení kritéria a při testování se neprojevily u žádné z aplikací zásadní slabá místa a problémy, bude toto kritérium při výpočtech nabývat pouze tří hodnot na škále, a to průměrná, dobrá a výborná.

3.1.5 **Zabezpečení**

Pro mnoho uživatelů se v případě aplikace pro mobilní bankovnictví jedná o nejdůležitější kritérium. Dalo by se předpokládat, že banky kromě šifrované komunikace mezi svými servery a klientem nabídnout obdobné možnosti uživatelského zabezpečení aplikace. To se ale liší například minimální délkou alfanumerického hesla k přihlášení do aplikace, možností změny hesla v aplikace nebo využitím bezpečnostních prvků, které jsou k dispozici v mobilním telefonu. Například u zařízení Apple to je čtečka otisků prstů Touch ID, která společně minimální s délkou a složitostí vstupního hesla bude sloužit při hodnocení bankovních aplikací u kritéria zabezpečení.

3.1.6 **Stanovení vah kritérií**

Při tvorbě modelu vícekriteriální analýzy variant je nutné mít všechny jeho komponenty k výpočtu pomocí vybrané metody AHP. Kromě výše uvedených kritérií, variant v podobě jednotlivých aplikací pro mobilní bankovnictví a kriteriální matice s hodnotami je nezbytné stanovit také relativní důležitost všech kritérií, jinými slovy určit jejich váhy.

K tomu účelu bude využita Saatyho metoda založena na porovnání důležitosti jednotlivých kritérií ve dvojicích. Výpočet vah probíhá v Saatyho matici za pomoci určené stupnice vyjadřující sílu preference jednoho kritéria oproti druhému. Stupnice nabývá hodnot 1;3;5;7;9, kdy 1 – znamená rovnost, 3 – slabou preferenci, 5 – silnou preferenci, 7 – velmi silnou preferenci a 9 – absolutní preferenci. Matice musí být vždy čtvercová (v řádcích a sloupcích jsou stejná kritéria) a také reciproční (při porovnání preferencí dvou kritérií musí platit obrácené hodnoty).

Následně se pro každý řádek (kritérium) vypočítá geometrický průměr ($\sqrt[n]{a_1 \times a_2 \times \dots a_n}$) označený jako R_i, který se pro určení váhy V_i normalizuje vztahem:

$$V_i = \frac{R_i}{\sum_{i=1}^{n} R_i}, i = 1,2, \dots, n, kde\ R_i\ je\ geometrický\ průměr\ i-tého\ kritéria$$

Pro stanovení vah jsou jednotlivá kritéria označena písmenem f s číselným indexem a výsledné hodnoty zaokrouhleny na 3 desetinná místa.

Tabulka 3 - Saatyho metoda – stanovení vah kritérií

	f1	f2	f3	f4	f5	Ri	Vi
f1	1	5	3	1/3	1	1,380	0,221
f2	1/5	1	1	1/7	1/5	0,356	0,057
f3	1/3	1	1	1/3	1/3	0,517	0,083
f4	3	7	3	1	1/3	1,838	0,295
f5	1	5	3	3	1	2,141	0,344
					Σ	6,233	1

Kritérium	Cena	Optimalizace	Recenze	Uživatelská zkušenost	Zabezpečení
Označení	f1	f2	f3	f4	f5
Váha	**0,221**	**0,057**	**0,083**	**0,295**	**0,344**

Zdroj: vlastní zpracování

3.2 Česká spořitelna

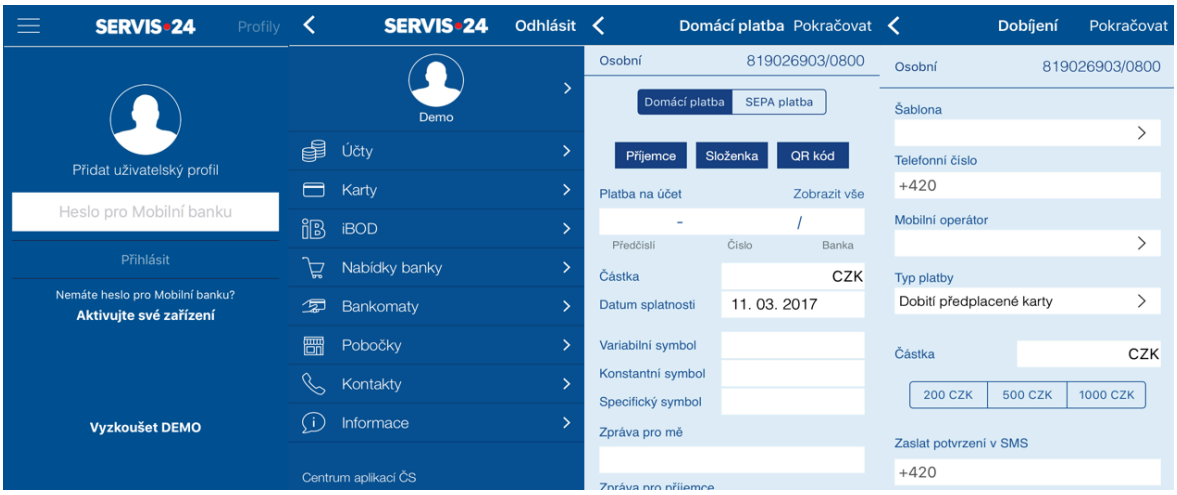
Banka s největším počtem klientů kromě plnohodnotné aplikace pro správu osobního účtu SERVIS 24 nabízí také další aplikace Můj stav a Friends 24. První zmíněná nabízí pasivní kontrolu zůstatků a pohybů a k přihlášení je možno použít čtečku otisků prstů Touch ID, která prozatím není k dispozici pro hlavní SERVIS 24. Friends 24 umožňuje realizovat odchozí platby bez znalosti čísla účtu příjemce. Postačí pouze kontaktní údaj v podobě telefonního čísla nebo například uživatelského jména na sociální síti.
Aktivace aplikace SERVIS 24 probíhá přes internetové bankovnictví, kde si uživatel vytvoří heslo, zapamatuje jednorázový aktivační kód a potvrdí kódem z SMS zprávy. Heslo, které musí obsahovat minimálně 8 znaků, z toho alespoň dvě číslice a dvě písmena, je uživatel kdykoliv změnit v prostředí mobilní aplikace, Touch ID v aktuální verzi 4.0.0 dosud není podporováno.
Vzhled aplikace je velice moderní a přehledný, všechny ovládací prvky jsou logicky umístěné. SERVIS 24 je kromě dostupnosti verze pro tablety iPad optimalizovaný i pro mobilní telefony s 5,5“ úhlopříčkou.
Největším problémem je cenová politika České spořitelny, kdy mimo poplatky za výběr z bankomatů jsou zpoplatněné také odchozí a příchozí platby.

Tabulka 4 - Vybrané poplatky – Česká spořitelna

	Odchozí platba	Trvalý příkaz	Příchozí platba	Výběr (ČS)	Výběr (Ostatní)
Četnost	5x	1x	3x	2x	1x
Cena	7 Kč	7 Kč	2 Kč	5 Kč	40 Kč
		Celkem/měsíc	**98 Kč**		

Zdroj: (Česká spořitelna 1, 2017, citováno online 25.2.2017), vlastní zpracování

Obrázek 3 – Prostředí aplikace Servis 24



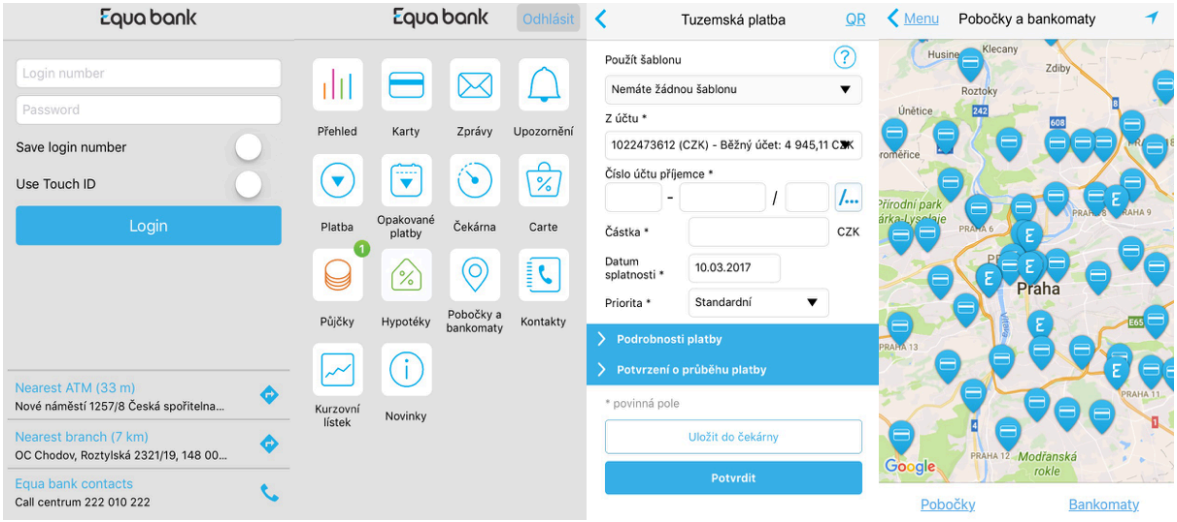
Zdroj: vlastní zpracování

Velkou předností je naopak skenování poštovní poukázky typu A za účelem platby, dále poté vytvoření platebních údajů ve formě QR kódu, nastavení limitů pro platby a možnost dobití předplacených telefonních karet z účtu. V hodnocení uživatelů na App Store získala aplikace SERVIS 24 3,5 hvězdiček z 5 možných.

3.3 Equa bank

Jediný zástupce konceptu nízkonákladových bank v porovnání je aplikace Equabank, která v mnoha kritériích obstála na výbornou. Jako jediná aplikace nabízí podporu Touch ID (mimo hesla 8-30 znaků, kde nelze použít 4 po sobě jdoucí stejné znaky).
Aktivace probíhá potvrzením na stránkách internetového bankovnictví, které nabízí téměř identický design. Přechod na mobilní platformu tak nebude pro uživatele žádný problém. Základní menu je v mřížkovém designu a nabízí přímý přístup k nejběžnějším funkcím. Nedostatkem je malý kontrast ovládacích prvků a absence verze pro tablet i neoptimalizované prostředí pro telefony s větší úhlopříčkou displeje. Vzhledem k nulovým poplatkům za všechny hodnocené služby nabízí aplikace již na úvodní aplikace možnost navigace k nejbližšímu bankomatu kterékoliv banky a pobočky Equa bank. Nevýhodou je absence jakékoliv demo verze.
Přes výhodu v podobě podpory Touch ID má aplikace hodnocení pouze 3 hvězdičky.

Obrázek 4 – Prostředí aplikace Equabank



Zdroj: vlastní zpracování

3.4 Era – Poštovní spořitelna

Aplikace Era Smartbanking jako jediná nepotřebuje ke své aktivaci zřízené internetové bankovnictví. Aplikaci uživatel uvede do provozu pomocí identifikačního čísla a PIN kódu, které získal při zřízení služby, následně potvrdí devítimístným SMS kódem a dále už se přihlašuje pouze zvoleným číselným PIN kódem o délce pouze pěti znaků.

Z porovnávaných aplikací pouze Era nabízí verzi pro hodinky Apple Watch, která je v aktuální verzi schopna zobrazit jen zůstatky a poslední pohyby na účtech. Až na barevnou kombinaci je vzhled totožný s aplikací od ČSOB a z testovaných se nejvíce přibližuje aplikaci SERVIS 24, rušivým prvkem je reklama umístěná již na přihlašovací stránce. Era je v App Store (hodnocení uživatelů 4 hvězdičky) k dispozici ve verzi pro tablety iPad, optimalizaci pro větší verze mobilního telefonu iPhone nenabízí.

Era – Poštovní spořitelna má poplatky u osobního účtu přibližně na úrovni České spořitelny, jediným rozdílem je vedení účtu, za který si Česká spořitelna měsíční poplatek neúčtuje.

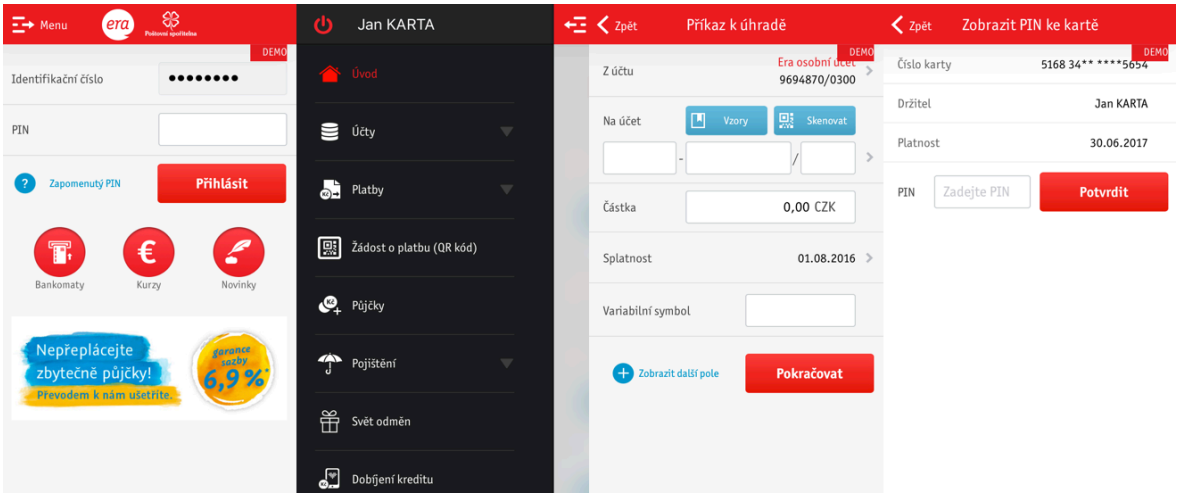
Mimo standardního nastavení u platebních karet (Nastavení limitů, blokace) umožňuje Smartbanking od Era zobrazit po zadání přístupového kódu a upozornění, zdali se uživatel nachází na bezpečném místě, PIN k dané platební kartě.

Tabulka 5 - Vybrané poplatky – Era Poštovní spořitelna

	Vedení účtu	Odchozí platba	Trvalý příkaz	Výběr (ČSOB)	Výběr (Ostatní)
Četnost	1x	5x	1x	2x	1x
Cena	34 Kč	2 Kč	2 Kč	5 Kč	40 Kč
		Celkem/měsíc	96 Kč		

Zdroj: (Era osobní účet, 2016, online citováno 25.2.2017), Vlastní zpracování

Obrázek 5 - Prostředí aplikace Era Smartbanking



Zdroj: vlastní zpracování

Obrázek 6 - Prostředí aplikace Era Smartbanking (Apple Watch)

Zdroj: vlastní zpracování

3.5 **Raiffeisenbank**

Mobilní aplikace od Raiffeisenbank s názvem Mobilní eKonto nabízí uživateli pouze běžné funkce, jedinou zajímavostí je možnost skenování čárových kódů a porovnání cen výrobků na základě internetového srovnávače cen heureka.cz.
Aktivace Mobilního eKonto probíhá přes internetové bankovnictví Raiffeisenbank, podobně jako u České spořitelny, jen k přihlášení do aplikace slouží u eKonta pouze čtyřmístný numerický kód, který lze změnit v menu aplikace. Po aktivaci je zobrazený typ mobilního telefonu, datum aktivace a možnost aplikaci deaktivovat. Bohužel prostředí internetového bankovnictví působí zastarale, nepřehledně a vzhledově neodpovídá mobilní aplikaci.
Základní osobní účet od Raiffeisenbank eKonto smart je při splnění podmínky měsíčního obratu na účtu bez poplatků.
Přes uživatelské recenze na App Store (3,5 hvězdičky), kde je k dispozici verze pro tablety iPad (aplikace není optimalizovaná pro telefony s větší úhlopříčkou) byla uživatelská zkušenost s aplikací vyhodnocena pouze jako průměrná. Zastaralý design, zdvojené ovládací prvky a nedostatek funkcionalit oproti ostatním porovnávaným aplikacím převážily nad jednoduchým a přehledným základním přehledem účtů.

Obrázek 7 - Prostředí aplikace Mobilní eKonto

Zdroj: vlastní zpracování

3.6 Vícekriteriální analýza variant

Model vícekriteriální analýzy variant sestavený za účelem výběru kompromisní varianty a sestavení pořadí jednotlivých aplikací dle hodnocení bude vypočten metodou analytického hierarchického procesu (AHP), jejímž základem je hierarchické struktura úlohy, kdy prvky na vyšší úrovni rozdělují svoji váhu na nižší úrovni hierarchie. Na každé úrovni je proto součet vah roven 1. I přes větší rozsah úlohy byla tato metoda zvolena, jelikož umožňuje dobře pracovat s neměřitelnými kritérii a na třetí úrovni hierarchie při výpočtu užitku jednotlivých variant podle daného kritéria v Saatyho matici dosáhnout přesnějších hodnot díky párovému porovnání.

Před samotným výpočtem je nutné sestavit kompletní model s komponenty vícekriteriální analýzy variant, které byly určeny v přechozích kapitolách práce.

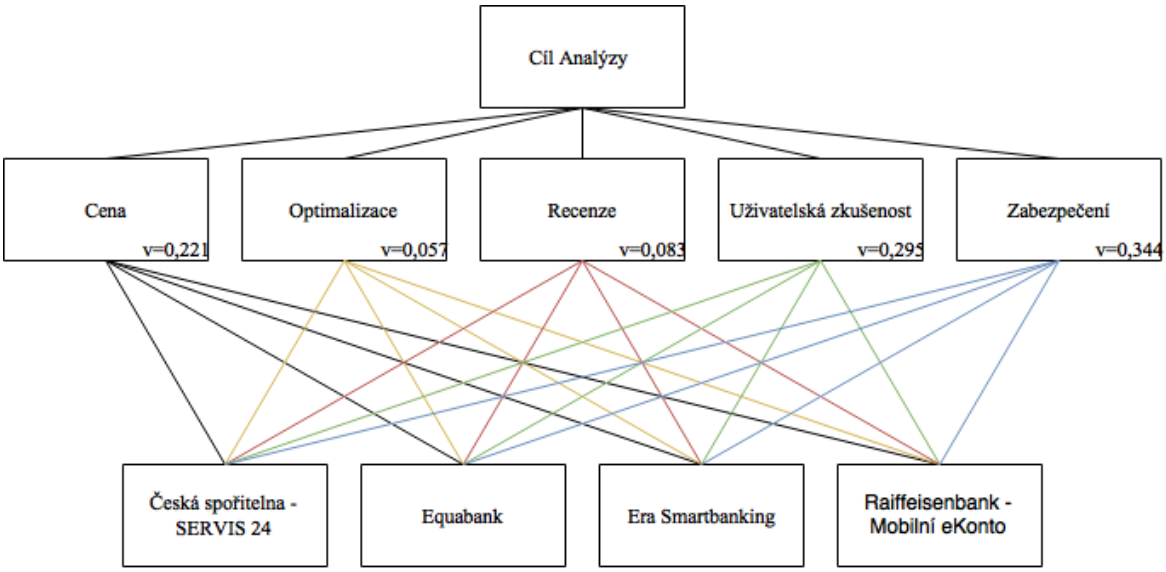
Tabulka 6 – Model vícekriteriální analýzy variant

		f1	f2	f3	f4	f5
		Cena	Optimalizace	Recenze	Zkušenost	Zabezpečení
a1	ČS SERVIS 24	98 Kč	chvalitebně	★★★½☆	Výborná	8 znaků (kombinace)
a2	Equabank	0 Kč	nedostatečně	★★★☆☆	Dobrá	8 znaků + Touch ID
a3	ERA Smartbanking	96 Kč	dobře	★★★★☆	Dobrá	5 znaků (číslice)
a4	RB Mobilní eKonto	0 Kč	dostatečně	★★★½☆	Průměrná	4 znaky (číslice)
	vi	0,221	0,057	0,083	0,295	0,344

Zdroj: vlastní zpracování

Po kompletním sestavení modelu je dalším krokem sestavení diagramu pro metodu AHP a následný výpočet užitku variant pro jednotlivá kritéria (U_{ij}), který probíhá výpočtem a normalizací geometrického průměru (R_i) v Saatyho matici dle váhy daného kritéria a určení kompromisní řešení a pořadí jednotlivých variant.

Obrázek 8 – Schéma metody AHP



Zdroj: vlastní zpracování

Tabulka 7 – Výpočet metodou AHP

f1	a1	a2	a3	a4	Ri	norm. Ri	Uij
a1	1	1/9	1/3	1/9	0,253	0,040	**0,009**
a2	9	1	7	1	2,817	0,441	**0,098**
a3	3	1/7	1	1/7	0,497	0,078	**0,017**
a4	9	1	7	1	2,817	0,441	**0,098**
					6,385	1	0,221
f2	a1	a2	a3	a4	Ri	norm. Ri	Uij
a1	1	7	3	5	3,201	0,564	**0,032**
a2	1/7	1	1/5	1/3	0,312	0,055	**0,003**
a3	1/3	5	1	3	1,495	0,263	**0,015**
a4	1/5	3	1/3	1	0,669	0,118	**0,007**
					5,678	1	0,057
f3	a1	a2	a3	a4	Ri	norm. Ri	Uij
a1	1	3	1/3	1	1,000	0,201	**0,017**
a2	1/3	1	1/5	1/3	0,386	0,078	**0,006**
a3	3	5	1	3	2,590	0,520	**0,043**
a4	1	3	1/3	1	1,000	0,201	**0,017**
					4,976	1	0,083

f4	a1	a2	a3	a4	Ri	norm. Ri	Uij
a1	1	5	5	9	3,873	0,632	**0,186**
a2	1/5	1	1	5	1,000	0,163	**0,048**
a3	1/5	1	1	5	1,000	0,163	**0,048**
a4	1/9	1/5	1/5	1	0,258	0,042	**0,012**
					6,131	1	0,295

f5	a1	a2	a3	a4	Ri	norm. Ri	Uij
a1	1	1/3	5	7	1,848	0,290	**0,100**
a2	3	1	7	9	3,708	0,582	**0,200**
a3	1/5	1/7	1	3	0,541	0,085	**0,029**
a4	1/7	1/9	1/3	1	0,270	0,042	**0,015**
					6,367	1	0,344

Zdroj: vlastní zpracování

Na základě výpočtu, budou určeny výsledky jednotlivých variant, a to jednoduchou sumací užitků variant podle všech pěti kritérií. Výsledky mohou nabývat hodnot z intervalu <0;1>, kdy číslo nejblíže jedné je uvažováno jako kompromisní řešení (nejlepší z porovnávaných).

Tabulka 8 – Výsledky vícekriteriální analýzy variant

Uij	f1	f2	f3	f4	f5	Výsledek
a1	0,009	0,032	0,017	0,186	0,100	0,344
a2	0,098	0,003	0,006	0,048	0,200	0,356
a3	0,017	0,015	0,043	0,048	0,029	0,153
a4	0,098	0,007	0,017	0,012	0,015	0,148

Zdroj: vlastní zpracování

4 Shrnutí výsledků

V úvodu praktické části byla definována kritéria, podle kterých byla provedena analýza aplikací pro mobilní platformu Apple umožňující správu osobního účtů čtyř bank působících v České republice. Na základě stanovené důležitosti kritérií cena, optimalizace, recenze, uživatelská zkušenost a zabezpečení byly prostřednictvím metody analytického hierarchického procesu stanovena kompromisní varianta a pořadí jednotlivých aplikací podle splnění jednotlivých kritérií.

Tabulka 9 - Interpretace výsledků

Aplikace pro mobilní bankovnictví	Hodnocení	Doporučení
Equabank	0,356	Lze doporučit
Česká spořitelna – SERVIS 24	0,344	Lze doporučit
Era Smartbanking	0,153	Nelze doporučit
Raiffeisenbank – Mobilní eKonto	0,148	Nelze doporučit

Zdroj: vlastní zpracování

Aplikace Equabank získala nejvyšší hodnocení následována službou SERVIS 24 od České spořitelny. Vzhledem odlišného konceptu těchto bank je možné z porovnaných aplikací doporučit alternativu pro klienty upřednostňující tradiční banku i moderní nízkonákladovou variantu v podobě Equabank.

Třetí a čtvrtou pozici obsadily Era Smartbanking a Mobilní eKonto od Raiffeisenbank, které získaly téměř stejné hodnocení. Vzhledem k nízkému hodnocení oproti prvním dvěma jmenovaným nelze tyto aplikace doporučit.

Pokud by Česká spořitelna změnila cenovou politiku u poplatků k běžnému účtu, umístila by se na prvním místě. U aplikace Equabank by vývojáři měli optimalizovat vzhled pro nová zařízení a tablety. Mobilní eKonto by si zasloužilo celkovou modernizaci nebo kompletně novou verzi, reflektující nové služby a možnosti zabezpečení běžné u konkurence. Řešení od Era – Poštovní spořitelna je v mnoha ohledech průměrné, do hodnocení se však promítly vysoké poplatky například za vedení účtu.

5 Závěr

Hlavním cíle bakalářské práce byla analýza a porovnání aplikací pro mobilní bankovnictví s orientací na aplikace bank působících v České republice. Hlavní cíl byl rozčleněný do čtyřech dílčích cílů, jejichž splnění bylo následující.

Charakterizovat současné bankovní aplikace s důrazem na bezpečnostní prvky:
Aplikace pro mobilní bankovnictví nabízí v dnešní době 15 bank působících na českém trhu. Prostřednictví elektronických distribučních kanálů jsou ke stažení do mobilních zařízení s operačním systémem iOS, Android OS a ve většině případů i Windows 10 Mobile.
Mezi funkcionality typické pro mobilní bankovnictví, které jsou rozdělené v rámci aplikace na veřejnou a uzavřenou část, patří použití QR kódu s platebními údaji. Moderním řešením se také pomalu stává využití NFC v mobilním zařízení namísto platební karty.
V souvislosti s charakteristikou mobilní platformy Apple byl představen bezpečnostní prvek v podobě čtečky otisků prstů Touch ID a možnosti zabezpečení na úrovni dat, aplikací, síťové komunikace a samotného zařízení. Neméně důležitou součástí je charakteristika bezpečnostních hrozeb, které mohou být cílem mobilního bankovnictví.

Analyzovat a porovnat vybrané mobilní aplikace českých bank:
Nejprve byly zvoleny čtyři aplikace pro mobilní bankovnictví a zvolena kritéria pro jejich analýzu. Konkrétně se jednalo o aplikace České spořitelny, Equabank, Era – Poštovní spořitelny a Raiffeisenbank. Kritéria byla zvolena na základě uživatelských potřeb. Mezi základní se řadí zabezpečení aplikace a cena poplatků spojených s využíváním mobilní aplikace. Dalším rozhodujícím kritériem byla uživatelská zkušenost autora, která přímo hodnotí použitelnost aplikací pramenící z osobních poznatků. Dílčími kritérii byly uživatelské recenze vybraných aplikací v obchodu App Store a optimalizace aplikací pro různá zařízení využívající mobilní platformu Apple.

Pomocí vhodných metod a postupů zhodnotit aplikace pro mobilní bankovnictví na platformě Apple:
Spolu s kritérii bylo nutné stanovit jejich relativní důležitost, která byla určena Saatyho metodou párového porovnání. Následně byla provedena charakteristika vybraných aplikací, jejich funkcionality a určeny hodnoty pro jednotlivá kritéria.

Po kompletaci modelu byla provedena vícekriteriální analýza variant pomocí metody analytického hierarchického procesu (AHP), který umožňuje pracovat s neměřitelnými kritérii a byl proto vhodný pro daný model. Výpočet umožnil stanovit pořadí aplikací a stanovit kompromisní variantu.

Formulace a závěrečná doporučení:

Mobilní bankovnictví je v současnosti stále rostoucím trendem, který převážně u mladší generace nahrazuje další formy komunikace s bankou a všeobecně mění pohled na klasický způsob správy bankovního účtu. Na základě výsledků analýzy je možné zcela doporučit dvě vybrané aplikace, konkrétně Equabank a SERVIS 24 od České spořitelny. Obě aplikace získaly velice podobný výsledek s mírnou preferencí Equabank. Zbylé dvě aplikace, Era Smartbanking a Mobilní eKonto od Raiffeisenbank, vzhledem k výsledkům analýzy, nelze ve verzi pro mobilní platformu Apple doporučit.

6 Seznam použitých zdrojů

APPLE 1: App Store. Apple.com [online]. 2017 [cit. 2017-02-25]. Dostupné z: https://developer.apple.com/support/app-store/

APPLE 2: Apple Pay participating banks and card issuers in Europe. Apple.com [online]. 2017 [cit. 2017-03-08]. Dostupné z: https://support.apple.com/cs-cz/ht206638

APPLE 3: iOS Security Guide. Apple.com [online]. 2016 [cit. 2017-02-21]. Dostupné z: http://www.apple.com/business/docs/iOS_Security_Guide.pdf

APPLE 4: iPhone Features. Web.archive.org [online]. 2007 [cit. 2017-02-06]. Dostupné z: http://www.apple.com/iphone/features/index.html

BLOCKCHAIN: My Wallet Features List. Blockchain.info [online]. [cit. 2017-02-06]. Dostupné z: https://blockchain.info/wallet/features

BRIGNALL, Miles: 'Error 53' fury mounts as Apple software update threatens to kill your iPhone 6. Theguardian.com [online]. 2016 [cit. 2017-02-22]. Dostupné z: https://www.theguardian.com/money/2016/feb/05/error-53-apple-iphone-software-update-handset-worthless-third-party-repair

BUBÁK, Zdeněk: ČSOB nabízí mobilní bankovnictví i pro chytré hodinky. Finaparada.cz [online]. 2017 [cit. 2017-02-20]. Dostupné z: http://finparada.cz/4137-CSOB-nabizi-mobilni-bankovnictvi-i-pro-chytre-hodinky.aspx?mobile=full

BUBÁK, Zdeněk: Začínáme seriál o mobilním bankovnictví v Česku. Postupně představíme aplikace vybraných bank. Finparada.cz [online]. 2015 [cit. 2017-01-20]. Dostupné z: http://www.finparada.cz/2665-Zaciname-serial-o-mobilnim-bankovnictvi-v-Cesku.aspx

CLOVER, Juli: Apple Releases iOS 7.1.2 With Mail Fixes, iBeacon Improvements. Macrumors.com [online]. 2014 [cit. 2017-02-18]. Dostupné z: https://www.macrumors.com/2014/06/30/apple-release-ios-7-1-2/

COLLINSON, Patrick: Lloyds bank accounts targeted in huge cybercrime attack. Theguardian.com [online]. 2017 [cit. 2017-01-24]. Dostupné z: https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

COSKUN, Vedat., Kerem. OK a Busra. OZDENIZCI. Near field communication: from theory to practice. Hoboken, NJ: Wiley, 2012. ISBN 9781119971092.

COSTELLO, Sam: A Definition of Jailbreaking on the iPhone. Lifewire.com [online]. 2017 [cit. 2017-02-13]. Dostupné z: https://www.lifewire.com/definition-of-jailbreaking-iphone-2000246

ČESKÁ BANKOVNÍ ASOCIACE: Standard ČBA – Formát pro sdílení platebních údajů v rámci tuzemského platebního styku v CZK prostřednictvím QR kódů. Czech-ba.cz [online]. 2015 [cit. 2017-02-03]. Dostupné z: https://www.czech-ba.cz/sites/default/files/standard_26_qr_externi_final_srpen_2015.pdf

ČESKÁ SPOŘITELNA 1: Ceník pro Základní účet. Csas.cz [online]. 2017 [cit. 2017-02-25]. Dostupné z: http://www.csas.cz/banka/nav/osobni-finance/zakladni-ucet-d00028444

ČESKÁ SPOŘITELNA 2: Průvodce aplikací Friends 24. Friends24.cz [online]. 2016 [cit. 2017-01-20]. Dostupné z: https://www.friends24.cz/#/r#o-aplikaci

ČESKÁ SPOŘITELNA 3: Základy bezpečeného používání internetbankingu. Csas.cz [online]. [cit. 2016-12-29]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/sc_2634.xml

ČESKÝ STATISTICKÝ ÚŘAD: Čechů s internetem v mobilu rychle přibývá. Czso.cz [online]. 2016 [cit. 2016-12-29]. Dostupné z: https://www.czso.cz/csu/czso/cechu-s-internetem-v-mobilu-rychle-pribyva

DENSO ADC: QR code essentials [online]. 2011 [cit. 2017-01-21]. Dostupné z: http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802

DOČEKAL, Daniel: Apple odstranil aplikace schopné šmírovat v šifrované komunikaci. Lupa.cz [online]. 2015 [cit. 2016-12-29]. Dostupné z: http://www.lupa.cz/clanky/apple-odstranil-aplikace-schopne-smirovat-v-sifrovane-komunikaci/

DORMEHL, Luke: Apple cuts App Store approval time to just one day. Cultofmac.com [online]. 2016 [cit. 2016-12-10]. Dostupné z: http://www.cultofmac.com/428101/apple-cuts-app-store-approval-time-to-just-one-day/

EDWARDS, Chris: List of QR Code readers for iPhone, Android, Windows Phone 7 and Blackberry. 708media.com [online]. 2010 [cit. 2017-01-22]. Dostupné z: http://www.708media.com/qrcode/qr-code-readers-iphone-android-blackberry-windows-phone-7/

ERA osobní účet: Ceník. Erasvet.cz [online]. 2016 [cit. 2017-02-25]. Dostupné z: https://www.erasvet.cz/fyzicke-osoby/ucty/stranky/osobni-ucet/cenik.aspx

FIREFOX: MarketPlace. Firefox.com [online]. 2017 [cit. 2017-02-19]. Dostupné z: https://marketplace.firefox.com

GOODE, Lauren: App Store 2.0. Theverge.com [online]. 2016 [cit. 2017-02-21]. Dostupné z: http://www.theverge.com/2016/6/8/11880730/apple-app-store-subscription-update-phil-schiller-interview

HOLZMAN, Ondřej: Apple Pay – slibná platforma, o níž se příliš nemluví. Jablickar.cz [online]. 2014 [cit. 2016-12-29]. Dostupné z: http://jablickar.cz/apple-pay-slibna-platforma-o-niz-se-prilis-nemluvi/

HOVORKA, Jiří: Fakturu zaplatíte přes foťák v mobilu. QR kódy se šíří. Zpravy.aktualne.cz [online]. 2014 [cit. 2017-02-06]. Dostupné z: https://zpravy.aktualne.cz/finance/fakturu-zaplatite-pres-fotak-v-mobilu-qr-kody-se-siri/r~e097d4c8897111e3ad9a0025900fea04/?redirected=1488221482

CHARTIER, David: iPhone OS gets new name, video calling. Macworld.com [online]. 2010 [cit. 2017-02-06]. Dostupné z: http://www.macworld.com/article/1151812/iphone_os_4_wwdc.html

IMPERVA 1: Denial of Service Attacks. Incapsula.com [online]. [cit. 2016-12-28]. Dostupné z: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

IMPERVA 2: Man in the Middle (MITM) Attack. Incapsula.com [online]. [cit. 2016-12-29]. Dostupné z: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

ISO 13616: Financial services - International bank account number (IBAN) -- Part 1: Structure of the IBAN. Iso.org [online]. 2007 [cit. 2017-02-03]. Dostupné z: https://www.iso.org/standard/41031.html

KALABIS, Zbyněk. Základy bankovnictví: bankovní obchody, služby, operace a rizika. Brno: BizBooks, 2012. ISBN 978-80-265-0001-8.

KEIZER, Greg: iOS App Store went on record-setting tear in 2012. Computerworld.com [online]. 2013 [cit. 2017-02-18]. Dostupné z: http://www.computerworld.com/article/2494477/mobile-apps/ios-app-store-went-on-record-setting-tear-in-2012.html

KEYWORTH, Marie: Hacker Lexicon: What Are Phishing and Spear Phishing? Bbc.com [online]. 2016 [cit. 2016-12-29]. Dostupné z: http://www.bbc.com/news/business-35201188

LASHINSKY, Adam. Inside Apple: the secrets behind the past and future success of Steve Job's iconic brand. London: John Murray, 2012. ISBN 1848547218.

LÁSKA, Jan: ČSOB spustila NFC platby mobilem. Bez operátorů. Mobilmania.cz [online]. 2016 [cit. 2017-01-20]. Dostupné z: http://www.mobilmania.cz/clanky/csob-spustila-nfc-platby-mobilem-bez-operatoru/sc-3-a-1334836/default.aspx

LEE, Jenny: Tesco's cool QR code advertising campaign. Vancouversun.com [online]. 2012 [cit. 2017-01-21]. Dostupné z: http://vancouversun.com/news/staff-blogs/tescos-cool-qr-code-advertising-campaign

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

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

MEDUNA, Martin. Bezpečnost mobilních zařízení s operačním systémem iOS. IT Systems. 2013, **2013**(1-2), 46-48. ISSN ISSN 1802-615X.

NICOLETTI, Bernardo. Mobile banking: evolution or revolution?. Palgrave studies in financial services technology series. ISBN 978-1-137-38655-7.

PEREZ, Sarah: Apple's big App Store purge is now underway. Techcrunch.com [online]. 2016 [cit. 2016-12-29]. Dostupné z: https://techcrunch.com/2016/11/15/apples-big-app-store-purge-is-now-underway/

QR CODE 1: History of QR code. Qrcode.com [online]. [cit. 2017-01-20]. Dostupné z: http://www.qrcode.com/en/history/

QR CODE 2: How to introduce it? [online]. [cit. 2017-01-21]. Dostupné z: http://www.qrcode.com/en/howto/

QR PLATBA: Generátor QR Platby. Qr-platba.cz [online]. 2017 [cit. 2017-02-06]. Dostupné z: http://qr-platba.cz/generator/#content-full

QUORA: What percentage of iPhones have been jailbroken? Quora.com [online]. 2017 [cit. 2017-02-16]. Dostupné z: https://www.quora.com/What-percentage-of-iPhones-have-been-jailbroken

ROSSIGNOL, Joe: Apple Watch Dominated Holiday Season With Estimated 5.2 Million Shipment. Macrumors.com [online]. 2017 [cit. 2017-02-18]. Dostupné z: https://www.macrumors.com/2017/02/01/apple-watch-q4-2016-estimated-sales/

ROUSE, Margaret: Definition Phishing. Techtarget.com [online]. 2015 [cit. 2016-12-29]. Dostupné z: http://searchsecurity.techtarget.com/definition/phishing

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

STATISTA 1: Annual Apple App Store revenue from 2013 to 2016. Statista.com [online]. 2017 [cit. 2017-02-21]. Dostupné z: https://www.statista.com/statistics/296226/annual-apple-app-store-revenue/

STATISTA 2: App Stores. Statista.com [online]. 2016 [cit. 2017-01-20]. Dostupné z: https://www.statista.com/topics/1729/app-stores/

STATISTA 3: Number of apps available in leading app stores. Statista.com [online]. 2017 [cit. 2017-02-19].

STORM, Darlene: Flaw in iMessage encryption could be exploited to decrypt iCloud photos and videos. Computerworld.com [online]. 2016 [cit. 2016-12-29]. Dostupné z: http://www.computerworld.com/article/3046101/security/flaw-in-imessage-encryption-could-be-exploited-to-decrypt-icloud-photos-and-videos.html

STRATEGY Analytics: Global Smartwatch Vendor Shipments and Marketshare. Strategyanalytics.com [online]. 2017 [cit. 2017-02-18]. Dostupné z: https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2017/02/01/

SYSTEM Online: Komerční banka vylepšila vylepšuje svoji aplikaci pro hodinky Apple Watch. Systemonline.cz [online]. 2016 [cit. 2017-02-18]. Dostupné z: https://www.systemonline.cz/zpravy/komercni-banka-vylepsila-vylepsuje-svoji-aplikaci-pro-hodinky-apple-watch-z.htm

ŠMÍDOVÁ, Veronika: Jedna fotka z mobilu a je zaplaceno. Nabídněte zákazníkům faktury s QR kódy. Byznys.ihned.cz [online]. 2015 [cit. 2017-02-03]. Dostupné z: http://byznys.ihned.cz/podnikani/inspirace-technologie/c1-64081000-jedna-fotka-z-mobilu-a-je-zaplaceno-nabidnete-zakaznikum-faktury-s-qr-kody

UApp Explorer. Uappexplorer.com [online]. 2017 [cit. 2017-02-19]. Dostupné z: https://uappexplorer.com

VAN GROVE, Jeniffer: SCVNGR Unveils QR Code Payment System. Mashable.com [online]. 2011 [cit. 2017-01-22]. Dostupné z: http://mashable.com/2011/10/12/scvngr-levelup-redo/#hVJUkC1pXkqy

WHITNEY, Lance: Apple remains king of app-store market. Cnet.com [online]. 2011 [cit. 2017-02-18]. Dostupné z: https://www.cnet.com/news/report-apple-remains-king-of-app-store-market/

ZÁKON č. 21/1992 Sb.: Zákon o bankách. Zakonyprolidi.cz [online]. 2017 [cit. 2017-03-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/1992-21

ZÁKON č. 284/2009 Sb.: Zákon o platebním styku. Zakonyprolidi.cz [online]. 2017 [cit. 2017-03-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-284

ZETTER, Kim: Hacker Lexicon: What Are Phishing and Spear Phishing? Wired.com [online]. 2015 [cit. 2016-12-29]. Dostupné z: https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

7 Seznam Grafů, obrázků a tabulek