Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Provádění platebních operací za pomoci mobilní platformy Android OS

Bc. Jakub Zemen

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jakub Zemen

Informatika

Název práce

Provádění platebních operací za pomoci mobilní platformy Android OS.

Název anglicky

Execution of payment transactions with the help of the mobile platform Android OS.

Cíle práce

Diplomová práce je tematicky zaměřena na problematiku elektronického platebního styku při využití mobilních zařízeních a další oblasti s tím spojené. Hlavní cíle této práce jsou zaměřeny na různorodé možnosti při provádění platebních operací, a to především za pomoci mobilní platformy Android OS a dále se zaměřuje na bezpečnostní rizika s transakcemi spojená. Dílčí cíle vychází z analýzy cílových skupin a jejich různorodých požadavků na danou bankovní aplikaci. Tyto požadavky budou konfrontovány s možnostmi reálné aplikace, přičemž dalším dílčím cílem je odhlalení jejich případných rezer, které by přinesly širší využití jejich potenciálu získáním nových uživatelů. V neposlední řadě mezi dílčími cíle patří analýza bezpečnosti provádění bankovních operací za pomocí mobilních zařízení obecně, ale i na dané platformě.

Metodika

Metodika této práce bude zpracována prostřednictvím kvalitativních a kvantitativních metod. Analýza zájmových skupin bude vycházet z dotazníkového šetření, za pomoci kterého budou načerpána relevantní data se zohledněním potřeb daných uživatelů vzhledem k jejich přiřazení k zájmové skupině. Možnosti smartbanking aplikací budou reálně otestovány u dvou bankovních institucí a na základě zjištěných informací bude provedena konfrontace se získanými údaji, což povede k odhalení případných rezerv u nabízených funkcí, které by pro uživatele mohly mít zásadní vliv. Analýza bezpečnostních rizik bude vycházet především z literární rešerše a následně z analýzy aktuálních trendů, které útočníci nejčastěji využívají.

Doporučený rozsah práce

60 až 80 stran

Klíčová slova

Android OS, smartbanking, bankovní operace, bezpečnost, rizika

---

Doporučené zdroje informací

BURIAN, Pavel. Internet inteligentních aktivit. Vyd. 1. Praha: Grada Publishing a.s., 2014, 336 s. ISBN 978-80-247-5137-5.

KONDABAGIL, Jayaram. Risk Management in electronic banking: concepts and best practices. Singapore: John Wiley & Sons (Asia) Pte Ltd, 2007, 251 s. ISBN: 978-0-470-82243-2.

NOVOTNÝ, O., POUR, J., SLÁNSKÝ, D.: Business Intelligence Jak využít bohatství ve vašich datech, 1. vyd. Praha: Grada Publishing, 2004. 192 s. ISBN 80-247-1094-3.

Předběžný termín obhajoby

2015/16 ZS – PEF

Vedoucí práce

Ing. Karel Kubata

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 24. 11. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Provádění platebních operací za pomoci mobilní platformy Android OS" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2015 _____

Poděkování

Rád bych touto cestou poděkoval především Ing. Karlu Kubatovi za trpělivé vedení a konzultace při zpracovávání práce. Dále pak Ing. Martinu Havránkovi, Ph.D. za konzultace k literární rešerši a Ing. Janu Rydvalovi, Ph.D. za konzultace k analytické části práce zaměřené na vícekriteriální analýzu variant. V neposlední řadě i celé rodině a přátelům za jejich silnou podporu a to nejen po dobu zpracovávání této práce, ale za dobu celého studia.

Provádění platebních operací za pomoci mobilní platformy Android OS

Souhrn

Práce je zaměřena na služby mobilních bankovních (smartbanking) aplikací, na jejich využívání v ČR a na jejich další možnosti (funkcionality). Autor práce zvolil nejrozšířenější mobilní platformu Android OS, která je v práci zkoumána jak z pohledu struktury, tak i z pohledu bezpečnostních rizik, jež by mohly postihnout uživatele mobilní bankovní aplikace. Analytická část práce je konkrétně zaměřena na určení oblastí, které mohou pomoci rozšířit řady uživatelů těchto smartbanking aplikací. V první části jsou analyzovány závislosti kvalitativních znaků vztahujících se k postojům uživatelů elektronického bankovnictví. Druhá část je zaměřena na analýzu preferencí uživatelů vůči jednotlivým nabízeným funkcionalitám. Z literární rešerše a analytické části práce je v jejím závěru určeno, že případná absence funkcionalit silně ovlivní normalizovaný přínos pro uživatele a které konkrétní funkce na něj mají nejvyšší vliv. Na podkladě těchto zjištění jsou uvedeny závěry, které napomohou rozšířit řady reálných uživatelů a eliminují případná bezpečnostní rizika například využíváním antivirové aplikace či návrhem na ochranu proti útokům typu DoubleDirect.

Klíčová slova: Android OS, smartbanking, bankovní operace, funkcionality mobilních bankovních aplikací, bezpečnost, rizika, malware, antivirové aplikace, Google Security, sandbox.

Execution of payment transactions with the help of mobile platform Android OS.

Summary

This work is focused on the services of mobile banking (smartbanking) applications, on their use in the Czech Republic and to their other capabilities (functionalities). The author of this work chose the most enlarged mobile platform Android OS, which is studied considering its structure, though also its security risks, which could affect users of mobile banking applications. The analytical part of this work specifically aims to identify areas, which could help extend the users of smartbanking applications. In the first part, the dependences of qualitative traits on the users attitudes of electronic banking are analyzed. The second part is focused on the analysis of users preferences according to single offered functionalities. The literature research and analytical part of the work are listed conclusions, that the eventual absence of the functionalities strongly affect the normalized benefits for user and which particular functions have the maximum effect of them. Based of those detections are listed conclusions, which allow to extend of the number of users of the smartbanking and eliminates eventual security risks, for example by using antivir applications or by proposal of protection against the DoubleDirect attacks.

Keywords: Android OS, smartbanking, banking operations, functionalities of mobile banking application, security, risks, malware, antivirus applications, Google Security, sandbox.

Obsah

1. Úvod

Diplomová práce je zaměřena na oblast neustále se rozvíjejících možností bezhotovostního platebního styku, a to především za pomoci přenosných (mobilních) zařízení. Mobilní zařízení s vlastním operačním systémem, který umožňuje více možností, než jen běžné telefonní funkce, v posledních letech nabývají značného trendu a jejich rozšíření podporuje i relativně nízkonákladová produkce, především tedy v Asijských státech. Tato zařízení zpravidla vychází z požadavků západního trhu a reflektují hardwarové možnosti jejich hlavních konkurentů, kterými jsou nejčastěji leadeři mezi výrobci v dané kategorii, přičemž oblast řídícího software a dalších utilit povětšinou již vychází vlastního vývoje jednotlivých výrobců.

Sledovanou oblastí je aktuálně jednoznačně dominující mobilní platforma Android OS (1) (2), která se pohybuje na poli open-source řešení, což otevírá dobré podmínky pro výrobce, a to nejen z pohledu na licence, ale i vzhledem k možnosti využití vlastních vývojářských řešení. Dále i vzhledem k přenositelnosti aplikací mezi jednotlivými zařízeními a především v rámci snadné distribuce softwarových nástrojů přes oficiální službu společnosti Google.

Finanční instituce nabízí v oblasti bezhotovostního elektronického platebního styku řadu řešení, přičemž za nejrozšířenější lze považovat běžné internetové bankovnictví. Jedná se o velmi nenáročný a mezi uživateli dobře známý způsob pro přístup a správu finančních prostředků. Pro užívání internetového bankovnictví tak uživateli postačí, vyjma nutnosti vyřízení administrativních formalit dané finanční instituce, zpravidla jakýkoliv běžně dostupný webový prohlížeč a přístup k internetu (3). Podstatnějším parametrem se tak stává především skutečnost, jaký způsob autentizace a autorizace platebních operací uživatel zvolí. Tato skutečnost je dále ovlivněna i tím, zdali je uživatelem běžně využívaný webový prohlížeč plně podporovaný konkrétní webovou aplikací, což může způsobit problém ve správném fungování všech bezpečnostních prvků.

Povětšinou se jedná o spojení webové aplikace a mobilního zařízení, na které jsou odesílány autentizační SMS zprávy, nebo případně ověření za pomoci bezpečnostních certifikátů. Avšak v případě mobilního platebního styku, kde řešení typu „W@P Banking“ prostřednictvím „SIM Toolkit“ apod. se stávají již určitým archaismem, se nejeví přístup přes webový prohlížeč příliš vhodným a finanční operace lze snadněji provádět za pomoci tzv. smartbanking aplikací. Jednotlivé softwarové produkty se však liší nabízenými funkcemi, které mohou být pro daného uživatele rozhodující. Využívání těchto aplikací je silně poddimenzované vzhledem k jejich potenciálu, (4) který se odvíjí nejen od možnosti vytvářet rychlé platební příkazy a sledovat pohyby na bankovním účtu v reálném čase, ale i v možnostech sledovat akciové a podílové kurzy, či provádět simulace úvěrů a hypoték. Uživatel tak získává okamžitý přístup k požadovaným informacím bez nutnosti využití osobního počítače či notebooku.

Riziko napadení softwarovými piráty za pomoci útoků typu Vishing, Phishing, Phraming, SMiShing, Keylogger, Distributed DOS, Man In The Middle a obecné bezpečností hrozby přenosných zařízení využívající platformy Android OS jsou obecně hlavní oblasti (5), které uživatele odrazují od jejich využívání. Z pohledu na bezpečné chování na internetu a rizika ztráty finančních prostředků obecně, jsou nejčastěji komunikovány a předávány informace o hrozbách tzv. Phishingu a Pharmingu (6), které jsou velmi úzce spjaty především se snahou útočníků získat přístup k citlivým vstupním údajům uživatele za pomoci podvodných zpráv či přesměrování na útočníkovy fiktivní webové stránky pro přihlášení. Tato rizika však vycházejí především ze způsobu, jak daný uživatel do příslušného rozhraní vstupuje. Samozřejmě je však nutné tuto skutečnost brát z pohledu na přístup uživatele, nikoliv na způsob jeho připojení k internetu.

Pokud se jedná o běžné internetové bankovnictví, které uživatel obsluhuje ze svého webového prohlížeče, vystavuje se odlišným rizikům oproti přístupu přes mobilní aplikaci. Hrozby využívání mobilního zařízení při provádění platebních operací velmi často uživatelé z řad laické veřejnosti směřují především k zařízení samotnému a riziku jeho odcizení. Informace o minimalizaci těchto rizik za pomoci automatického odhlášení vázaného na gravitační senzor či prostého zhasnutí displeje zařízení, totiž nejsou nijak potenciálním uživatelům předány, případně pouze velmi nedostatečnou formou.

Ožehavějším bezpečnostním rizikem, kterým je samotná platforma Android OS, jež zahrnuje jak oficiální distribuce Android OS od společnosti Google, Inc., tak i neoficiální distribuce jednotlivých nízkorozpočtových výrobců, které spadají pod vývojovou větev AOSP (Android Open Source Project). Zde se vyskytují již první znatelné rozdíly, které mohou mít pro uživatele podstatný dopad. Samotná platforma a především její oficiální distribuční kanál s aplikacemi, je považována za relativně bezpečnou, avšak právě i v tomto zdroji se nalézá více než pětinový podíl potenciálně škodlivého kódu, který má neustále rostoucí tendenci. Uživatel je tak v oblasti bezpečnostních rizik značně dezorientovaný, což je další z příčin nízké využívanosti smartbanking aplikací. Vzhledem k výše uvedenému autor práce spatřuje za více než vhodné se na danou problematiku v práci zaměřit.

2. Cíle a metodika

Cíle práce jsou zaměřeny na:

1) Stanovení návrhu na eliminaci bezpečnostních rizik a rezerv nabízených funkcionalit mobilních bankovních aplikací pro rozšíření počtu reálných uživatelů.
2) Stanovení současného pohledu na mobilní bankovnictví a jeho využívání.
3) Analýzu bezpečnostních rizik mobilní platformy Android OS a určení reálných hrozeb pro uživatele mobilní bankovní aplikace.
4) Provedení analýzy závislosti kvalitativních znaků vycházejících z dotazníkového šetření.
5) Provedení vícekriteriální analýzy variant, vycházejících z dotazníkového šetření, pro určení preference uživatelů na dostupné funkcionality ve třech předem zvolených bankovních aplikacích.

Danou oblast autor práce považuje za velmi podhodnocenou a hlavní cíl je tedy stanoven v návrhu konkrétních řešení na eliminaci bezpečnostních rizik a funkcionálních nedostatků, které napomohou rozšířit řady reálných uživatelů smartbanking aplikací.

Pro upřesnění tedy souhrnně dílčí cíle práce vycházejí z několika posloupností, jež jsou v druhém bodě směřovány k získání představy o využívání možnosti provádění platebních operací na chytrém mobilním telefonu a zároveň k získání bližších informací o postoji uživatelů k dané možnosti.

Oblast bezpečnosti platformy Android OS má obecně dva kontroverzní názorové protipóly, které rizika buď nadmíru navyšují, nebo naopak zcela vyvrací. Další dílčí cíl je stanoven v získání závěru o bezpečnostních rizikách, která mohou mobilní zařízení s platformou Android OS postihnout s ohledem na reálná rizika, se kterými se může uživatel mobilní bankovní aplikace setkat.

Poskytované funkcionality daných aplikací jsou však také podstatnou oblastí pro provedení analýzy, jelikož pouze otázka bezpečnosti nemusí být pro uživatele stěžejní, pokud se při jeho rozhodování projeví absence některé z požadovaných funkcionalit. Cíl, stanovený ve vícekriteriální analýze variant, sleduje tři konkrétně zvolené finanční instituce pro zhodnocení dostupných funkcionalit ve srovnání s preferencemi všech uživatelů a vytvořených uživatelských skupin.

K získání bližší představy o bližších podnětech a motivech uživatelů ovlivňující jejich návyky a postoje vůči elektronickému platebnímu styku je stanoven dílčí cíl ve vypracování analýzy závislosti kvalitativních znaků u elektronického platebního styku.

Metodika práce byla zvolena na podkladě provedené literární rešerše, která je hlavním zdrojem teoretických podkladů vytvořených textací, analýz a vyhodnocených cílů v závěru. V rámci rešerše jsou čerpána data z dostupné tuzemské i cizojazyčné literatury, jež zaobaluje sledovanou oblast. Vzhledem k relativně krátké historii mobilních bankovních aplikací a s odkazem na rychlý vývoj právě v této oblasti, jsou využity mnohé webové zdroje, mezi kterými jsou především zohledněny specializované servery. S odkazem na bezpečnost platformy Android OS je především provedena literární rešerše vztahující se k bližšímu pohledu na mobilní platformu Android OS a k určení aktuálních hrozeb. V rámci literární rešerše jsou rovněž zohledněny i výsledky testů renomovaného

bezpečnostního serveru www.av-test.org. U získaných dat je rovněž zohledněn i určitý vývoj v čase, kdy je zahrnut i dlouhodobý vícefázový test mobilních antivirových aplikací.

Po sestavení teoretické struktury práce byla vytvořena datová základna se vstupními údaji pro vytvoření analýz a ověření předpokládaných závěrů. Nezbytná data jsou načerpána z dotazníkového šetření, které je zaměřeno na předem nespecifikovanou skupinu respondentů. Samotný sběr dat vychází z online dotazníku vytvořeného za pomoci bezplatné služby Google Forms, přičemž jeho sestavení vychází z praxe autora DP v oblasti výzkumu trhu s ohledem na požadavky, které jsou kladeny na dotazníková šetření. Konkrétně se jedná o postup dle jednotlivých etap tvorby dotazníku (7), dále s ohledem na požadavky pro výzkumné metody (8) a rovněž s odkazem na požadavky pro dotazník, jakožto průzkumné metody (9).

V dotazníkovém šetření jsou využity především uzavřené otázky, které mají za úkol vytvořit soubor konzistentních dat. V neposlední řadě jsou zde zaneseny otázky pro již konkrétní vyfiltrovanou skupinu uživatelů mobilních zařízení na platformě Android OS, především v pohledu na prevenci bezpečnosti vycházející z jejich aktuálně využívaného softwarové řešení. V poslední části dotazníku všichni respondenti, bez ohledu na platformu či jiná omezení, určují na maximalizační bodové škále své preference vůči jednotlivým nabízeným funkcím, kterými disponují 3 předem zvolené mobilní bankovní aplikace. Mezi dostupné funkce byly zahrnuty i dvě další, které stanovil autor práce, přičemž v rámci analýzy kvantitativních znaků jsou sledovány preference uživatelů vůči nim.

Po vytvoření popisných statistik a souhrnného popisu získaných dat je využito statistických metod k určení závislosti kvalitativních znaků, která je v datech prokazována za pomoci Fisherova a Chí-kvadrát testu. (10) V případě, že se závislost kvalitativních znaků potvrdí, bude určena i její síla za pomoci Cramerova či Phi koeficientu. (11) Předpoklad výskytu závislosti kvalitativních znaků autor práce předpokládá především mezi oblastmi využívání internetového bankovnictví, znalosti pojmu smartbanking, využívání mobilních bankovních aplikací a orientace respondentů v oblasti ICT. Na základě získaných a kriticky ověřených souvislostí je následně možné určit strategii,

zacílení a způsob dalšího vývoje a propagace mobilních bankovních aplikací pro vyšší procentuální využití jejich již aktuálně vysokého potenciálu.

Význam využití vícekriteriální analýzy variant se nalézá v samotných nabízených funkcionalitách dostupných v třech předem zvolených mobilních bankovních aplikacích. Získaná data umožní určit váhu jejich absence vzhledem k požadavkům uživatelů. Cílem je zaujmout uživatele na takové míře, že možnosti bankovní aplikace osloví jeho individuální potřeby a přimějí ho k jejímu využívání. Samotné určení vah a stanovení důležitosti kritérií je provedeno za pomoci vícekriteriální analýzy variant. V rámci postupu byla využita bodovací metoda pro vytvoření matice výskytu nabízených funkcí, jelikož metoda pořadí by zde ztrácela význam pro své zaměření na ordinální informace. Dále byla aplikována bodovací metoda s vahami, jež vychází z preferencí stanovených uživateli. (12) Rovněž byl vypočten normalizovaný přínos pro uživatele, kterým je určeno pořadí významnosti zvolených aplikací.

Pro získání závěrů zpracované problematiky bylo vyjma analytických nástrojů využito i metod kritického vyhodnocení analýz a dedukce. Konkrétně jsou za pomoci dedukce určeny závěry o změně návyků a postojů uživatelů a návrh k poskytnutí garance mobilní bankovní aplikaci. Na základě metody kritického vyhodnocení výsledků analýz poté byly navrženy a sledovány dvě nové funkcionality, které doposud aplikace nenabízí a stanoven návrh řešení pro předávání informací uživatelům.

3. Elektronický platební styk

Z hlediska bližší představy je nutné definovat pojem elektronický platební styk prováděný za pomoci ICT zařízení, v rámci kterého má uživatel možnost provádět aktivní či pasivní finanční operace. Ve slovníku pojmů České národní banky je definováno elektronické bankovnictví následující formulací: *„Dle znění § 15 Zákona o platebním styku (1) Elektronickým platebním prostředkem je prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem.“* (13)

3.1 Legislativní úprava pro elektronický platební styk

- Základ v zákoně 124/2002 sb. a jeho 4. části, ze které vychází hlavní 3. body:

  a) provádění převodu peněžních prostředků,
  b) vydávání a užívání el. platebních prostředků,
  c) vznik a provozování platebních systémů.

- Vše je řízeno dle Směrnice 98/26/EU o neodvolatelnosti zúčtování v platebních systémech a systémech pro obchodování s cennými papíry.
- V pokračování dle Směrnice 2002/65/ES o uvádění finančních služeb na trh na dálku.
- Pro ochranu spotřebitele při uzavírání smluv na dálku a vymezení postupu při zneužití platební karty je Směrnice 97/7/ES.
- Ochrana práv držitele ve vztahu vydavatele a držitele dle doporučení komise ES č. 97/489/ES.
- Vymezení práv a povinností subjektů účastnících se převodu peněžních prostředků se týká zákon o platebním styku dle základní úpravy v zákona č. 124/2002 Sb.
- Vyhláška ČNB 62/2004 sb. provádění platebního styku mezi bankami, zúčtování na účtech s technickými postupy pro opravné zúčtování.
- Tuzemské banky vychází ze zákona č. 21/1992 sb., jenž vytyčuje, že všechny převody mezi finančními subjekty jsou prováděny pomocí Platebního styku.
- Platební styk je ošetřen zákony: § 20c podmínky opravného zúčtování, § 38 bankovní tajemství ve vazbě na platební styk a §41 s následujícími pro pojištění pohledávek. (14) (15)

3.2 Smartbanking

„Je absolutně nejmladší, ale zároveň nejrychleji se rozvíjející formou komunikace s bankou. Smartbanking je založen na využívání vysoké přenosové rychlosti moderních telekomunikačních sítí prostřednictvím tzv. „chytrého“ mobilního telefonu, nebo internetového tabletu s vlastním operačním systémem. Aplikace se buď přímo instaluje do přenosného zařízení, nebo využívá rozsáhlé možnosti optimalizace webové aplikace pro mobilní internetové prohlížeče na těchto přístrojích. Zaměřuje se na dvě nejčastější

platformy tohoto odvětví tj. iOS a Google Android. Ojediněle jsou vyvíjeny i pro platformy Symbian, Windows Mobile a BlackBerry (RIM). V případě optimalizovaných webových stránek pro mobilní prohlížeče není závislá na platformě, ale pouze na podpoře daného mobilního prohlížeče technologie HTML, CSS nebo JavaScript.“ (5)

3.3 Mobilní bankovní aplikace v ČR

V případě mobilních bankovních aplikací finanční instituce v ČR nabízí různorodá řešení. Dané aplikace jsou zpravidla vyvíjené pro platformy iOS od společnosti Apple a dále pro Android OS. Podpora platformy Windows Phone je méně častá, než tomu bylo u předchozích dvou. Vzhledem k stále se rozvíjející oblibě platformy Android OS je zcela logické, že v rámci nabízených aplikací má u každé finanční instituce své zastoupení.

V minulosti bylo možné za pomoci mobilního zařízení provádět platební operace za pomoci zpravidla šifrovaných SMS zpráv SIM Toolkit. Tato technologie umožňovala od roku 1995 prostřednictvím předdefinovaných SMS zpráv komunikovat s finančními institucemi, avšak jako služba se tato technologie v ČR začala využívat až v roce 2001. Tyto služby jsou však již v dnešní době velmi omezené a dalo by se říci, že ne příliš uživatelsky přívětivé. Mobilní bankovnictví přes SIM Toolkit aktuálně stále nabízí například Česká spořitelna a Raiffeisenbank. Vzhledem k rozvoji možností mobilních bankovních aplikací se například UniCredit Bank již v roce 2011 se spuštěním aplikace Smart Banking rozhodla službu GSM banking ukončit. Rovněž ČSOB přistoupilo k podobnému kroku, i když s určitým časovým odstupem, a to konkrétně 21.3.2015. Česká spořitelna prozatím tuto službu poskytuje, avšak plánované datum její ukončení je již přibližně nastaveno v průběhu roku 2016. Raiffeisenbank prozatím pouze uvádí, že danou službu již nebude dále vyvíjet, avšak o jejím úplném pozastavení zatím neuvažuje. Z pohledu na počty klientů využívající GSM Banking se dá hovořit o relativně rozsáhlé základně uživatelů, jelikož například u České spořitelny má službu aktivovanou 60 000 klientů, i když ji aktivně využívá pouze 30 procent z tohoto počtu. U Raiffeisenbank je počet klientů využívající tento způsob komunikace s bankou o něco nižší, a to okolo 3 000, kteří však stále realizují přibližně 6 000 plateb měsíčně. (16)

Tabulka 1 - Mobilní bankovní aplikace v ČR (17) (18)

Banka	Název aplikace	iOS	Android	Windows Phone
Air Bank	Mobilní bankovnictví Air Bank	Ano	Ano	2015
Citi	Citi Cz	Ano	Ano	ve výhledu
ČSOB	ČSOB smartbanking	Ano	Ano	Ano
Česká spořitelna	Servis 24 Mobilní banka	Ano	Ano	Ano
Era	Era smartbanking	Ano	Ano	Ano
Equa Bank	Equa bank mobilní bankovnictví	Ano	Ano	ve výhledu
GE Money Bank	GE Money CZ	Ano	Ano	ve výhledu
Komerční banka	Mobilní banka 2	Ano	Ano	Ano
mBank	mBank 2.0	Ano	Ano	2015
Sberbank	Sberbank Smartbanking	Ano	Ano	2015
Raiffeisenbank	Mobilní eKonto	Ano	Ano	2015
UniCredit Bank	Smart Banking	Ano	Ano	Ano
ZUNO BANK	Zuno Mobile Banking	Ano	Ano	Ano
Fio	Fio Smartbanking	Ano	Ano	Ano
ING Bank	ING Bank CZ	Ano	Ano	ne
Waldviertler Sparkasse Bank	WSPK Smartbanking	Ano	Ano	Ano

I z těchto důvodů je rovněž vhodné zaměřit se na problematiku mobilních bankovních aplikací, jelikož klienti daných finančních institucí v brzké době nebudou mít jinou možnost, jak spravovat své finanční prostředky za pomoci mobilního zařízení jinak, než prostřednictví výše uvedených aplikací, či optimalizovaných webových stránek pro mobilní telefony, což ve srovnání s nativní bankovní aplikací rovněž není zcela optimální řešení.

Vyjma výše uvedených plnohodnotných bankovních aplikací dále nabízí Česká spořitelna rozšiřující aplikaci MŮJ STAV, která slouží k pasivnímu zobrazení zůstatků na účtech, či jiné informace o využívaných produktech. Zajímavostí je skutečnost, že pro mobilní platformu Android OS je podporována od verze 4.0, na rozdíl od plnohodnotné bankovní aplikace Servis 24, která je podporována pro zařízení Android OS verze 2.3 a vyšší.

3.4 Uživatelská základna bankovních aplikací

Oblast mobilního bankovnictví je velmi často rozebírána z hlediska přidávaných funkcionalit a případně v pohledu na bezpečnost. Určitý vývoj je patrný i v uživatelských návycích a celkově v přístupu klientů finančních institucí k inovacím, které s novými technologiemi přicházejí. Jednou z těchto inovací jsou i bankovní aplikace, které s rostoucím počtem uživatelů chytrých telefonů, a s tím velmi úzce spjatým nárůstem uživatelů mobilního internetu, s sebou nesou mnoho přínosů pro jejich uživatele.

Rovněž by se dalo hovořit o určité změně návyků uživatelů a jejich postojů ke správě finančních prostředků. Dle vyjádření Tomáše Kofroně, mluvčího Raiffeisenbank, se zvyšuje zájem o aktuálnější přehled o zůstatcích na účtech, jelikož v případě běžného internetového bankovnictví se průměrný uživatel přihlásil přibližně osmkrát měsíčně, zatímco v případě bankovní aplikace se uživatel průměrně přihlásil dvaadvacetkrát. Tento trend potvrzuje i Vladimír Komjati z Air Bank, který uvádí, že: *„Kouzlo mobilních aplikací spočívá v tom, že máte o svých penězích dokonalý přehled, ať jste kdekoliv. Stačí sáhnout do kapsy,“*. Vladimír Michna, mluvčí Zuno Bank, dále uvádí: *„Zároveň se také ukazuje, že chytré telefony a mobilní aplikace bank ovlivňují nákupní chování lidí a vedou k úsporám,“* (17) Vladmír Michna ze Zuno Bank rovněž uvedl, že dle jejich statistik se *„Téměř sedmdesát procent zákazníků se před nákupem „poradí“ se svou aplikací pro mobilní bankovnictví,“*. (19) Tento trend se rovněž projevil v globálním měřítku, kde v rámci mezinárodního průzkumu ING bank 85 % z dotázaných Evropanů využívající mobilní bankovní aplikaci uvedlo, že aplikace přispívá k lepšímu hospodaření s finančními prostředky, jelikož o nich mají podstatně lepší přehled. (4)

Obecně se lze setkat s informacemi o rostoucím počtu uživatelů, jenž se meziročně pohybovalo mezi padesáti až sto procenty. Tato informace byla komunikována v říjnu roku 2015 s tím, že se tento prudký nárůst opět značně zpomalí. Z ankety E15.cz vyplynulo, že aplikaci mobilního bankovnictví měsíčně využije alespoň jednou 1,13 milionu klientů, nicméně dále již nebylo rozváděno, zdali tomu je za účelem aktivní operace, například zadání platebního příkazu, nebo se jedná pouze o pasivní operace, kterou je například zjištění zůstatku na běžném účtu. (19)

Tabulka 2 - Počty uživatelů mobilních bankovních aplikací 2015 (19)

Počty uživatelů mobilního bankovnictví 2015	
Banka	**Počet klientů s mobilní aplikací (v tisících)**
Raiffeisenbank	80
ČSOB	140
Zuno	100
Česká spořitelna	243
Komerční banka	145
Air Bank	115
UniCredit Bank	85
mBank	133
Equa Bank	25
Fio banka	60

Z výše uvedeného vyplývá, že zájem o bankovní aplikace a počty jejich uživatelů rostou. Suma v tomto případě však udává pouze počty uživatelů, kteří se do aplikace alespoň jednou měsíčně přihlásili. Samotné využití aplikací je patrnější z objemu provedený platebních operací, kdy například přes aplikaci Servis 24 od České spořitelny je měsíčně proveden obrat přes půl miliardy korun rozložený v 200 000 platebních transakcích. Přes konkurenční aplikaci Mobilní bankovnictví Air Bank je objem plateb obdobný, okolo 600 000 000 korun, realizovaný přes přibližně 120 000 transakcí. V Komerční bance je situace podobná, jelikož přes aplikaci Mobilní banka 2 je v přibližném počtu měsíčně realizováno okolo 120 000 transakcí. (17) Nicméně z výše zmíněného mezinárodního průzkumu ING Bank vyplynulo, že v globálním pohledu patří ČR k zemím s nejnižším počtem uživatelů, což i přes rostoucí trend přispívá k tvrzení autora, že v ČR je jejich potenciál stále podhodnocený a uživateli ne zcela využitý. Jejich využití je především spojeno s věkem uživatelů, jelikož zcela logicky zde vyplynulo, že mezi nejčastější uživatele patří mladší generace, nebo skupiny uživatelů, které se o nové technologické možnosti aktivně zajímají. (4)

3.5 Použitelnost bankovních aplikací

Mobilní aplikace v rámci rychlého vývoje nabízí různé možnosti doplňujících funkcí, které by měli uživateli mobilního telefonu nabídnout veškeré potřebné informace. Nabízené funkce však nejsou jediným kritériem pro zhodnocení, zdali daná aplikace je pro uživatele přínosná a dále je nutné zohlednit její strukturu, což má vliv na uživatelskou přívětivost, tj. jestli je tzv. „user friendly“.

3.5.1 Rozdělení funkcionalit v aplikaci vzhledem k přihlášení

Aplikace pro obsluhu běžného účtu již dávno neplní funkci pouhého zadání platby či zobrazení aktuálního zůstatku, ale obsahují další rozšiřující funkce. Mezi těmito funkcemi se nalézá například i možnost dohledání nejbližšího bankomatu, či pobočky, případně zobrazení kontaktních informací. Z tohoto důvodu jsou aplikace rozděleny do dvou částí, kdy libovolný uživatel, který ani nemusí být klientem dané banky, má možnost využívat funkcí, jež nevyžadují přihlášení ke konkrétnímu klientskému číslu. Je celkem i logické, že pro sledování kurzovních lístků, či dohledání informací o nabízených produktech banky jsou veřejné informace, které nevyžadují zabezpečený přenos dat. Funkcionality lze tedy rozdělit na veřejnou a uzavřenou část, která již vyžaduje přihlášení.

1) Veřejná část obecně nabízí tyto funkce a informace:

   - *seznam nebo mapa poboček, navigace k nejbližší pobočce*
   - *seznam nebo mapa bankomatů, navigace k nejbližšímu bankomatu (např. Equa bank ukazuje bankomaty všech bank - výběry z bankomatů ostatních bank jsou u ní totiž zdarma)*
   - *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, apod.)*
   - *veřejné zprávy od banky* (18)

2) Uzavřená část, která již vyžaduje přihlášení, zpravidla nabízí tyto možnosti:

   - *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, apod.)*
   - *informace o platebních kartách, někdy i s možností zneaktivnění, změny PINu 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* (18)

Výše uvedený výčet však není zcela podmíněný, jelikož například aplikace mBank 2.0 například nabízí možnost zobrazení zůstatku běžného účtu či limitu kreditní karty ještě před přihlášením uživatele (20), což v případě rizika zobrazení zůstatku nepovolané osobě dle názoru autora není příliš bezpečné.

3.5.2 Komunikace zařízení se servery banky

Komunikace mezi bankovní aplikací a serverem banky je v oficiálních zdrojích komunikována pouze jakožto šifrovaná, nicméně dle dokumentace všeobecných podmínek ING Belgium je pro bezpečnost síťové komunikace využit protokol SSL v3. (21) Stejný protokol TLS/SSL je obecně využíván pro služby internetového bankovnictví v ČR. Vzhledem k tomu, že se finanční instituce odkazují na stejnou úroveň zabezpečení mobilních bankovních aplikací jako u internetového bankovnictví, tak je možné logicky identifikovat, že se jedná o TLS/SSL protokol.

3.5.3 Aktivace a ztráta zařízení

Aktivace mobilní bankovní aplikace je zpravidla prováděna přes internetové bankovnictví, kde uživatel nalezne sekci k aktivaci této služby. V této části je vygenerováno jedinečný aktivační kód. Zde se již aplikace liší, jelikož například uživatel České spořitelny dále volí heslo pro bankovní aplikaci, které na rozdíl uživatelé Air Bank zadávají až přímo v aplikaci. Nicméně aplikace je přímo vázána na IMEI daného zařízení. Rychlou deaktivaci při ztrátě zařízení může uživatel provést za pomoci zákaznické linky, nebo přímo v rámci internetového bankovnictví, kde službu aktivoval.

3.6 Nové technologické trendy pro autentizaci

Mezi relativně mladé trendy v oblasti mobilních technologií je možné zařadit i nové způsoby provádění autentizace klientů. V současnosti byly pro ověření klientů prováděny autentizace na základě ověření znalosti, což se zpravidla vztahovalo k určitému PIN kódu, či ověření na základě vlastnictví, které zpravidla v případě běžného internetového bankovnictví zastřešil bezpečnostní certifikát, jenž mohl být uložen například na USB tokenu. Na základě nově implementovaných peripetií mobilních zařízení tak přichází do reálného prostředí nově i metody biometrické autentifikace, kdy například UniCredit bank již ve svých bankovních aplikacích využívá vestavěné čtečky otisků prstů mobilních zařízení iPhone společnosti Apple, ale v rámci řešené problematiky i podstatnější mobilní zařízení od společnosti Samsung s Android OS. (22 str. 17)

Tento způsob ověření zpravidla snímá a ukládá pořízený otisk přímo do zařízení, takže bance nejsou odesílána žádná data a vše je řešeno přímo v rámci daného zařízení. V roce 2009 tento způsob ověření označovaný jakožto „chytrá revoluce“ globálně využívalo přibližně 7 miliard uživatelů, přičemž v roce 2014 to již bylo miliard 16, což rovněž přispívá k celkovému postoji, že tento způsob ověření se stává podstatně bezpečnějším, než ověření za pomoci znalosti či vlastnictví. Níže je uvedena tabulka se srovnáním autentifikace za pomoci čtečky otisku prstů. (23)

Tabulka 3 - Srovnání biometrické autentifikace čtečkou otisků prstů (23)

	VEGA LTE-A	iPhoine 5S	Galaxy S5
Sensor Position	Back side button	Home button	Home button
Authentication methods	Up⟶down rubbing	Touch in all direction	Up⟶Down rubbing
	Registration of two fingerprint	Registration of five fingerprint	Registration of three fingerprint
Mobile checking	unsupported	AppStore, iBooks	Paypal
Fingerprint sensor	Crucialtec	Apple (Authentic takeover, 2012)	Synaptics

4. Android OS

Android OS nese označení mobilní operační systém, který byl vyvinut společností Google, Inc. Tento operační systém našel využití v mnoha zařízeních, počínaje chytrými telefony až po tablety, nicméně existují i modifikované PC verze, avšak ty jsou víceméně určené spíše pro nadšence a vývojáře, než pro běžného uživatele. Běžně dostupná zařízení disponující tímto operačním systémem však nevychází pouze z produkce společnosti Google, která by byla ve strategické alianci s nějakým konkrétním výrobcem, což jsou konkrétně aktuálně především zařízení od výrobce Nexus (popř. HTC), ale i dalších producentů mobilních technologií, kteří nejsou v přímém spojení se společností Google, jakožto společnosti Samsung, Lenovo, Sony, Motorola apod. Tato zařízení zpravidla vychází z modifikované verze AOSP (Android Open Source Project).

4.1 Historický vývoj platformy

Historický milník platformy sahá až do roku 2007, kdy byla v listopadu vydána první Alpha verze operačního systému. Rovněž byla v tomto období 5. Listopadu 2007 vydána první Beta verze a 12. listopadu tohoto roku byl vydán i první SDK (Software Developer Kit). Samotný vznik společnosti Android, Inc. a vývoj tohoto operačního systému je datován až do roku 2003, přičemž nejvyšší historický vliv zde měla v roce 2005 společnost Google, Inc., která společnost Android, Inc. v daném roce zakoupila. První oficiálně vydaná verze byla Android 0.9, jež prozatím nenesla žádné později již typické kódové označení, pod kterými jsou jednotlivé verze tohoto operačního systému známé dnes. (24) Historicky první zařízení na této platformě bylo od společnosti HTC, která jej ve strategické alianci s mobilním operátorem T-mobile distribuovala pod označením HTC G1 a verzí systému Android 1.0 Apple pie. (25)

Následující verze Android OS s sebou přinášely inovace, které se projevovaly nejen v nových uživatelských funkcích, ale i v přidaných možnostech pro vývojáře a narůstajícím počtu využitelných API (Application Programming Interface), pro efektivnější spojování jednotlivých částí zdrojového kódu. Chronologický vývoj jednotlivých verzí, včetně nárůstu použitých API je uveden v tabulce 4 (viz níže).

Tabulka 4 – Verze Android OS (24)

Verze	Název verze	Datum vydání	API		Verze	Název verze	Datum vydání	API
Android 0.9		2008 Aug 22			Android 3.2.4	Honeycomb	2011 Dec 15	13
Android 1.0	Apple pie	2008 Sep 23	1		Android 4.0.3	Ice Cream Sandwich	2011 Dec 16	15
Android 1.1	Banana bread	2009 Feb 9	2		Android 3.2.6	Honeycomb	2012 Feb 15	13
Android 1.5	Cupcake	2009 Apr 30	3		Android 4.0.4	Ice Cream Sandwich	2012 Mar 28	15
Android 1.6	Donut	2009 Sep 15	4		Android 4.1	Jelly Bean	2012 Jul 9	16
Android 2.0	Eclair	2009 Oct 26	5		Android 4.1.1	Jelly Bean	2012 Jul 23	16
Android 2.0.1	Eclair	2009 Dec 3	6		Android 4.1.2	Jelly Bean	2012 Oct 9	16
Android 2.1	Eclair	2010 Jan 12	7		Android 4.2	Jelly Bean	2012 Nov 13	17
Android 2.2	Froyo	2010 May 20	8		Android 4.2.1	Jelly Bean	2012 Nov 27	17
Android 2.3	Gingerbread	2010 Dec 6	9		Android 4.2.2	Jelly Bean	2013 Feb 11	17
Android 2.3.3	Gingerbread	2011 Feb 9	10		Android 4.3	Jelly Bean	2013 Jul 24	18
Android 3.0	Honeycomb	2011 Feb 22	11		Android 4.4	KitKat	2013 Oct 31	19
Android 2.3.4	Gingerbread	2011 May 10	10		Android 4.4.1	KitKat	2013 Dec 5	19
Android 3.1	Honeycomb	2011 May 10	12		Android 4.4.2	KitKat	2013 Dec 9	19
Android 3.2	Honeycomb	2011 Jul 15	13		Android 4.4.3	KitKat	2014 Apr 14	19
Android 2.3.5	Gingerbread	2011 Jul 25	10		Android 4.4.4	KitKat	2014 Jun 23	19
Android 2.3.6	Gingerbread	2011 Sep 2	10		Android 5.0	Lollipop	2014 Oct 17	21
Android 3.2.1	Honeycomb	2011 Sep 20	13		Android 5.0.1	Lollipop	2014 Dec 2	21
Android 2.3.7	Gingerbread	2011 Sep 21	10		Android 5.0.2	Lollipop	2014 Dec 19	21
Android 3.2.2	Honeycomb	2011 Sep 30	13		Android 5.1	Lollipop	2015 Mar 9	22
Android 4.0	Ice Cream Sandwich	2011 Oct 18	14		Android 5.1.1	Lollipop	2015 Apr 21	22
Android 4.0.1	Ice Cream Sandwich	2011 Oct 19	14		Android 6	Marshmallow	2015 Oct 5	23
Android 4.0.2	Ice Cream Sandwich	2011 Nov 28	14					

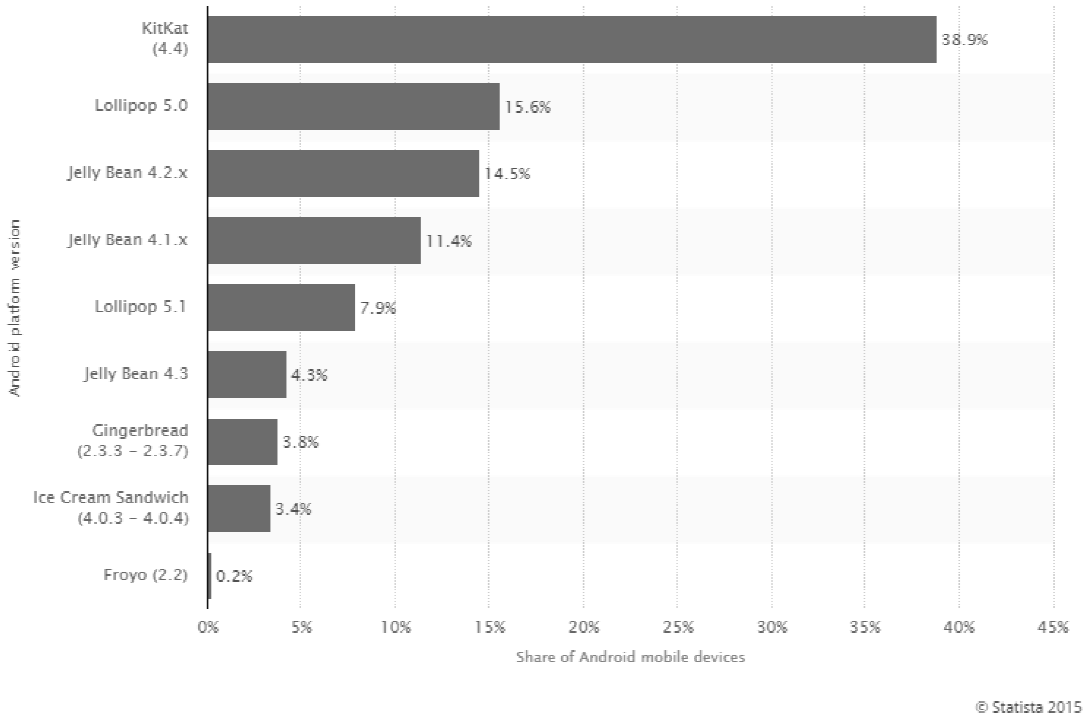
Z tabulky 4 je rovněž patrné, že se jedná o velmi intenzivní vývoj, v rámci kterého jsou přibližně v několikaměsíčních intervalech vydávány nové verze tohoto operačního systému. Tento progres je však patrný především od vydání verze Android 2.3, která je zároveň limitující pro využívání aplikací mobilního bankovnictví. (26) (27) (28)

4.2 Rozdělení aktuálních verzí platformy

Rovněž je vhodné uvést aktuální rozložení verzí tohoto mobilního operačního systému, které vychází z dat o návštěvnosti online úložiště aplikací Obchod Google Play v rozmezí sedmidenního období, jež končilo dne 5. října 2015. V uvedeném výčtu jsou pouze verze Android 2.2 a vyšší, které podporují aktuální aplikace dostupné na Obchod Play. (2) Tato skutečnost je velmi podstatná, jelikož smartbanking aplikace jsou zpravidla

podporovány pro verzi Android 2.3 a vyšší (26) (27) (28), nicméně například aplikace Smart Banking od UniCredit Bank je podporována již pro verzi Android 2.2, avšak s požadavky na minimální rozlišení displeje 480x800 px, což také nebývá zcela běžné. (29)

Z obrázku 1 je zcela patrné, že požadavky na nejnižší verzi Android OS se vztahují na valnou většinu uživatelů, i když daný graf vyobrazuje globální pohled na rozložení verzí platformy, nikoliv pouze pro ČR, tak lze obecně uvést, že pro rozšíření počtu uživatelů mobilního bankovnictví není verze jejich Android OS podstatnou překážkou.



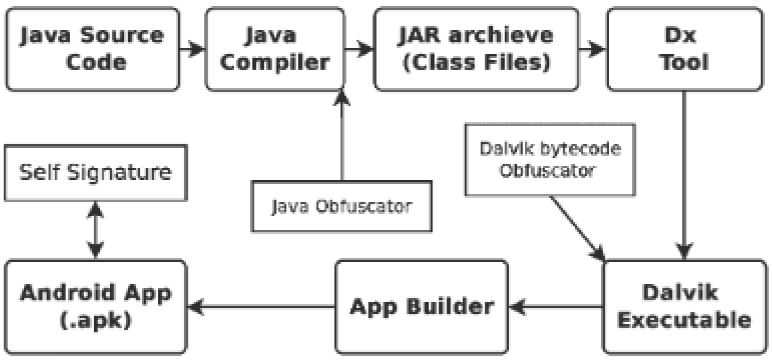
Obrázek 1 – Aktuální rozložení verzí Android OS (2)

4.3 Zdrojový kód a aplikace

Samotný operační systém je založen na otevřeném linuxovém jádru (kernelu). Ve srovnání s další nejrozšířenější platformou, kterou je iOS vyvinutý společností Apple, je Android OS open source řešení, což umožňuje vývojářům jej individuálně upravovat pro jednotlivá zařízení. Z tohoto důvodu mohou mít rozličná zařízení využívající Android OS rozdílná grafická uživatelská rozhraní (GUI), i když se jedná o shodnou platformu.

U zařízení s platformou Android OS je typické, že obsahují určité již nativně vestavěné aplikace a dále podporují aplikace třetích stran. Vývojáři tak mohou produkovat aplikace za pomoci tzv. Android SDK (Software Developer Kit). (30) V rámci platformy Android OS je nástroj SDK podporován pro všechny platformy PC tj. Windows, Mac OS i Linux, přičemž jeho licence je freeware. (31) Aplikace jsou zpravidla vytvářené v programovacím jazyku Java a jsou spouštěny přes virtuální vrstvu „Dalvik“ od společnosti Google (viz obrázek 2 a obrázek 3), která je optimalizuje pro mobilní zařízení. (32) Hlavním zdrojem aplikací pro uživatele je online úložiště Obchod Google Play, nicméně po zrušení defaultně nastaveného bezpečnostního prvku zvaného „neznámé zdroje“ se otevírá možnost instalovat i aplikace, které z Obchod Google Play nepochází (viz obrázek 11). Nicméně tato možnost může kolidovat s bezpečností daného uživatele, jelikož dává k dispozici systémové prostředky aplikaci, která pochází z neověřeného zdroje (viz Google Android Security).

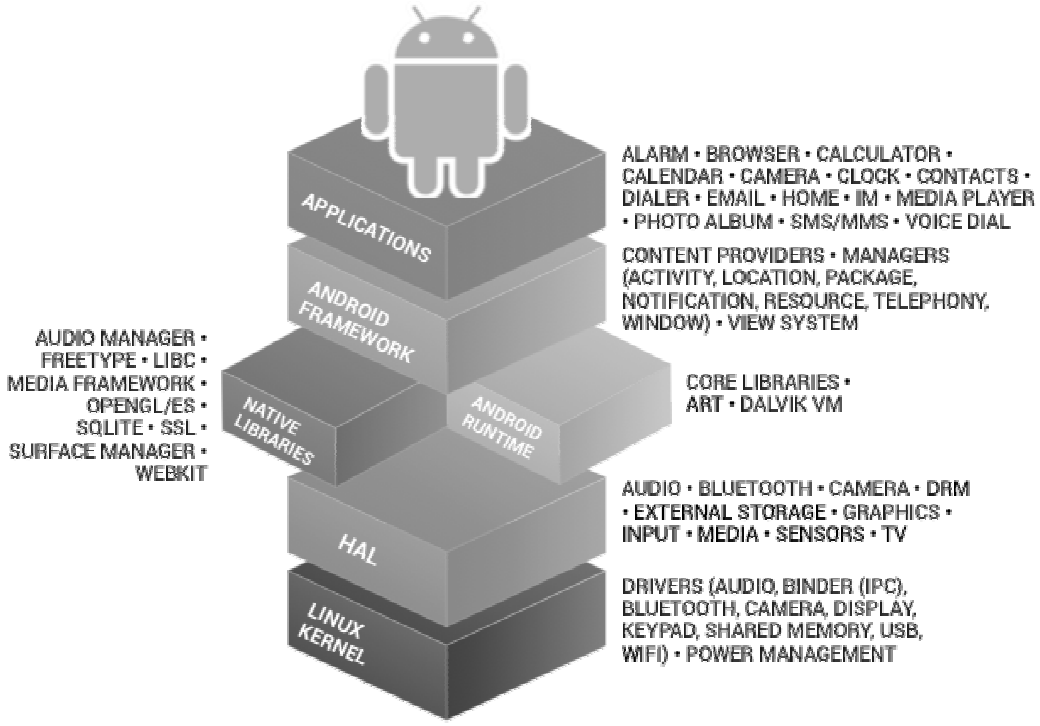
Při vývoji aplikací pro platformu Android OS je zdrojový kód v jazyce Java kompilován do bytecode pro Java Virtual Machine. Zde vytváří řadu „.class“ souborů z přechodného Java-bytecode, které vychází z tříd definovaných ve zdroji. Za pomoci Dx nástroje jsou poté přeloženy sloučeny do jednotného Dalvik spustitelného souboru „.dex“ (Dalvik EXecutable) či „.odex“ (Optimalize Dalvik EXecutable). Dalvik Executable je určen především pro systémy, které mají určitá paměťová nebo výkonností omezení kapacity. (33)



Obrázek 2 - Proces tvorby aplikace pro Android OS (33)

4.4 Vrstvy Android OS

Samotný systém je složen z několika vrstev, které jsou uvedeny na obrázku 3. Vrstva linuxového jádra je na nejnižší hierarchické úrovni mezi hardware a software daného zařízení, jelikož obsahuje ovladače jednotlivých peripetií, kterými je tato vrstva řídí. S výjimkou malého množství zdrojového kódu Andorid OS, který je spouštěn v „root“, je veškerý kód nad linuxovým jádrem omezen Sandboxem, tj. v aplikační karanténě. (34)



Obrázek 3 – Vrstvy Android OS (35)

4.4.1 Vrstva HW zařízení

Android OS běží na široké škále hardwarových konfigurací zahrnující chytré telefony, tablety a set-top-boxy. Android OS je nezávislý na procesoru daného zařízení, avšak dokáže využívat specifických bezpečnostních hardwarových vlastností, jako je například ARM v6 eXecute-Never. (34) Tato konkrétní vlastnost je podporována v rámci procesorové jednotky MPU (Memory Protection Unit), která dokáže definovat paměťové regiony, jichž může být až osm. U těchto regionů lze poté nastavovat rozdílná práva, mezi která patří i XN, tj. eXecute-Never, jež zakazuje spouštění kódu z daného regionu. (36)

4.4.2 Android Operační Systém

Jádro operačního systému je postaveno na vrcholu Linux kernel. Všechny zdroje daného zařízení, jakožto například funkce fotoaparátu, GPS data, funkce Bluetooth, telefonní funkce, sítová připojení apod. jsou zpřístupňována pouze prostřednictvím operačního systému.

4.4.3 Runtime aplikací Android

Aplikace pro Android jsou nejčastěji napsané v programovacím jazyce Java a dále spouštěny ve virtuálním stroji Dalvik. Nicméně mnoho aplikací, včetně implementovaných služeb a aplikací Android, jsou již nativní aplikace nebo obsahují nativní knihovny. Oba způsoby, tj. virtuální vrstva Dalvik i běh nativních aplikací, jsou podmíněny stejnému bezpečnostnímu prostředí uvnitř aplikačního Sandboxu. Aplikace získávají vyhrazené části souborového systému, ve kterém mohou zapisovat privátní data, včetně databází a souborů typu raw. (34)

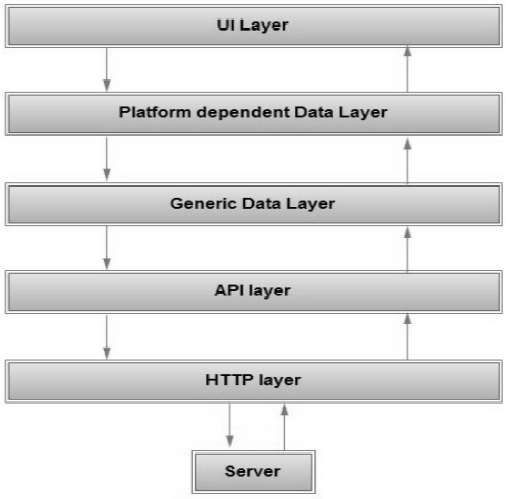
Android OS obsahuje sadu základních knihoven, které poskytují většinu funkcionalit z dostupných Java API (Application Programming Interfaces). Nicméně dostupné API jsou nižší verzí toho, co by se dalo očekávat v J2SE. I když zde například není podpora pro Swing nebo AWT, tak jádra knihovny v sobě zahrnují knihovny specifické pro Android (například SQLite, OpenGL). Vzhledem k tomu by použití J2SE mělo za následek režii ve vnitřním prostředí a použití J2ME se váže na licenci a další důsledky na bezpečnost. Použití J2ME by znamenalo hrazení licenčních poplatků společnosti Oracle za každé zařízení. Dále z bezpečnostních důvodů každá aplikace v rámci Android OS běží ve vlastním VM, přičemž po implementaci J2ME by všechny aplikace běžely uvnitř jednoho VM a tím se snížila účinnost bezpečnostní karantény Sandbox. (30)

Tabulka 5 - Nativní knihovny Android OS (30)

Library	Description
Media Libraries	Enables playback and recording of audio and video formats. Based on OpenCore from PacketVideo
SQLite	Provides relational databases that can be used by applications and systems
SSL	Provides support for typical cryptographic functions
Bionic	System C library
WebKit	Browser-rendering engine used by Android browsers
Surface Manager	Provides support for the display system
SGL	Graphics engine used by Android for 2D

4.4.4 Aplikace založené na webových službách

V případě aplikací komunikujících se servery je využíván vývojový model vrstveného přístupu. Nejnižší úrovní je zde vrstva HTTP, která zodpovídá za odesílání požadavků serveru metodami GET a POST a obdržení odpovědi od serveru. Druhou vrstvou je zde API, která analyzuje odpověď serveru a formuje další požadavky, jenž opět předává zpět do vrstvy HTTP. Vrstva API poté dostane řetězec odpovědi z vrstvy HTTP, který analyzuje. Následně vrstva API extrahuje nezbytná pole, která předává do datové vrstvy. Obecná datová vrstva obsahuje komponenty, které zastřešují jak projekční činnost vrstev, tak i implementované funkce typu mezipaměti, řízení výjimek, přihlašování a ověřování. Následuje datová vrstva závislá na platformě, která přebírá a využívá data z API vrstvy, jež jsou následně ukládána dle požadavků platformy. Poslední vrstvou je uživatelská vrstva UI, která již zobrazuje data uživateli a zastřešuje interakci s ním. Obsahuje dvě složky, a to uživatelské rozhraní a procesní uživatelské komponenty. Komponenty uživatelského rozhraní umožňují interakci mezi uživatelem a aplikací. Procesní uživatelské komponenty synchronizují a organizují interakci s uživatelem. Nejvyšší UI vrstva je zodpovědná za zobrazování v systému, což mohou být různé náhledy, tlačítka apod. (37)



Obrázek 4 - Vrstvená architektura (37)

4.5 Sandbox

Sandbox je bezpečnostní mechanismus sloužící ke spuštění nedůvěryhodného kódu v prostředí, které bylo navrženo a je velmi široce používané, jakožto nástroj izolující potenciálně škodlivý kód od ostatních komponent. Obecně Sandbox umožňuje pouze omezený přístup procesů k systémovým zdrojům na základě určitých práv, které mohou být pro přístup k paměti zařízení, přístupu na určité servery, porty apod. V praxi Sandbox vychází z práv, které uživatel dané aplikaci při instalaci povolí a ta nemá možnost využívat jiné systémové prostředky.

```
<permission name="android.permission.INTERNET" >
    <group gid="inet" />
</permission>
```

Obrázek 5 - Zobrazení aplikace s oprávněními pro přístup k internetu (30)

Od vydání první verze Android OS v roce 2008 se vývojáři zaměřili na návrh různých frameworků, mezi kterými byly i analytické nástroje pro report funkčnosti aplikace, nebo provedení klasifikace, zda je aplikace benigní nebo škodlivá. Statické analytické techniky jsou zpravidla zaměřeny na balíček aplikace (APK) a Dalvik bytecode. Dynamické analytické techniky sledují chování aplikace v kontrolovaném prostředí.

Výsledky statické analýzy mohou také posílit výsledky dynamické analýzy, například účinnou stimulací cílené aplikace a spouštěním rozšiřujícího prostředí, což vede k vytvoření hybridního analytického přístupu. (38)

Framework	Implementation Details		Analysis Type			Analyzed Features			
	Android Version	Inspection Level	Static	Tainting	GUI Interactions	File	Network	Phone	Native Code
AASandbox	–	Kernel	•		•	•	•	•	
AppIntent	2.3	Kernel	•	•	•				
ANANAS	2.3-4.2	Kernel	•		•	•	•	•	•
Andrubis	2.3.4	QEMU & Dalvik	•	•	•	•	•	•	•
AppsPlayground	–	Kernel	•	•	•				
CopperDroid	2.2.3	QEMU	•		•	•	•	•	•
DroidBox	2.3-4.1	Kernel		•		•	•	•	
DroidScope	2.3	Kernel & Dalvik		•		•	•	•	•
ForeSafe	?	?	•		•	•	•		
Joe Sandbox Mobile	4.0.3 / 4.0.4	Static Instrumentation	•		•	•	•	•	
Mobile Sandbox	2.3.4	Dalvik	•	•	•		•	•	•
SandDroid	?	?	•	•	?	•	•	?	?
SmartDroid	2.3.3	Kernel	•	•	•	•	•	•	
TraceDroid	2.3.4	Dalvik	•		•	•	•	•	
vetDroid	2.3	Kernel & Dalvik	•	•	•	•	•	•	
VisualThreat	?	?	•			•	•	•	•

Obrázek 6 - Srovnání analytických Sandboxů pro Android malware (38)

5. Bezpečnost platformy Android OS

S rostoucí popularitou OpenSource platformy Android OS jsou na veřejnosti stále více komunikována rizika spojená s jejím využíváním a otevírají se diskuse o její nebezpečnosti. Mnozí uživatelé však oproti svému běžnému PC značně podceňují hrozby spojené právě s tímto operačním systémem. Mezi uživateli tak koluje mýtus o absolutní bezpečnosti při používání těchto zařízení, což při ignoraci potřeby využití kvalitní antivirové aplikace může přinést nedozírné následky. Naopak z odborných zdrojů jsou častěji komunikovány informace o nárůstu hrozeb dané platformy, oproti ostatním mobilním platformám.

5.1 Bližší pohled na obecnou bezpečnost platformy Android OS

O určitém šarlatánství z pohledu na mobilní antivirové aplikace, se kterým autor práce ani v rámci dobové situace nesouhlasí, v minulosti polemizoval i programový manažer

open-source softwaru u společnosti Google Chris DiBona, který konkrétně uvedl, že: *„Společnosti využívají váš strach, aby se pokusily prodat ochranný software pro Android, RIM a iOS. Jsou to šarlatáni a podvodníci. Pracujete-li pro antivirové společnosti prodávající ochranu pro Android, RIM či IOS, měli byste se za to stydět.“* (39) V rámci tohoto vyjádření DiBona dále uvedl, zatím nenarazil na žádný závažný problém mobilního telefonu, který by způsobil virus podobně jako ve Windows nebo Mac. (40)

Nicméně tato informace byla komunikována v roce 2011, což však bylo v době, kdy společnost Google nijak oficiálně nepřipustila možnost škodlivého kódu přímo v aplikacích dostupných na Obchod Play (viz kapitola Google Android Security). V daném roce byl rovněž podchycen první masově šířený škodlivý kód prostřednictvím oficiálního zdroje Obchodu Play (respektive v té době Android marketu). Jednalo se o nákazu typu DroidDream, která vyhlíží jakožto legitimní aplikace, avšak tento malware dovedl v daném zařízení například změnit způsob připojení, nastavit používaný řídící server botnetu, samovolně začít stahovat další aplikace či vyzývat přes notifikační lištu například ke stažení dalších aplikací nebo stažení autorizovaného instalačního APK souboru. (41) Rovněž dovedl podobně, jakožto tomu je u bezpečnostní hrozby phishingu, vyzývat k návštěvě určité škodlivé URL adresy.

Nicméně dané tvrzení bylo velmi rychle konfrontováno s reakcí renomované antivirové společnosti Kaspersky Lab, jež konkrétně uvedla: *„Na rozdíl od iOS a RIM roste androidí malware rychlým tempem. Vzhledem k tomu, že je Android velmi úspěšný, není překvapením to, že k němu tíhnou kybernetičtí zločinci. Tento exponenciální růst malwaru pro Android je velmi podobný růstu malwaru pro Windows. I když anti-malwarové produkty pro Android ještě nejsou nutností jako na PC, uživatelé by měli vážně uvažovat o jejich použití, pokud se obávají o informace, které mají uložené ve svých zařízeních a o bezpečnost finančních transakcí, které provádějí.*

Je také třeba poznamenat, že „viry“ pro Android sice dnes neexistují, trojské koně ale ano. Jen samotný DroidDream napadl více než 100 000 uživatelů. Otevřenost Android Marketu a platformy výrazně pomohly společnosti Google k dosažení takového rychlého a obrovského nárůstu, který dnes ale také znamená, že se Android stal preferovanou platformou mezi kybernetickými zločinci.“ (39) (40) Toto se posléze potvrdilo o několik let později (viz kapitola Google Android Security) a z čehož rovněž vyplývá, že v případě

využívání mobilního zařízení pro přístup a správu finančních prostředků, se antivirová aplikace stává nedílnou součástí pro zachování bezpečnostní integrity systému.

V rámci této problematiky došlo i k uveřejnění postoje ČNB, která riziko napadení mobilního zařízení zahrnula do vydaného upozornění na rizika spojená s využíváním elektronického bankovnictví, a to konkrétně v bodě „c“, čímž v rámci prevence kyberkriminality připouští jakožto hlavní finanční ústav ČR možná rizika:

„K obsluze bankovního účtu jsou v současné době využívány nejen počítače, ale také tablety a mobilní telefony tzv. SmartPhony (dále jen "zařízení").

Doporučujeme proto věnovat pozornost následujícím skutečnostem:

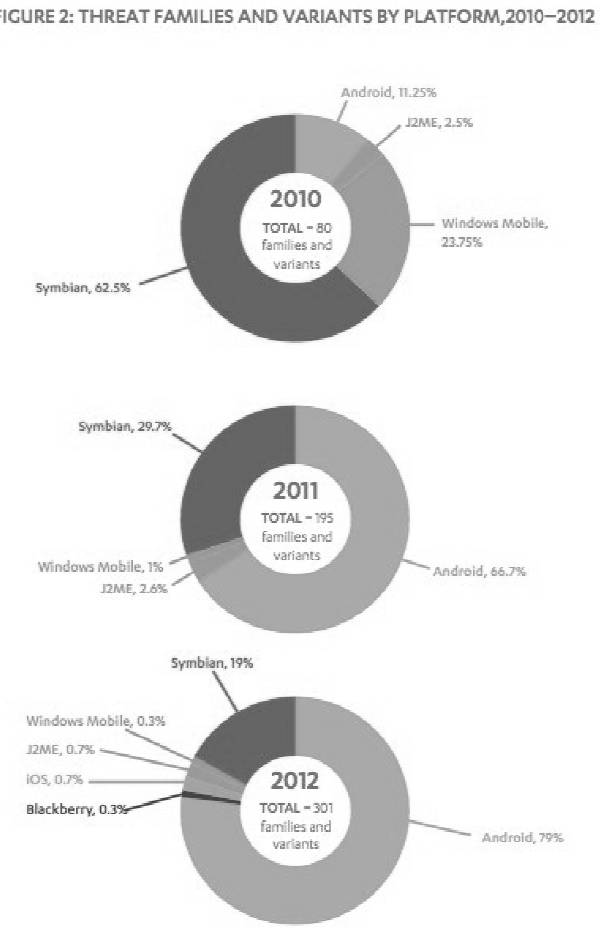
1. *Zařízení využívané pro obsluhu bankovního účtu by mělo být vybaveno:*

a) *aktualizovaným operačním systémem (pravidelné aktualizace odstraňují bezpečnostní slabiny systému odhalené až při jeho využívání),*

b) *aktualizovaným internetovým prohlížečem (k aktualizaci dochází zpravidla automaticky s aktualizací celého operačního systému),*

c) *funkčním (trvale zapnutým) a aktualizovaným antivirovým programem (aktualizace je obvykle prováděna automaticky). Současně by měl uživatel pravidelně spouštět antivirovou kontrolu.“* (13)

Nicméně výše uvedená doporučení ČNB jsou pouze obecně zaměřená na mobilní zařízení s nespecifikovanou platformou. Avšak důvod, proč je nutné se na danou problematiku vzhledem k mobilní platformě Android OS zaměřit, vychází z analýzy společnosti F-Secure, která mapovala výskyty bezpečnostních hrozeb na těchto zařízeních v letech 2010 až 2012 v závislosti na dané platformě. (38)

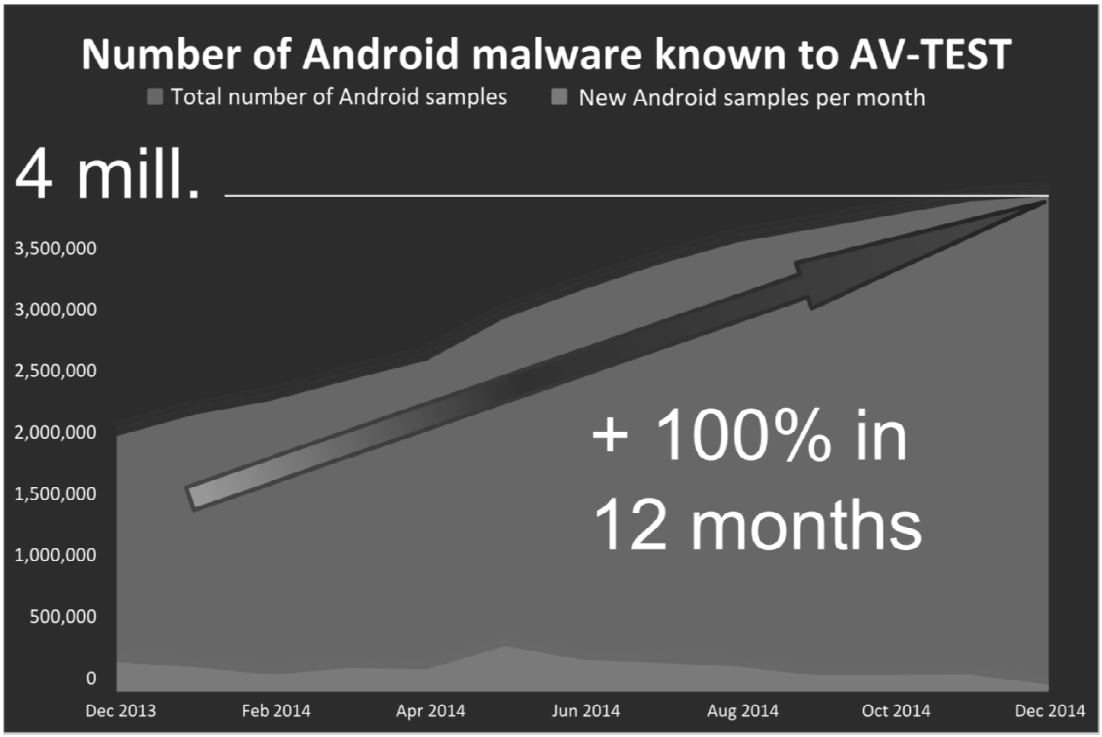


Obrázek 7- Bezpečnostní hrozby dle platforem 2010 - 2012 (42)

Z obrázku 7 je zcela patrné, že již v těchto letech měly výskyty potenciálních rizik u mobilní platformy Android OS stoupající tendenci, která pokračuje i nadále. (42)

Vyobrazené rozložení rizik je však dle názoru autora práce poněkud zavádějící, jelikož jsou zde zohledněna veškerá možná rizika platformy, nikoliv pouze aplikace pocházející z oficiálního zdroje Obchod Play (viz. Analýza společnosti Trend Micro).

O stoupajícím trendu nárůstu malware pro mobilní platformu Android OS svědčí i analýza renomovaného bezpečnostního serveru AV-test.org, ze které vyplývá, že během roku 2014 byl zaznamenán přibližně dvojnásobný počet odhalených hrozeb pro danou platformu. Tento zdroj se v rámci příčin tohoto razantního nárůstu odkazuje na odhadovaný celosvětový počet uživatelů okolo 2 biliónů s tím, že například v sousedním Německu má platforma Android OS více než 80 procentní zastoupení mezi všemi mobilními zařízeními. (43)



Obrázek 8 - Vývoj bezpečnostních hrozeb Android OS 2014 (43)

Bezpečnostní rizika přitom uživatel může do jisté míry eliminovat nejen antivirovými aplikacemi s hrazenou licencí, ale i zcela freeware verzemi alternativních bezpečnostních aplikací.

Pro zhodnocení případných rizik je nejprve nutné opětovně zmínit strukturu Android OS (viz obrázek 3), což má velmi podstatný vliv na možný nechtěný průnik. Systém je rozdělen do několika úrovní, přičemž každá nižší úroveň by měla mít vyšší ochranu. Samotné jádro systému však běží bez jakéhokoliv zabezpečení a u případných nadstaveb je to již otázka SandBoxu, ve kterém běží každá aplikace odděleně.

5.2 Typy bezpečnostních hrozeb

5.2.1 Phishing (spear phishing)

Mezi nejčastější útoky na internetové bankovnictví patří takzvaný Phishing, což je označení pro podvodnou techniku získání citlivých uživatelských dat. Zpravidla je charakterizován zasláním e-mailové zprávy, či využitím instant message, pod kterou se skrývá fiktivní administrátor webu, jenž vyzývá zadání citlivých přihlašovacích údajů na falešné webové stránky, které jsou však téměř nerozeznatelné od originálních. Ochranou uživatele je tak vždy na podobné zprávy nereagovat, i když může přijít ze zdánlivě korektní e-mailové adresy vedené pod doménou dané finanční instituce, což rovněž působí velmi autenticky.

V praxi tento způsob hrozby přináší rizika pro uživatele běžného internetového bankovnictví, jelikož v případě mobilní aplikace se uživatel přihlašuje přímo do rozhraní dané aplikace. Nicméně tento způsob podvodného získání citlivých údajů byl rozvinut i pro mobilní telefony a nese označení tzv. „spear phishing“. Tato technika uživatele bankovní aplikace může ohrozit, jelikož namísto hypertextového odkazu na fiktivní webové stránky může obsahovat například přílohu ve formě „.apk“ souboru se zdánlivou novou verzí bankovní aplikace, která po instalaci přenese citlivé přihlašovací údaje přímo útočníkovi. (44)

5.2.2 Pharming

Pharming patří mezi další, avšak propracovanější techniky podvodného získání citlivých uživatelských dat. Oproti Phishingu však nevyužívá podvodné e-mailové zprávy, ale přímo napadá DNS, kde přepisuje IP adresu a uživatel je tak po zadání regulérního URL přesměrován na podvodné webové stránky útočníka. Nicméně v oblasti mobilních aplikací tato technika nepřináší uživateli žádná rizika.

5.2.3 Vishing

Touto technikou se útočník, obdobně jako tomu bylo u metody Phishing, snaží získat citlivé údaje od uživatele. Rozdílem je však forma provedení útoku, jelikož není prováděn prostřednictvím e-mailových zpráv, ale telefonicky. Útočník zpravidla působí jakožto operátor dané finanční instituce a pod záštitou nastavení dalších služeb, či potřeby administrace účtu se snaží z oběti vylákat citlivé informace. Nicméně z důvodu vyšší důvěryhodnosti tyto útoky mohou probíhat ve více fázích, kdy při prvním útoku útočník zjistí například posledních několik znaků přihlašovacích údajů a při dalším telefonátu, který realizuje s odstupem času, se útočník zaměří na zbývající část přihlašovacích údajů, aniž by kvůli časovému odstupu uživatel pojal podezření na zneužití jeho údajů.

5.2.4 SMiShing

Smishing je možné definovat jako obdobu útoku typu Vishing s tím rozdílem, že útočník se snaží od uživatele získat jeho citlivá data prostřednictvím SMS zpráv. Zaslaná podvodná zpráva může opět obsahovat výzvu k odeslání přihlašovacích údajů. (45 str. 158)

Rizikovost technik Vishing a SMiShing není v případě bankovních aplikací příliš vysoká, jelikož by útočník poté musel fyzicky získat zařízení, na kterém je aplikace nainstalovaná. Nicméně pokud by v rámci útočníkovy SMS zprávy došlo ke stažení a instalaci škodlivé aplikace, riziko je již podstatně vyšší.

5.2.5 Keylogger

Keylogger nese označení typ software, jenž zpravidla běží na pozadí a detekuje stisk klávesy či dotyku displeje, které souhrnně monitoruje a ukládá. Tento typ útoku je nejčastěji cílen na získání přihlašovacích údajů do internetového bankovnictví. U mobilní platformy Android OS je možné se s tímto pojmem setkat cíleně v oblasti rodičovských kontrol (46), nicméně při zaměření na potenciální rizika pro mobilní zařízení není samotné riziko zneužití tak vysoké, jako tomu bylo u běžných osobních počítačů. Osobní počítače totiž disponují běžnou hardware klávesnicí, jejíž aktivitu keylogger sleduje. V případě mobilních zařízení, která jsou však vybavena dotykovým displejem, má uživatel

k dispozici klávesnici softwarovou, která je založena na mapování dotyků v rámci nastaveného rozložení znaků, což si vývojáři různých aplikací mohou nastavit individuálně. Útočníkovi tedy již nestačí monitorovat hodnoty přenášené se stisky fyzických kláves, ale musí zachycovat X a Y souřadnice oblastí na obrazovce a dále je kombinovat s místy dotyku na obrazovce, aby odvodil, co patrně uživatel zadával. Tato hrozba se však vztahuje především na zařízení s přidělenými právy „superuživatele“, neboli „root“. (47)

5.2.6 Distributed DOS

Nejen uživatel může být cílem útoku, jelikož ten může být směřován i na vzájemnou komunikaci či přímo servery banky. Distributed Denial Of Service je forma útoku, kdy se v rámci komunikace klient-server útočník snaží zahltit server svými požadavky a tím zpomalit prováděné operace, případně útok dovést až k jeho pádu. Tento útok je zpravidla cílen a časován na nějakou určitou službu, nicméně je možné jej distribuovat i na více služeb současně. (48)

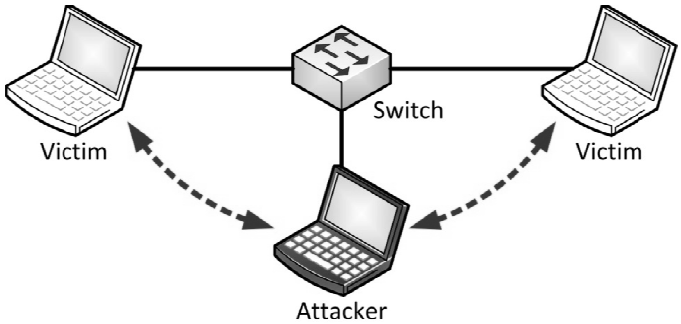
Nejčastěji se tyto útoky vztahovaly na webové stránky, na kterých se uživatelé přihlašovali do svého internetového bankovnictví, avšak v případě, že se podaří útočníkovi zacílit servery, na kterých běží bankovní aplikace, tak tento způsob útoku může ohrozit i smartbanking. Mezi projevy DDOS se vyskytuje extrémní zátěž hardware, změny v konfiguračním nastavení či extrémní přetížení operačního systému, které se projeví jeho pádem, což se vůči uživateli projeví tím, že jsou požadované služby nedostupné.

5.2.7 Man in the Middle

MITM víceméně napadá hashovací funkci a mění otisk zasílané zprávy. V důsledku toho je možné měnit obsah zprávy, což v případě přístupu k bankovnímu účtu může nést fatální následky. V praxi tato situace může nastat především, když si účastníci komunikace chtějí vyměnit veřejné klíče pro další komunikaci a tyto klíče jsou zachyceny útočníkem. Ten poté může předávat falešné klíče obsahující informaci, že patří druhé straně a stává se tak nežádoucím prostředníkem jejich komunikace. U místní síťové komunikace se velmi často vyskytuje zneužití ARP (Address Resolution Protocol), které nese označení ARP spoofing a spočívá v přesměrování přenášených paketů na MAC adresu útočníka.

Malware pro tento typ útoku byl objeven v roce 2012 společností McAfee Labs. Tato škodlivá aplikace se konkrétně zaměřovala na velmi známé finanční subjekty využívající tzv. Token Generátor u svých aplikací. Malware využíval logo a barvy ikony bankovní aplikace, takže se pro uživatele zdál autentičtější. Pro získání falešného tokenu musel uživatel projít prvním stupněm autentizace, což je zpravidla zadání navoleného hesla, které mu umožní vstup do části správy bankovního účtu. Pokud nebyl tento krok proveden, aplikace zpravidla ukázala nějaké chybové hlášení a pokud dále uživatel zvolil generovat, tak malware zobrazil falešný token, což bylo v podstatě náhodné číslo. Nicméně v tomto kroku malware odeslal heslo na konkrétní telefonní číslo spolu s identifikátory napadeného zařízení (tj. IMEI a IMSI). Stejná informace je zároveň zaslána na jeden z kontrolních serverů společně s dalšími údaji, jakožto telefonní číslo přístroje. Seznam řídících serverů je totiž umístěn v XML souboru originální APK. (49)

První dva seznamy jsou použity k provedení MITM útoku za pomoci filtrování příchozích SMS zpráv kvůli získání těch, které obsahují mTAN, což je mobilní verze transakčního autentifikačního čísla (mobile Transaction Authentication Number). Pokud jsou původní adresa a text zprávy nalezeny v seznamu zachycených dat, tak je obsah zaslán výchozímu řídícímu serveru. SMS zprávy mohou být rovněž přesměrovány na jiné číslo, které je uvedené v XML, pokud je v seznamu zachycených dat nakonfigurován atributem „toSms". Dalším podobným malware jsou Zeus a SpyEye, u kterých útočník může vytvořit bezdrátový přístupový bod ze svého zařízení, které se jeví jako veřejný přístupový bod Wi-Fi a jakmile se oběť přihlásí, tak útočník může sledovat jakýkoliv provoz pro pozdější analýzu. (49)



Obrázek 9 - MITM útok (50)

5.2.7.1 DoubleDirect

Nová technika MITM útoku, která je cílená na bezdrátové síťové přenosy mobilních zařízení, nese název DoubleDirect. Konkrétně využívá ICMP Redirect (Internet Control Message Protocol), jenž je využíván k informování směrovače pro možnost volby lepší trasy, a který útočník zneužívá pro přesměrování pro přesměrování síťové komunikace přes své zařízení. Vzhledem k tomu, že je tento typ útoku Full-duplex, což svědčí o tom, že útočníkem zvolený uzel je schopen současné oboustranné komunikace, tak je velmi nebezpečný. Útok je možné eliminovat za pomoci zakázání funkce ICMP Redirect, kterou využívají operační systémy iOS, Android a OS X. (51)

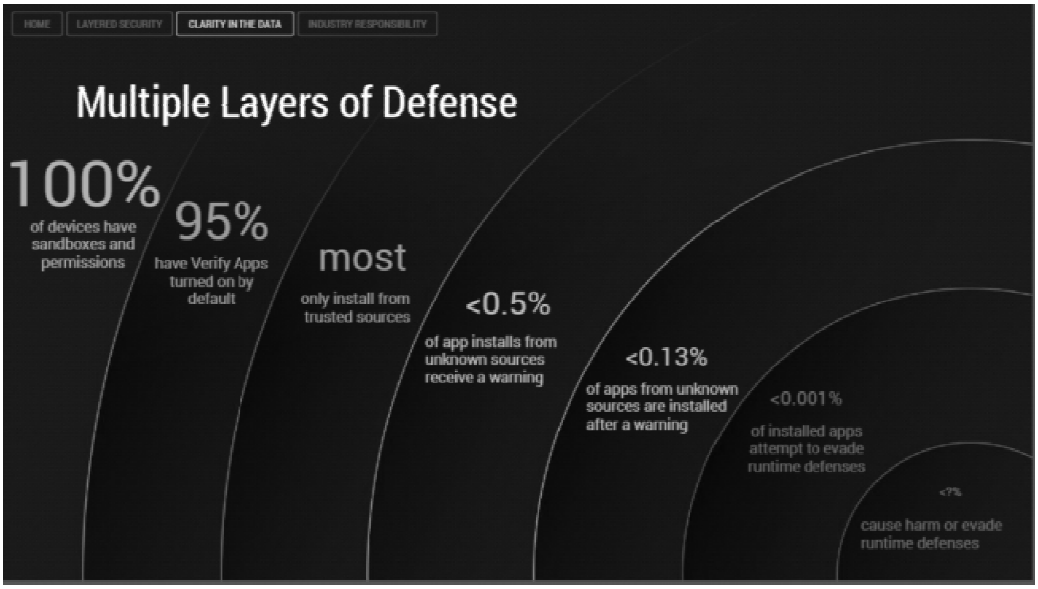
5.3 Analýza společnosti Trend Micro

Tvrzení o lukrativnosti platformy Android OS pro softwarové piráty bylo rovněž potvrzeno se zveřejněním analýz od společnosti Trend Micro, která si v celém světě vybrala a analyzovala přes 2 miliony aplikací. Výsledkem bylo odhalení 293 091 zcela jasně škodlivých aplikací tzv. PHA – Potentially Harmful Application, přičemž 69 tisíc infikovaných aplikací bylo staženo z oficiálního Android marketu označeného Obchod Google Play. Služba Google Play aktuálně nabízí aplikací více než 700 tisíc a zjištěné infekce svědčí o vážnosti tohoto problému. Další značně rizikovou oblastí jsou alternativní zdroje třetích stran, které jsou možným neoficiálním zdrojem aplikací pro uživatele, jenž se tak může vystavovat zbytečnému riziku při existenci dané aplikace v oficiální distribuci. Bohužel však existují státy, ve kterých není Google Play podporován, tudíž uživateli nezbývá jiná možnost než využití alternativních zdrojů. (52)

Po instalaci aplikace z neznámého zdroje však zapůsobí další obranný mechanismus s označením Verify Apps, který v průběhu instalace vytvoří její jedinečný otisk a odešle jej na sever Google, jenž jej porovná s databází škodlivých kódů a seznamem PHA. (53)

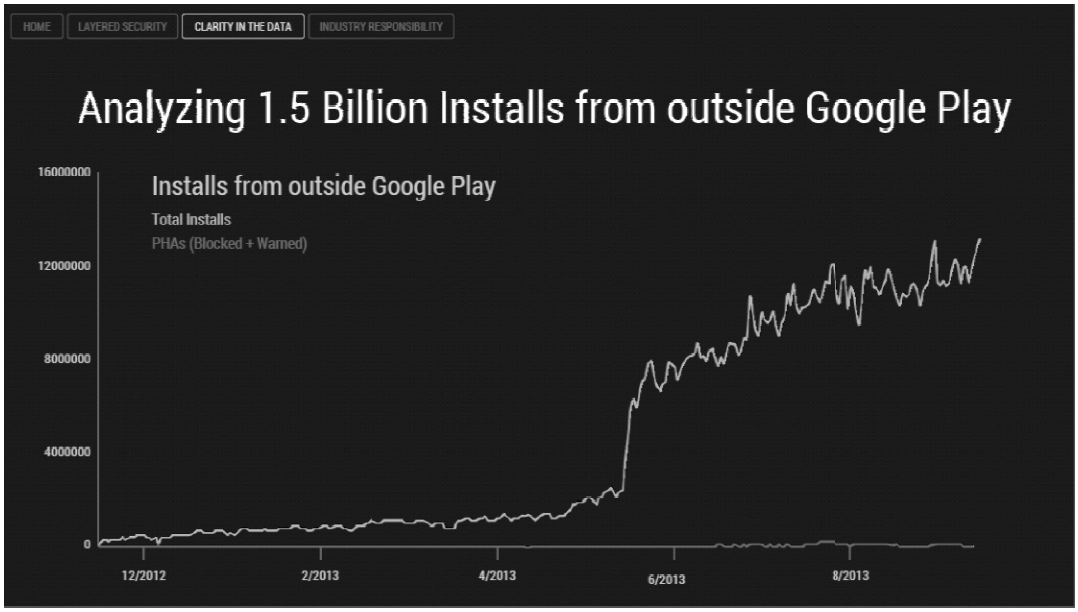
5.4 Google Android Security

Společnost Google riziko malware až do roku 2013 nijak oficiálně nekomentovala, jelikož v minulosti neměla analytickou platformu pro zálohování bezpečnostních hlášení systému, což se změnilo se zavedením Google Android Security. Na konferenci Virus Bulletin 2013 v Berlíně byla zveřejněna data o nižší než 0,001% množství aplikací, které dokážou obejít mnohostupňovou ochranu systému.



Obrázek 10 – Rizikovost dle vrstev OS (54)

V rámci zvýšení bezpečnosti bylo založeno CDC (centrum pro kontrolu nemocí), které má za úkol evidovat případné hrozby malware a nové bezpečnostní mechanismy kontrolují jednotlivě nainstalované aplikace s databází CDC. V systému je tak defaultně nastavena kontrola a blokování potenciálně nebezpečných aplikací, kterou však uživatel může deaktivovat. Na základě těchto služeb se kontroluje více než 1,5 miliardy aplikací. Při namátkové kontrole 1 milionu aplikací pak bylo nalezeno 1200 potenciálně škodlivých aplikací, což činí 0,12%.



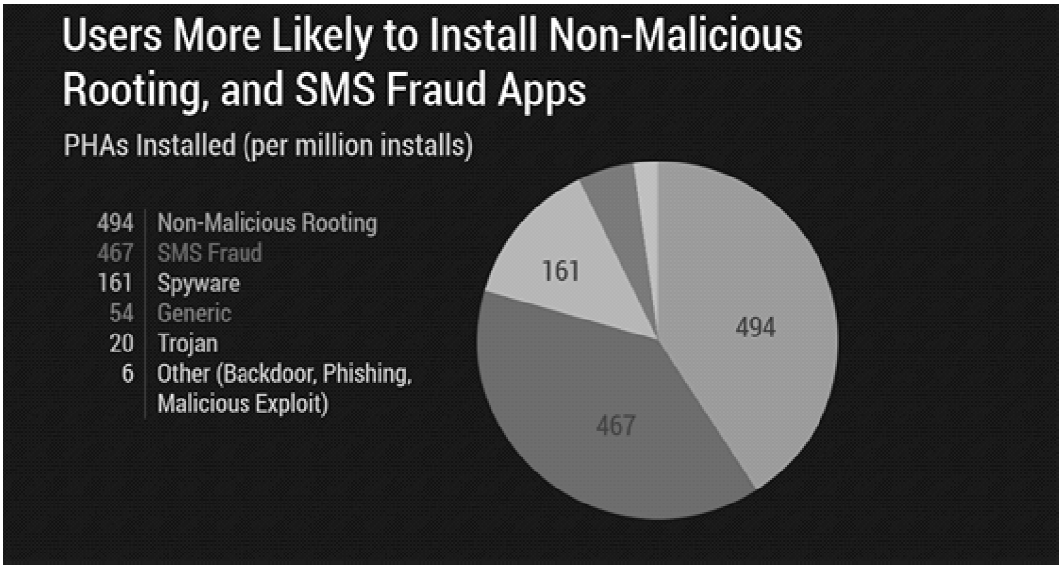
Obrázek 11 – Instalace aplikací mimo Google Play (54)

Po varování systému již záleží pouze na uživateli, zdali na toto riziko přistoupí, nebo danou aplikaci raději nenainstaluje. Konkrétní službou Play Store, která skenuje potenciální rizikovost aplikace, je služba Bouncer. (38) Tato služba nemá stoprocentní výsledky, avšak z hlediska množství nabízených aplikací je stále dostatečnou alternativou namísto jednotlivého ručního testování. Pokud by však uživatel přesto nebezpečnou aplikaci nainstaloval, tak Google může za pomoci mechanismu tzv. Kill Switch případný malware přes vzdálené připojení odstranit. (53)

5.5 Výsledky testování Google Android Security

Z nalezených potenciálně škodlivých aplikací jich bylo necelých 40% typu fraudware, jenž se zaměřuje na zpřístupnění uživatelovo zařízení pro příjem reklamních nabídek či rozesílání placených SMS. Zhruba stejné množství škodlivých aplikací bylo typu „rooting", jež jsou zaměřeny na přístroje nadšenců a vývojářů, kteří mají povolena práva „superuživatele“, neboli tzv. „root“. Dalších zhruba 15% škodlivých kódů bylo typu spyware, které na základě stisků kláves uživatele monitorují jeho činnost a poté odesílají již cílený komerční malware na konkrétní zájmové skupiny. (54)

Z hlediska bližšího rozboru typu škodlivého kódu u PHA připadá z celkového množství 1,5 miliardy testovaných aplikací v průměru na 1 milion odhaleno 494 případů PHA související se superuživatelskými právy v daném zařízení. Dalších 467 PHA bylo spjato s odesíláním SMS a 161 PHA bylo typu spyware. Objevily se zde i PHA typu Trojan a další hrozby z oblasti Phishingu.

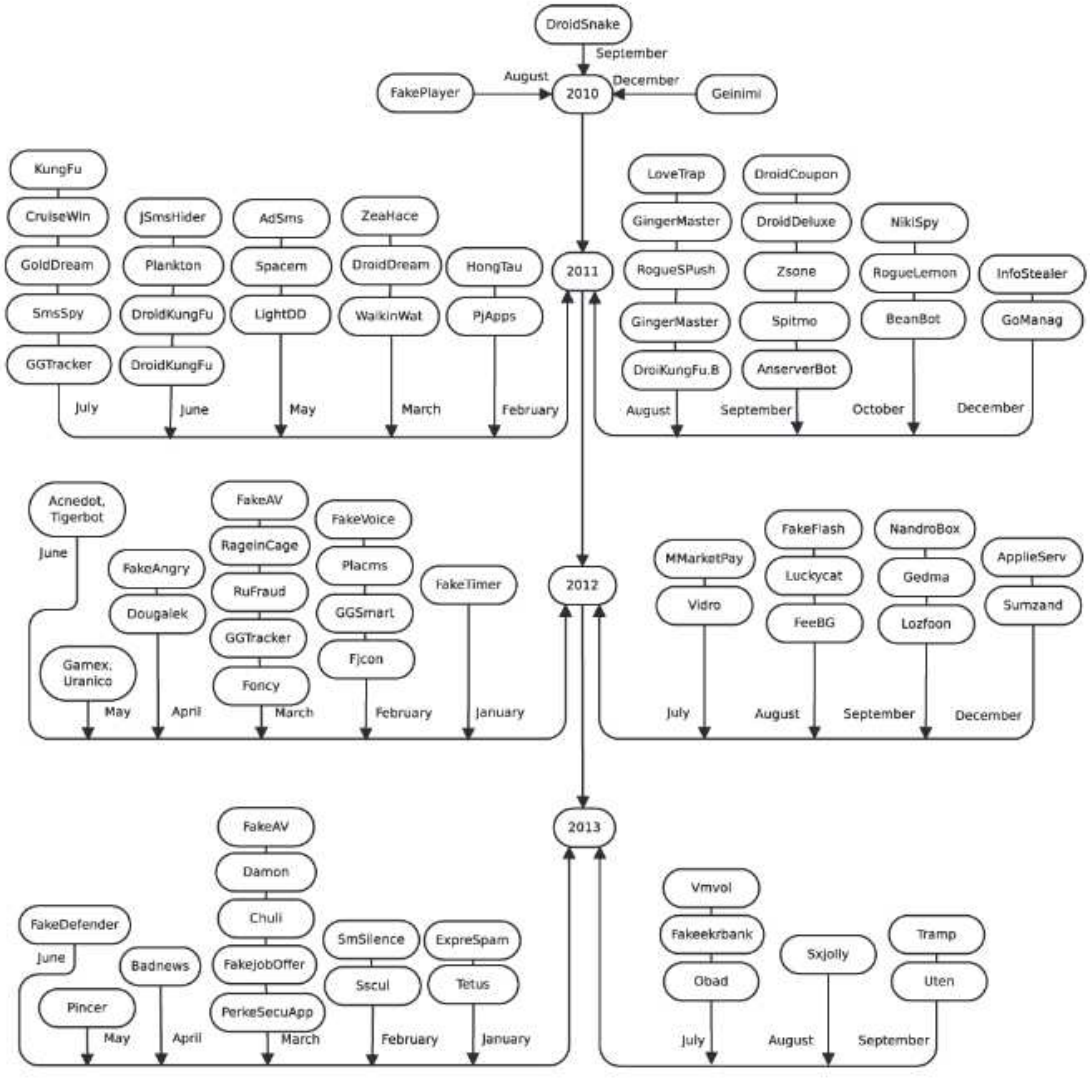


Obrázek 12 – Podíl nalezených hrozeb dle jejich typu (53)

Velmi podstatný vliv na bezpečnost instalovaných a používaných aplikací mají oprávnění, které uživatel instalované aplikaci přiřadí. Může se jednat například o sledování polohy, přístup k osobním údajům, přístup k internetu či možnosti odesílat SMS zprávy. Uživatel tak při své neopatrnosti může přehlédnout přidělení tohoto oprávnění dané aplikaci, která začne rozesílat placené SMS a uživatel tak bez jakéhokoliv vědomí přichází o značné finanční prostředky. Vhodným řešením je tuto možnost zablokovat u využívaného mobilního operátora. (54)

5.6 Rodokmen Android OS malware

Uvedené informace o nárůstu bezpečnostních hrozeb Android OS se vztahovaly především k počtu a typu rizik. Autor práce považuje za podstatné, představit i konkrétní typy hrozeb, které jsou vyobrazeny v chronologickém vývoji na obrázku 13.



Obrázek 13 - Chronologický vývoj bezpečnostních hrozeb platformy Android OS (33)

5.7 Testy antivirových aplikací (AV-Test.org)

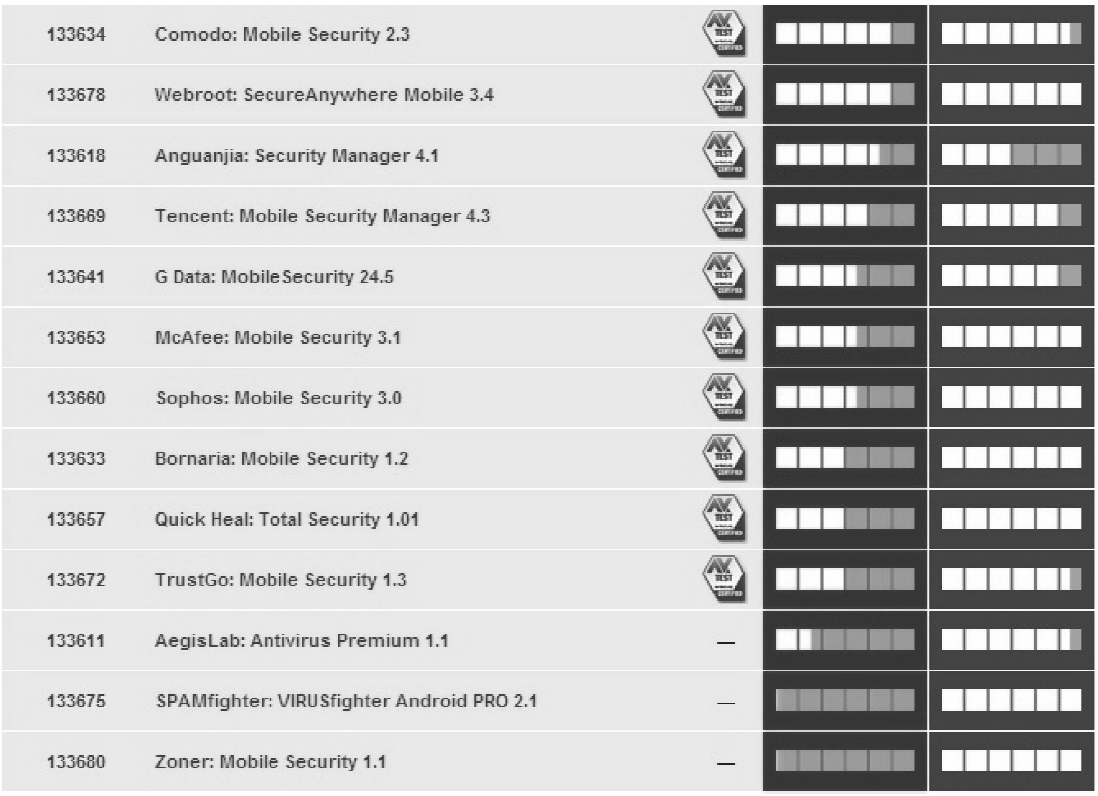
Z předchozích kapitol vyplývá, že sama společnost Google se snaží eliminovat rizika spojená s PHA, avšak pro vyšší uživatelský komfort je vhodné zvolit ochranu

pomocí antivirové aplikace. Další mýtus kolující mezi uživateli této platformy vychází z obavy o přílišné zátěži systémových prostředků daného zařízení a s tím spojenou výdrží baterie.

5.7.1 Testování antivirových aplikací 2013

Server AV-Test.org v září roku 2013 otestoval 28 bezpečnostních aplikací, ze kterých 26 nemělo zásadní vliv na výkon či výdrž baterie přístroje. Z celkového výběru 1460 aplikací byla průměrná úspěšnost odhalení PHA 90,5 % a jedenáct aplikací se dostalo na hranici 99 %. Rovněž 22 z vybraných bezpečnostních aplikací již v základu podporuje funkce anti-theft, dálkového vymazání dat a lokalizaci daného zařízení. Z tohoto výběru zároveň 19 aplikací podporovalo pokročilou možnost blokování příchozích hovorů pro nevyžádaný telemarketing. (55)

Testreport	Producer: Product	PROTECTION	USABILITY
133655	Qihoo: 360 Mobile Security 1.2		
133615	AhnLab: V3 Mobile 2.1		
133620	Antiy: AVL 2.2		
133622	Armor for Android: Armor for Android 2.1		
133624	Avast: Mobile Security 3.0		
133628	Avira: Free Android Security 2.0		
133632	Bitdefender: Mobile Security 1.2		
133638	ESET: Mobile Security 2.0		
133640	F-Secure: Mobile Security 8.2		
133643	Ikarus: mobile.security 1.7		
133648	Kaspersky: Mobile Security 11.1		
133649	Kingsoft: Mobile Security 3.0		
133650	Lookout: Security & Antivirus 8.21		
133667	Symantec: Norton Mobile Security 3.6		
133670	Trend Micro: Mobile Security 3.1		



Obrázek 14 – Výsledky testů antivirových aplikací (55)

5.7.2 Dlouhodobé testování antivirových aplikací 2014

Avšak vzhledem k rozvoji bezpečnostních hrozeb platformy Android OS je vhodné uvést časové srovnání testovaných aplikací, které vychází z dlouhodobého testu výše jmenovaného serveru, jenž probíhal během šesti měsíců roku 2014. V rámci daného testu bylo vybráno 35 antivirových aplikací, které byly podrobeny sérii třech testů, z nichž 26 aplikací prošlo všemi třemi fázemi. Rovněž zde bylo, vyjma ochrany daného zařízení, testováno, jaká je použitelnost dané aplikace a jaké obsahuje další vestavěná rozšíření. V rámci testování aplikace získávaly body, jejichž maximum bylo pro celé testování stanoveno na 13 bodů. Z testovaných 26 aplikací, které prošly všemi třemi fázemi testu, získalo 7 aplikací plné hodnocení, přičemž dalších 10 se pohybovalo v rozmezí 12.3 až 12.8 získaných bodů. (43) V této části je nutné vyzdvihnout skutečnost, že 5 ze 7 nejlépe hodnocených aplikací spadá pod freeware licenci.

Vzorek pro testování antivirových aplikací vycházel z průměrně 2 600 infikovaných aplikací za jedno období, které byly identifikovány za pomoci „hlídacích psů“ pro Android a následně zařazeny do testu. Tento postup byl opakován pro každý následující test. Výsledkem bylo, že osm testovaných aplikací dokázalo odhalit veškeré hrozby. Konkrétně se jednalo o aplikace Antiy, Bitdefender, Cheetah Mobile (3 verze), ESET, Qihoo a Trend Micro. Avšak dalších 5 testovaných aplikací dokázalo odhalit 99,9% hrozeb. Celkově tak 19 z 26 testovaných aplikací dokázalo odhalit 99% a více škodlivého kódu. (43)

V rámci testu byla rovněž, vyjma hodnocení detekce a ochrany před případnou hrozbou, testována i použitelnost daných aplikací. V této části testu jsou především zohledněny požadavky, které klade aplikace na systémové zdroje a s tím spojený vliv výdrž baterie daného zařízení. Rovněž zde byl zohledněn častý výskyt tzv. falešných poplachů, kdy antivirová aplikace mylně vyvolá zdání rizika i v aplikacích, které pochází z ověřeného zdroje. Z tohoto důvodu byla nastavena aspirační úroveň pro toto kritérium na hranici 3 000 testovaných aplikací, u kterých nesměl být vyvolán tento falešný poplach. Zde se již objevují jisté rezervy u aplikací od vývojářů Symantec a AVG, které dosáhly nejnižšího počtu 4,3 bodu na 6 bodové stupnici. Zbylých 24 ze 26 testovaných aplikací v tomto testu získalo mezi 5 až 6 body.

Poslední část testu byla zaměřena na rozšiřující vestavěné funkce, avšak kvůli neexaktní povaze tohoto testu byl aplikacím přidělován pouze jeden bod. V rozšiřujících možnostech se nejčastěji vyskytovaly funkce zaměřené na rizika spojená s odcizením daného zařízení. Konkrétně se jednalo například o funkce blokování zařízení, lokalizace jeho polohy nebo vzdáleného vymazání uživatelských dat. Rovněž se zde objevovaly funkce rodičovské kontroly, blokování příchozích hovorů, filtrování zpráv, kódování úložiště nebo rezidentní webový štít.

Manufacturer	Product	Protection (max. 6 pts)	Usability (max. 6 pts)	Features/Extras (max. 1 pt)	Overall Points Total (max. 13)	Number of Tests	AV-TEST Certificate
Antiy	AVL	6.0	6.0	1.0	**13.0**	3	YES
Bitdefender	Mobile Security	6.0	6.0	1.0	**13.0**	3	YES
Cheetah Mobile	Kingsoft Mobile Security	6.0	6.0	1.0	**13.0**	3	YES
Cheetah Mobile	Clean Master	6.0	6.0	1.0	**13.0**	3	YES
Cheetah Mobile	CM Security	6.0	6.0	1.0	**13.0**	3	YES
ESET	Mobile Security & Antivirus	6.0	6.0	1.0	**13.0**	3	YES
Qihoo 360	360 AntiVirus	6.0	6.0	1.0	**13.0**	3	YES
AhnLab	V3 Mobile	5.8	6.0	1.0	**12.8**	3	YES
Trend Micro	Mobile Security	6.0	5.8	1.0	**12.8**	3	YES
McAfee	Mobile Security	5.7	6.0	1.0	**12.7**	3	YES
Sophos	Mobile Security	5.7	6.0	1.0	**12.7**	3	YES
Anguanjia	Security Manager	5.8	5.8	1.0	**12.6**	3	YES
avast!	Mobile Security	5.5	6.0	1.0	**12.5**	3	YES
Kaspersky	Internet Security	5.8	5.7	1.0	**12.5**	3	YES
Quick Heal	Total Security	5.7	5.8	1.0	**12.5**	3	YES
Baidu	Mobile Security	5.7	5.7	1.0	**12.4**	3	YES
Avira	Free Android Security	5.8	5.5	1.0	**12.3**	3	YES
F-Secure	Mobile Security	4.8	5.8	1.0	**11.6**	3	YES
Tencent	Mobile Security Manager	5.3	5.0	1.0	**11.3**	3	YES
Symantec	Norton Mobile Security	5.8	4.3	1.0	**11.1**	3	YES
G Data	Internet Security	5.0	5.0	1.0	**11.0**	3	YES
Webroot	SecureAnywhere Mobile	4.0	5.8	1.0	**10.8**	3	YES
Ikarus	Mobile Security	4.2	5.5	1.0	**10.7**	3	YES
Comodo	Mobile Security	4.0	5.5	1.0	**10.5**	3	YES
Bornaria	Mobile Security	3.7	5.7	1.0	**10.4**	3	YES
AVG	AntiVirus FREE	4.8	4.3	1.0	**10.1**	3	YES
Other apps with just 2 tests							
BullGuard	Mobile Security	6.0	6.0	1.0	**13.0**	2	YES
PSafe	Total	6.0	6.0	1.0	**13.0**	2	YES
Trustlook	Antivirus	5.8	6.0	1.0	**12.8**	2	YES
TrustGo	Mobile Security	5.5	5.8	1.0	**12.3**	2	YES
NSHC	Droid-X 3	2.8	6.0	1.0	**9.8**	2	YES
Other apps with just one test							
DU Apps Studio	DU Speed Booster	5.5	6.0	1.0	**12.5**	1	YES
Alibaba	Mobile Security	6.0	4.0	1.0	**11.0**	1	YES
Jarviz	MobileHeal Pro	0.0	5.5	1.0	**6.5**	1	NO
White Gate	AntiVirus	0.0	4.0	1.0	**5.0**	1	NO

Please note: Products with the same points totals are listed in alphabetical order, Cheetah Mobile is the vendor formerly known as the companies Kingsoft and KS Mobile.

Obrázek 15 - Výsledky dlouhodobého testu antivirových aplikací (43)

Obecně lze tedy potvrdit postoj autora práce, že rizika spojená s mobilní platformou Android OS zcela jistě mohou mít zásadní dopad na uživatele, nicméně nejčastější veřejně komunikované skutečnosti ohledně rizik, které se vztahují k jejich rostoucímu počtu, jsou především otázkou zemí, ve kterých není podporován oficiální zdroj aplikací Obchod Play. Rovněž je nutné uvést, že není vhodné využívat bankovní aplikace na přístrojích, u kterých jsou přidělena práva „superuživatele“, na což upozorňuje i Česká národní banka (13), se kterými se objevují další případná rizika nechtěného průniku softwarovými piráty. Běžnému uživateli tedy postačí využití antivirové aplikace, nicméně nejpodstatnější vliv

má především jeho obezřetné chování, jako si tomu běžně navykli uživatelé osobních počítačů.

5.8 Společenská odpovědnost finančních institucí

Výše uvedené skutečnosti a doporučení se vztahují na uživatelskou část této problematiky, přičemž je nutné zohlednit, že za rizika napadení nese odpovědnost především finanční instituce, která mobilní aplikaci nabízí. Problematika možných rizik a obav klientů daných finančních institucí z využívání této formy komunikace s bankou je rovněž zakořeněna v postojích finančních institucí v ČR k odpovědnosti za případný útok. Obecně je možno odkazovat se na světový trend, kdy se banky snaží ochránit klientovy finance a berou na sebe tzv. společenskou zodpovědnost. Tato skutečnost se například odráží v postojích daných bank, které poskytují garance pro uživatele internetového bankovnictví. (56)

Podobný přístup však v ČR není zaveden a tím pádem se otevírají značné rezervy v PR daných software produktů pro správu finančních prostředků za pomoci mobilního zařízení. Otázka informační gramotnosti vzhledem k této situaci dle autora práce zapadá do pozadí problému, jelikož v případě, kdy banka poskytne svým klientům garance k využívání jimi distribuovaného softwarového produktu, zdůrazní vlastní důvěru v poskytované řešení. Zároveň většina klientů nemusí mít přílišný zájem se o danou problematiku aktivně zajímat a rozšiřovat tak aktivně svoji informační gramotnost, tudíž poskytnutá garance by pro ně byla silnějším motivem upustit od svých obav, než případné spontánní individuální hledání potřebných informací uživatelem.

Vzhledem k výše uvedeným rizikům, možnostem a postojům, se tak zcela ideální kombinací, kterou je pro banku reálné realizovat, jeví garance odpovědnosti rizik, ve spojení s vytvořenými a efektivně komunikovanými doporučeními na bezpečné zacházení s chytrým telefonem disponujícím mobilní platformou Android OS a dále případně nastavení určitého „věrnostního programu“, v rámci kterého by klienti dané banky měli možnost získat licenci prověřené antivirové aplikace. V případě bezpečnosti, která je prospěšná obou zúčastněným stranám, autor práce vidí větší význam poskytnout antivirovou licenci, namísto běžných a mnohdy zcela bezpředmětných propagačních

předmětů. Nejen pro základní, ale zcela plnohodnotnou ochranu, není výsledně nutné volit hrazenou licenci. V této oblasti existuje prostor kvalitního freeware řešení, v rámci kterého by tak uživatel získal potřebnou ochranu. (43) Banka by tak zvýšila podvědomí o bezpečném užívání těchto zařízení a zároveň by pasivně zvýšila bezpečnost svých klientů.

6. Analytická část

Vypracování analytické části práce vychází ze sběru dat za pomoci dotazníkového šetření, jež je uvedeno v metodice práce. Dotazníkové šetření bylo provedeno za pomoci online nástroje Google Forms a to konkrétně od 30.9.2015 do 8.11.2015, kdy se do dotazníkového šetření zapojilo 101 respondentů. Vzhledem k specifické povaze zaměření práce byl formulář nastaven pro příjem odpovědí respondentů starších 15-ti let, což bylo ošetřeno filtrovací otázkou, která respondenty mladší 15 let nezaznamenala mezi získané odpovědi, jelikož dle legislativy ČR nemohou mít jakékoliv příjmy z pracovní činnosti, tudíž jejich nízká solventnost není pro potřeby analýzy preferencí uživatelských funkcí rozhodující. Kompletní znění dotazníku je k dispozici v příloze této práce.

6.1 Sledovaná problematika

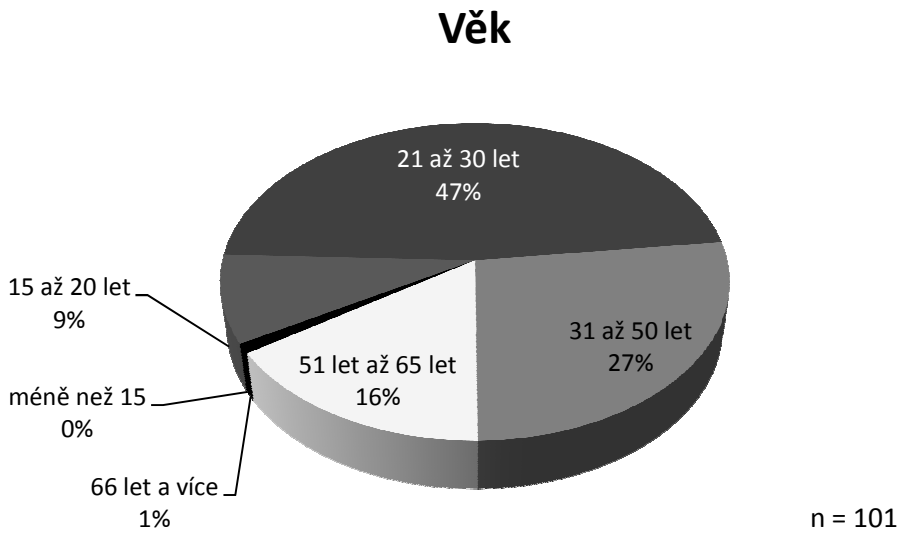
Získaná data budou nejprve představena za pomoci popisných statistik, následně na nich bude provedena analýza závislosti kvalitativních znaků pomocí statistického programu SAS a výsledně budou sloužit jakožto datová základna pro realizaci vícekriteriální analýzy variant k získání závěrů o preferencích uživatelů v oblasti nabízených funkcionalit bankovních aplikací.

Bankovní aplikace byly zvoleny od tří finančních institucí, a to konkrétně od České spořitelny a jejich řešení označené Servis 24. Druhá finanční instituce ve výběru je Komerční banka se svoji aplikací Mobilní Banka 2. Třetí vybranou aplikací Mobilní bankovnictví Air Bank od stejnojmenné finanční instituce. První dvě banky byly vybrány na základě jejich relativně vysokého podílu na trhu, jelikož v ČR patří mezi rozšířenější. Obě dvě tyto instituce patří do velkých zahraničních skupin, a to konkrétně Société Générale v případě Komerční banky a Erste Group v případě České spořitelny. Třetí

finanční instituce patřící do tuzemské skupiny PPF má svá určitá specifika, jelikož namísto běžné strategie fyzických poboček prosazuje vzdálený přístup a správu finančních prostředků, především za pomoci online nástrojů, což vznáší předpoklad o propracovanosti nabízené mobilní bankovní aplikace na nejvyšší míře.

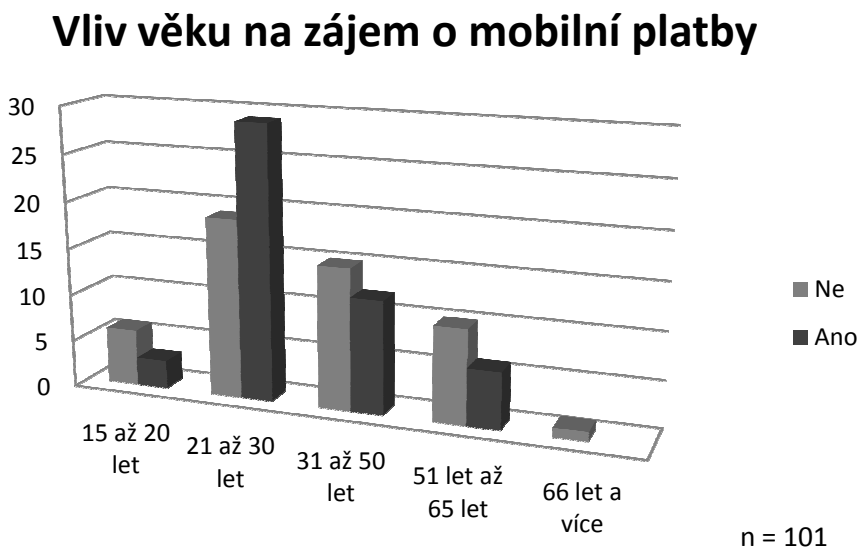
6.1.1 Popisné statistiky

Pro bližší představu o analyzovaných datech je vhodné uvést nejprve jejich popisné statistiky charakterizující respondenty dotazníkového šetření.



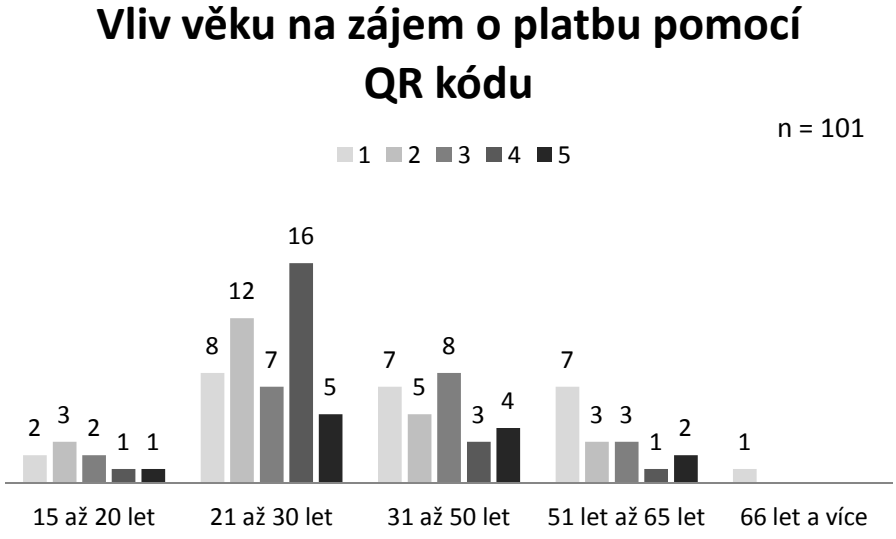
Obrázek 16 - Věk respondentů (vlastní)

Z pohledu na věk respondentů je patrné, že nejvyšší podíl datové základny tvoří respondenti ve věku 21 až 30 let. Další rozsáhlou skupinu tvoří respondenti věkové kategorie 31 až 50 let. Následujících 16% respondentů spadá do věkové skupiny 51 až 65 let a v neposlední řadě své zastoupení má i věková skupina 15 až 20 let, a to mezi 9% respondentů. Věková kategorie 66 let a více zde byla zastoupena jedním dotázaným.



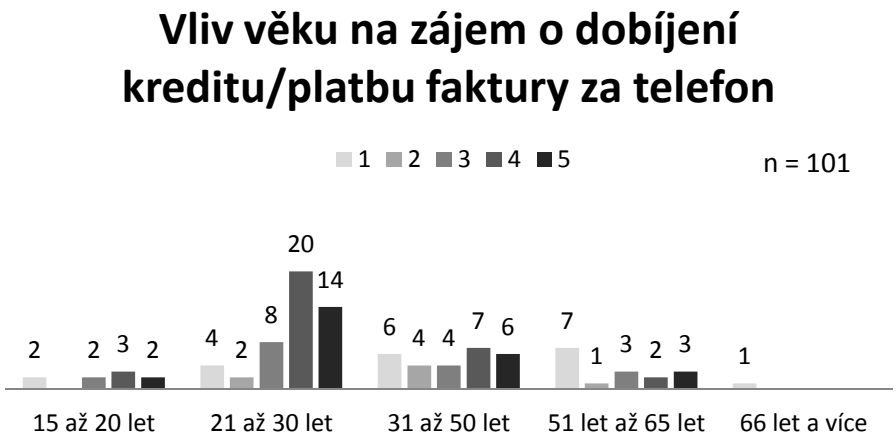
Obrázek 17 - Vliv věku na zájem o mobilní platby (vlastní)

Na základě výše uvedeného kontingenčního grafu je možné pozorovat určitý vliv věku na postoje uživatelů v rámci zájmu o platby za pomoci mobilního zařízení. Zde je zcela patrné, že nejotevřenější jsou této možnosti respondenti věkové kategorie 21 až 30 let, kteří patrně nejsou tak konzervativními uživateli. V rámci vyššího věku by se dalo usoudit, že respondenti jsou naopak konzervativnější. Z pohledu na kategorii 15 až 20 let lze usoudit, že respondenti spadají do nižší příjmové kategorie a případně stále žijí ve společné domácnosti s rodiči, tudíž zde není takový prostor pro plnohodnotné využití potenciálu mobilních bankovních aplikací.



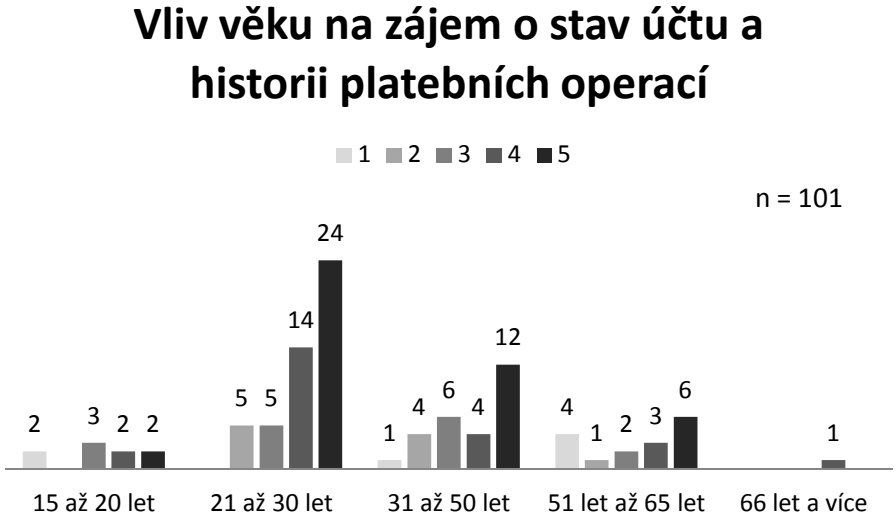
Obrázek 18 - Vliv věku na zájem o platbu pomocí QR kódu (vlastní)

Vzhledem k věku je možné pozorovat i určitý konzervativní přístup k novým trendům v oblasti přenášení platebních údajů, mezi které patří například možnost vytvoření platebního příkazu za pomoci načtení QR kódu. Zde je opět pozorovatelný zájem u věkové kategorie 21 až 30 let, přičemž naopak v kategorii od 51 let tento zájem opět klesá.



Obrázek 19 - Vliv věku na zájem o dobíjení kreditu/platbu faktury za telefon (vlastní)

Obdobnou situaci ohledně vlivu věku k zájmu o nabízené funkce je možné vypozorovat i vzhledem k vlivu tohoto parametru na zájem o možnost dobíjení kreditu či úhrady faktury za telefon.



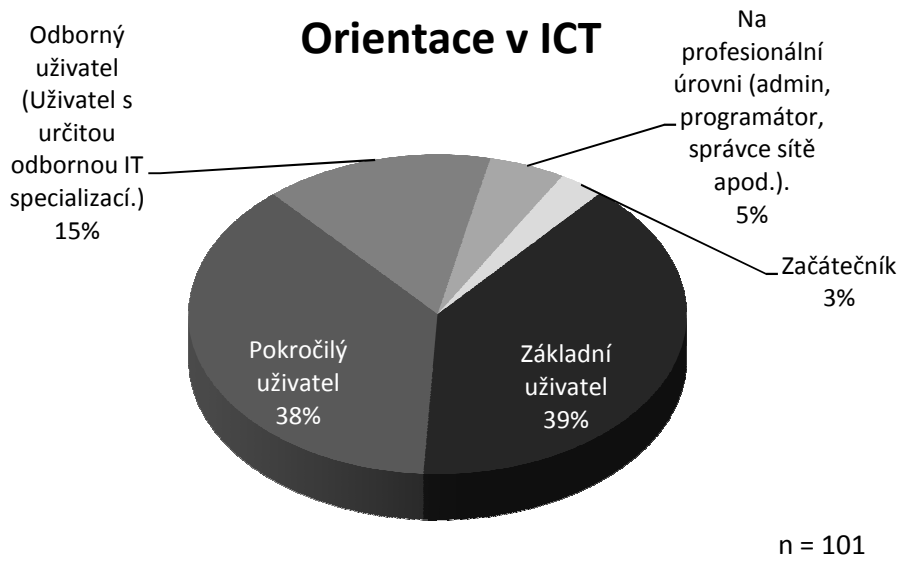
Obrázek 20 - Vliv věku na zájem o stav účtu a historii platebních operací (vlastní)

Naopak rostoucí zájem s ohledem k věku je možné pozorovat u zájmu o aktuální informace o stavu účtu a případném zobrazení historie platebních operací, na které patrně

nemá vliv konzervativní přístup uživatelů k mobilní bankovní aplikaci, jakožto obecný zájem o aktuální přehled o stavu finančních prostředků.

Obrázek 21 - Dosažené vzdělání respondentů (vlastní)

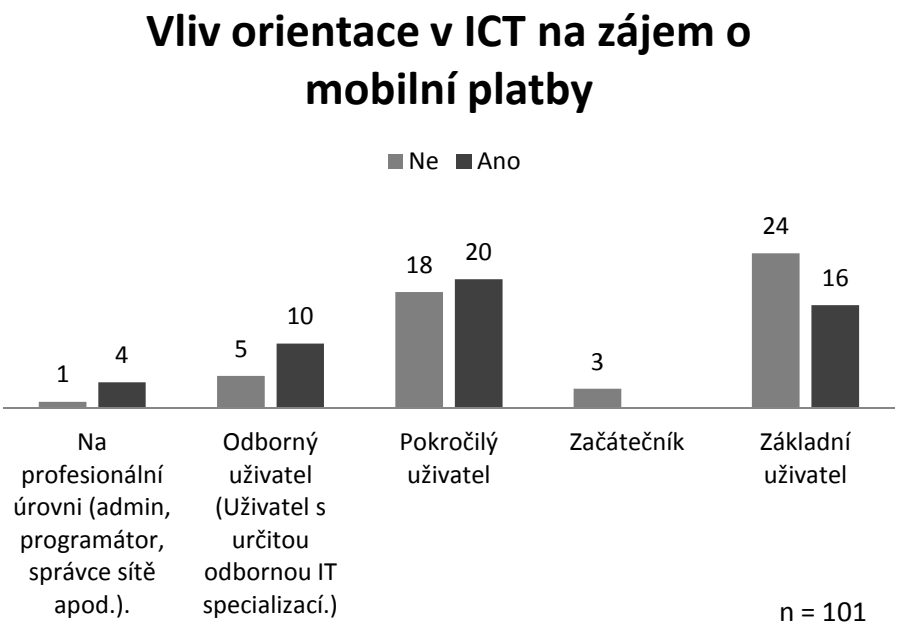
Dalším velmi podstatným sledovaným parametrem je nejvyšší dosažené vzdělání respondentů, které může mít vliv na výši jejich příjmu a rovněž i na návyky a postoje vztahující se k elektronickému platebnímu styku. Nejvyšší podíl zde tvoří skupina respondentů s dosaženým vysokoškolským vzděláním. Následně druhý nejvyšší podíl tvoří respondenti, kteří dosáhli středoškolského vzdělání s maturitou. V menším zastoupení se mezi respondenty vyskytlo vyšší odborné vzdělání, případně i v několika případech pouze základní či odborné vzdělání zakončené výučním listem.



Obrázek 22 - Orientace respondentů v oblasti ICT (vlastní)

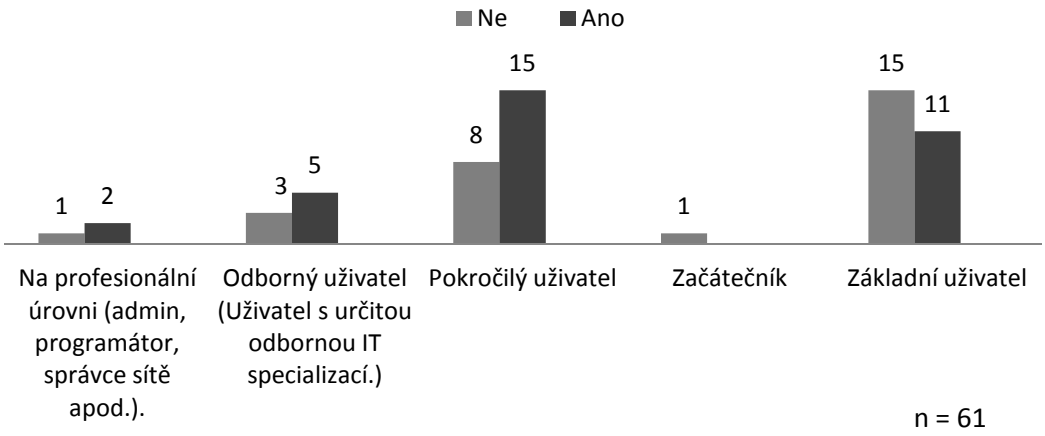
Výše uvedený graf určuje rozložení orientace respondentů v oblasti ICT, jelikož nejvyšší dosažené vzdělání nemusí být zárukou vysokého stupně informační gramotnosti. Vzdělání respondentů již není blíže charakterizováno oborem, ve kterém bylo dosaženo, což v případě například v oblasti humanitních oborů nemusí být zárukou vysoké informační gramotnosti.

Nicméně tento parametr má zpravidla silný vliv na chování a postoje uživatele, který by s vyšší mírou odborného přístupu k výpočetní technice měl přinášet i vyšší míru obecné informovanosti a lepší orientace v oblasti ICT. V datové základně se v nejvyšším podílu vyskytují uživatelé se základními dovednostmi a ve srovnatelném zastoupení i pokročilí uživatelé. V menší míře se zde objevují respondenti, kteří mají v oblasti ICT určitou odbornou specializaci. V okrajovém poměru jsou zde i zástupci, kteří se v této oblasti pohybují na profesionální úrovni, nicméně v několika případech se jedná i o naprosté začátečníky.



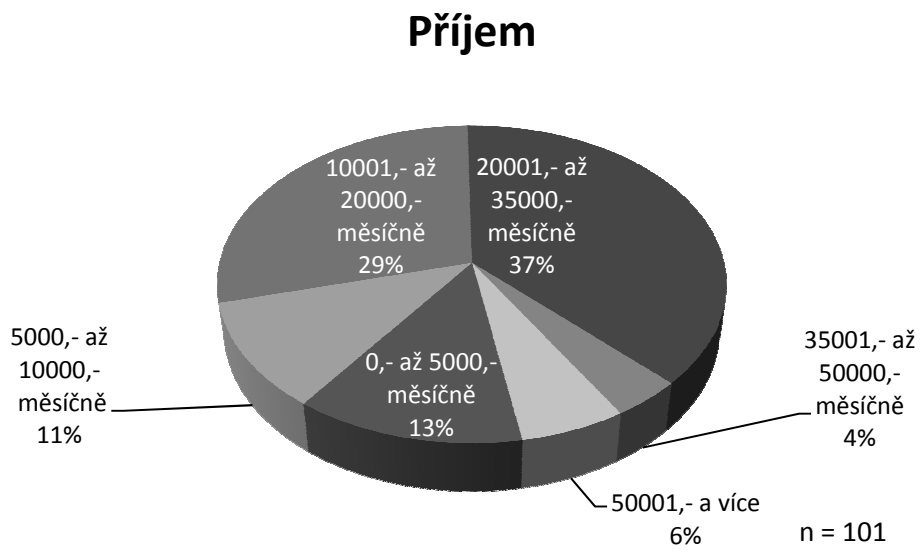
Obrázek 23 - Vliv orientace v ICT na zájem o mobilní platby (vlastní)

Na výše uvedeném kontingenčním grafu lze pozorovat vliv orientace respondentů na jejich zájem o mobilní platby. V daném grafu je patrné, že se zde objevuje nástin určitého trendu, kdy při rostoucím vzdělání roste i zájem o provádění platebních operací za pomoci mobilní bankovní aplikace.



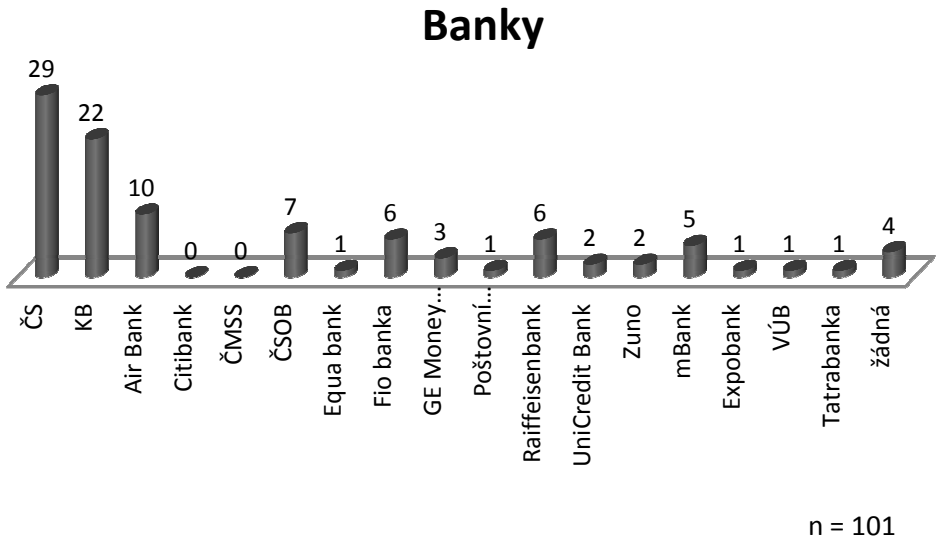
Obrázek 24 - Vliv orientace v ICT na využívání antivirové aplikace na Android OS

Rovněž je podstatné zaměřit se na vliv orientace respondentů v oblasti ICT na jejich případný postoj k využívání antivirové aplikace na mobilním zařízení s platformou Android OS. Z obrázku 23 je patrné, že s rostoucí informační gramotností se zvyšuje četnost využívání antivirové aplikace.



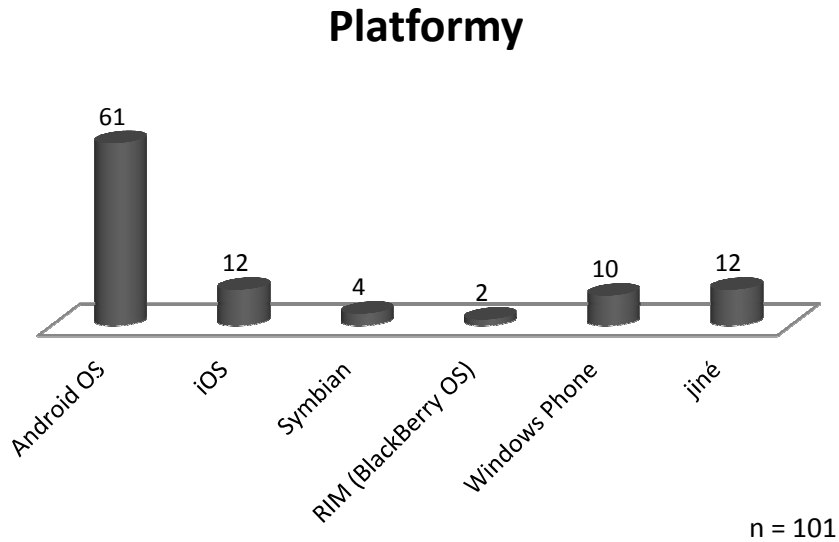
Obrázek 25 - Příjem respondentů (vlastní)

Vzhledem k zaměření práce na správu finančních prostředků za pomoci mobilní bankovní aplikace je rovněž vhodné uvést i rozřazení do skupin dle výše měsíčního příjmu. Z tohoto parametru je i celkem logické, že lze předpokládat přímou úměru mezi výší průměrného měsíčního příjmu a četnosti využívání elektronického bankovnictví, či zájmu o snadnější přístup k realizaci platebních operací ať aktivních, tak i pasivních. Z výše uvedeného grafu je patrné, že nejvyšší podíl zde tvoří respondenti spadající do příjmové kategorie 20 001,- až 35 000,- Kč hrubého měsíčně, což je kategorie, do které patří i průměrná měsíční mzda v ČR, jež činí 26 287,- Kč. (57) Další výraznou kategorií je skupina respondentů spadající do příjmové kategorie 10 001,- až 20 000,- hrubého měsíčně. Přibližně čtvrtina dotázaných uvedla rozmezí svých měsíčních příjmů mezi 0,- až 10 000,- Kč, přičemž naopak 10% dotázaných uvedlo své příjmy přesahující hranici 35 000,-.



Obrázek 26 – Banky respondentů (vlastní)

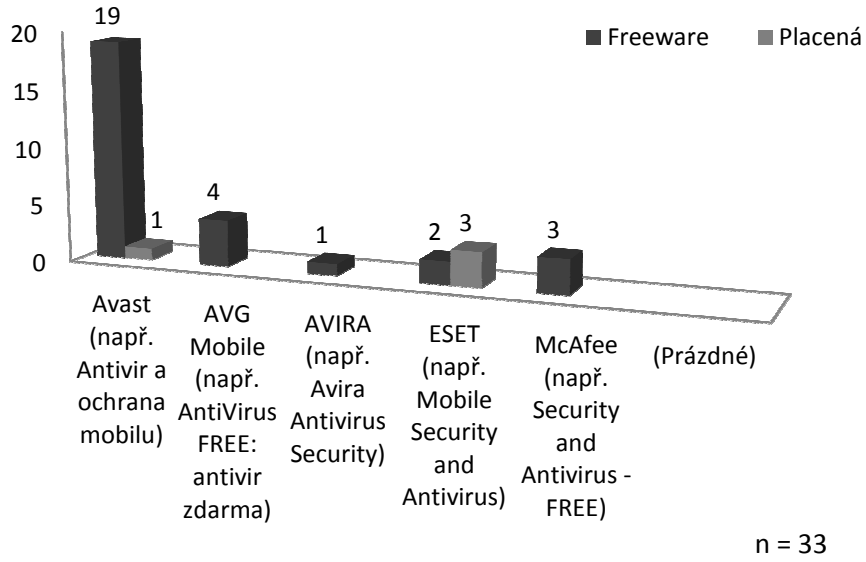
Vzhledem k zaměření další části práce, která je směřována k výběru tří finančních institucí, je rovněž vhodné uvést rozložení finančních institucí, u kterých respondenti spravují své finance. Nejvyšší četnost zde má zastoupení České spořitelny a dále Komerční banky. Třetí nejvyšší podíl zastává Air Bank. Mezi respondenty se rovněž vyskytli i příslušníci slovenské národnosti, jelikož své ojedinělé zastoupení zde má i VÚB či Tatrabanka.



Obrázek 27 – Zastoupení platforem zařízení respondentů (vlastní)

Mezi stěžejní parametr, který měl i vliv na průchod otázky dotazníku, je sledovaná platforma mobilního zařízení respondentů. V náhodném výběru respondentů se opět potvrdila dominance mobilní platformy Android OS, kterou na svém zařízení mělo 61 ze 101 dotázaných.

Dále bylo u uživatelů mobilní platformy sledováno, zdali na svém zařízení využívají antivirovou aplikaci, což potvrdilo 33 ze 61 uživatelů. V následujícím kontingenčním grafu je pro přehled uvedeno, od jakého vývojáře a o jakou licenci antivirové aplikace se jednalo. Naopak mezi uživateli, kteří antivirovou aplikaci nepoužívají, se nejčastěji vyskytovala odpověď, že to nepovažují za nezbytné a v sestupném pořadí dále uváděli, že je to případně nenapadlo či z obav ze zpomalení zařízení.



Obrázek 28 - Vývojáři a licence využívaných antivirových aplikací (vlastní)

6.2 Analýza závislosti kvalitativních znaků pomocí programu SAS

Kvůli určení závislosti kvalitativních znaků je nutné získaná data analyzovat za pomoci statistického programu SAS. V rámci provedených analýz bude určena přítomnost korelace mezi jednotlivými oblastmi, na které bylo zaměřeno dotazníkové šetření, a to konkrétně na datech získaných od 101 respondentů. V rámci tohoto postupu je vždy stanovena nulová hypotéza H0, jenž vychází ze skutečnosti, že testované znaky jsou na

sobě nezávislé. V opačném případě, kdy je potvrzena závislost kvalitativních znaků, je určena i případná síla dané závislosti.

6.2.1 Analýza vztahu využívání internetového bankovnictví a informovanosti o existenci smartbanking aplikace

První sledovanou oblastí je vztah respondentů k využívání běžného internetového bankovnictví a jejich informovanosti o existenci možnosti provádět platební operace za pomoci mobilní bankovní aplikace tzv. smartbanking. V rámci analýzy závislosti těchto kvalitativních znaků je nejprve nutné určit nulovou hypotézu H0.

H0: Ovlivní využívání internetového bankovnictví informovanost respondentů ohledně možnosti provádění platebních operací za pomoci mobilní bankovní aplikace? Existuje závislost mezi těmito znaky? Jak silná je případně síla závislosti? Nulová hypotéza vychází ze skutečnosti, že dané znaky na sobě jsou nezávislé.

Procedura FREQ

V rámci provedení analýzy závislosti kvalitativních znaků je nejprve nutné provést import získaných dat do statistického programu SAS. Po provedeném importu je možné nahlédnout na sledovaná data, včetně četností. Sloupec „Vyuzivani_IB“ představuje řádkovou proměnnou a sloupec „Znalost_smartbanking“, který vychází ze znalosti respondentů smartbanking aplikací, je zde proměnnou sloupcovou.

	Vyuzivani_IB	Znalost_smartbanking	pocet
1	ano	ano	58
2	ano	ne	29
3	ne	ano	5
4	ne	ne	9

Obrázek 29 - Zdroj dat pro SAS analýzu č. 1 (vlastní)

Zdrojová data byla v programu SAS uložena pod označení „vyuzivani“, přičemž pro získání vztahu mezi kvalitativními znaky je nutné zadat následující proceduru, která obsahuje dodatečné instrukce „norow nocol nopercent“, jež slouží k potlačení tisku řádkových, sloupcových a procentuálních četností.

```
proc freq data=vyuzivani;
tables vyuzivani_ib*znalost_smartbanking/norow nocol nopercent expected chisq measures exact;
weight pocet;
run;
```

Obrázek 30 - Procedura SAS pro analýzu č. 1 (vlastní)

V rámci získaného výstupu ze zadané procedury je možné vysledovat výpis řádkových a sloupcových proměnných, u kterých jsou dále zaznamenány očekávané a empirické četnosti. V tomto případě empirické četnosti, které jsou pro snazší orientaci ve výstupu označené „Frequency“, nabývají hodnot 58, 29, 5 a 9. Očekávané četnosti, které pro snazší orientaci nesou označení „Expected“, nabývají hodnot 54.267, 32.733, 8.7327 a 5.2673. Tyto hodnoty je nutné zohlednit vzhledem ke skutečnosti, že pokud by výše uvedená hypotéza H0 platila a mezi sledovanými znaky neexistovala závislost, tak ani v rámci těchto četností by neexistoval žádný statisticky významný rozdíl.

The SAS System

The FREQ Procedure

Frequency Expected	Table of Vyuzivani_IB by Znalost_smartbanking		
	Znalost_smartbanking(Znalost_smartbanking)		
Vyuzivani_IB(Vyuzivani_IB)	ano	ne	Total
ano	58 54.267	29 32.733	87
ne	5 8.7327	9 5.2673	14
Total	63	38	101

Obrázek 31 - Empirické a očekávané četnosti (vlastní)

Výše uvedené rozdělení četností skrývá další význam, a to ve skutečnosti, že má vliv na správný výběr testu. Z výše uvedeného obrázku je zcela patrné, že parametr na vyšší množství rozsahu výběru, než je souhrn očekávaných četností alespoň 20, byl splněn. Rovněž zde nenastala situace, kdy by jednotlivé očekávané četnosti byly menší než 5 ve více než 20% jednotlivých případech. Tato kritéria jsou stěžejní pro určení závislosti za pomoci tzv. Chí-kvadrát testu (χ^2).

Statistics for Table of Vyuzivani_IB by Znalost_smartbanking

Statistic	DF	Value	Prob
Chi-Square	1	4.9230	0.0265
Likelihood Ratio Chi-Square	1	4.7602	0.0291
Continuity Adj. Chi-Square	1	3.6925	0.0547
Mantel-Haenszel Chi-Square	1	4.8743	0.0273
Phi Coefficient		0.2208	
Contingency Coefficient		0.2156	
Cramer's V		0.2208	

Obrázek 32 - Výsledky Chí-kvadrát testu (vlastní)

Na základě uvedené p-hodnoty, která v tomto případě nabývá konkrétní hodnoty 0.0265, je možné určit, že na základě vztahu $p<0,05$ je nulová hypotéza H0 zamítnuta a mezi těmito znaky existuje závislost na hladině významnosti $\alpha = 5\%$.

Dále je na základě splnění podmínek pro Chí-kvadrát test a potvrzení závislosti sledovaných kvalitativních znaků možné určit sílu závislosti. Dle rozměru kontingenční tabulky 2x2 byl zvolen Phi koeficient, jelikož nebyla naplněna podmínka pro využití Cramerova koeficientu. Sílu závislosti dle tohoto koeficientu, který je uveden pod označením Phi Coefficient, je možné určit na základě jeho hodnoty 0.2208, což svědčí o výskytu nízké až střední závislosti mezi sledovanými veličinami, která je definována intervalem 0.10 až 0.29. Phi koeficient, který patří mezi nejkvalitnější Chí-kvadrátové míry závislosti, tedy potvrzuje střední závislost sledovaných znaků, konkrétně 22.08%.

6.2.2 Analýza vlivu informovanosti o smartbanking aplicích na zájem o provádění plateb za pomoci mobilní bankovní aplikace

Další sledovanou oblastí je určení vlivu informovanosti respondentů o smartbanking aplikacích na jejich zájem o provádění plateb za pomoci mobilního zařízení. V rámci analýzy závislosti těchto dvou kvalitativních znaků je nejprve nutné určit nulovou hypotézu H0. Tato závislost je sledována především na základě skutečnosti, že v dotazníkovém šetření uvedlo 63 respondentů, že vědí, k čemu slouží smartbanking

aplikace. Nicméně pouhých 50 respondentů uvedlo, že je zajímá možnost provádění plateb přes mobilní zařízení a výsledně pouze 26 respondentů aplikaci využívá. Pokud se zde projeví závislost těchto dvou kvalitativních znaků, tak je možné určit, že zájem o provádění plateb přes mobilní zařízení vychází ze znalosti smartbanking aplikace, kterou neznalo 38 ze 101 dotázaných.

H0: Ovlivní zájem o provádění platebních operací za pomoci mobilního zařízení informovanost respondentů o smartbanking aplikacích? Existuje závislost mezi těmito znaky? Jak silná je případná síla závislosti? Nulová hypotéza vychází ze skutečnosti, že dané znaky jsou na sobě nezávislé.

Procedura FREQ

Pro realizaci analýzy závislosti kvalitativních znaků je opět nutné provést import nasbíraných dat do statistického programu SAS. Po importu zdrojových dat je znovu k dispozici náhled dat s jejich četnostmi. Sloupec „Zajem_mobilni_platby“ v tomto případě představuje řádkovou proměnnou a sloupec „Znalost_smartbanking“, který představuje informovanost respondentů o smartbanking aplikacích, v tomto případě vyjadřuje sloupcovou proměnnou.

	Zajem_mobilni_platby	Znalost_smartbanking	pocet
1	ano	ano	39
2	ano	ne	11
3	ne	ano	24
4	ne	ne	27

Obrázek 33 - Zdroj dat pro SAS analýzu č. 2 (vlastní)

Zdrojová data byla následně pro práci s programem SAS uložena s názvem „znalost“, což je patrné i z následující procedury, která byla zadána pro získání vztahu mezi kvalitativními veličinami. Rovněž zde byly doplněny instrukce pro potlačení tisku řádkových, sloupcových a procentuálních četností.

```
proc freq data=znalost;
tables zajem_mobilni_platby*znalost_smartbanking/norow nocol nopercent expected chisq measures exact;
weight pocet;
run;
```

Obrázek 34 - Procedura SAS pro analýzu č. 2 (vlastní)

Po spuštění výše uvedené procedury je opět získána tabulka obsahující očekávané a empirické četnosti. Empirické četnosti v rámci této analýzy nabývají hodnot 39, 11, 24 a 27. Očekávané četnosti zde nabývají konkrétních hodnot 31.188, 18.812, 31.812 a 19.188. Opět je nutné uvést, že pokud by mezi sledovanými neexistovala závislost a potvrdila by se tak nulová hypotéza H0, tak ani mezi těmito četnostmi by neexistoval statisticky významný rozdíl.

The SAS System

The FREQ Procedure

Frequency Expected	Table of Zajem_mobilni_platby by Znalost_smartbanking		
	Znalost_smartbanking(Znalost_smartbanking)		
Zajem_mobilni_platby(Zajem_mobilni_platby)	ano	ne	Total
ano	39 31.188	11 18.812	50
ne	24 31.812	27 19.188	51
Total	63	38	101

Obrázek 35 - Empirické a očekávané četnosti (vlastní)

Na základě výše uvedeného výčtu četností je možné určit, že souhrn všech očekávaných četností je vyšší než 20 a zároveň se zde nevyskytuje nižší očekávaná četnost než 5, což svědčí o splnění podmínek pro použití Chí-kvadrát testu (χ^2).

Statistics for Table of Zajem_mobilni_platby by Znalost_smartbanking

Statistic	DF	Value	Prob
Chi-Square	1	10.2994	0.0013
Likelihood Ratio Chi-Square	1	10.5476	0.0012
Continuity Adj. Chi-Square	1	9.0231	0.0027
Mantel-Haenszel Chi-Square	1	10.1974	0.0014
Phi Coefficient		0.3193	
Contingency Coefficient		0.3042	
Cramer's V		0.3193	

Obrázek 36 - Výsledky Chí-kvadrát testu (vlastní)

Z výše uvedeného výstupu provedeného Chí-kvadrát testu je možné určit, že na základě p-hodnoty, která v tomto případě nabývá konkrétní hodnoty 0.0013, což splňuje požadavek z podmínky $p<0.05$, je nulová hypotéza H0 zamítnuta a mezi sledovanými kvalitativními znaky existuje závislost na hladině významnosti $\alpha = 5\%$.

Vzhledem k určení závislosti mezi těmito dvěma znaky je dále nutné určit sílu závislosti, která vychází z hodnoty uvedeného Phi koeficientu, jelikož nebyla splněna podmínka rozměru matice pro využití Cramerova koeficientu, jež v tomto případě nabývá stejné hodnoty 0.3193. V rámci vysledované závislosti je uvedená hodnota Phi koeficientu z intervalu 0.3 až 0.5, což svědčí o středně silné přímé závislosti mezi sledovanými hodnotami. Hodnota Phi koeficientu tedy určuje 31.93% závislost.

6.2.3 Vliv orientace respondentů v ICT na zájem o provádění platebních operací za pomoci mobilního zařízení

Třetí sledovanou oblastí je určení vlivu orientace respondentů v oblasti ICT na jejich zájem o provádění platebních operací za pomoci mobilních zařízení. V rámci analýzy závislosti těchto dvou kvalitativních znaků je opět nezbytné nejprve stanovit nulovou hypotézu H0. Závislost těchto dvou znaků je sledována především s ohledem na nejednoznačné informace kolující o bezpečnostních rizikách plynoucích z využívání mobilních zařízení. Pokud se závislost potvrdí, tak je možné určit, že důvod nízkého počtu využívání mobilní bankovní aplikaci přímo závisí na informační gramotnosti.

H0: Ovlivní úroveň orientace respondentů v oblasti ICT jejich zájem o provádění platebních operací za pomoci mobilního zařízení? Existuje závislost mezi těmito znaky? Jak silná je případně síla závislosti? Nulová hypotéza vychází ze skutečnosti, že sledované znaky jsou na sobě nezávislé.

Procedura FREQ

Před provedením analýzy závislosti kvalitativních znaků je nejprve nutné získaná data importovat do statistického programu SAS. Importovaná data je možné opět zobrazit

včetně jejich četností. První sloupec s označením „ICT_orientace“ představuje řádkovou proměnnou a druhý sloupec v pořadí, který nese označení „Zajem_mobilni_platby“ představuje proměnou sloupcovou.

	ICT_orientace	Zajem_mobilni_platby	pocet
1	Na profesionální úrovni (admin, programátor, správce sítě apod.),	ano	4
2	Odborný uživatel (Uživatel s určitou odbornou IT specializací.)	ano	10
3	Pokročilý uživatel	ano	20
4	Začátečník	ano	0
5	Základní uživatel	ano	16
6	Na profesionální úrovni (admin, programátor, správce sítě apod.),	ne	1
7	Odborný uživatel (Uživatel s určitou odbornou IT specializací.)	ne	5
8	Pokročilý uživatel	ne	18
9	Začátečník	ne	3
10	Základní uživatel	ne	24

Obrázek 37 - Zdroj dat pro SAS analýzu č. 3 (vlastní)

Zdrojová data byla po importu uložena pod označením „zajem“ s tím, že v rámci níže uvedené zadané procedury byl opět potlačen tisk řádkových, sloupcových a procentuálních četností za pomoci instrukcí „norow nocol nopercent“.

```
proc freq data=zajem;
tables ict_orientace*zajem_mobilni_platby/norow nocol nopercent expected chisq measures exact;
weight pocet;
run;
```

Obrázek 38 - Procedura SAS pro analýzu č. 3 (vlastní)

Po spuštění výše uvedené procedury je vyobrazen výpis řádkových a sloupcových proměnných s jejich očekávanými a empirickými četnostmi. Empirické četnosti v tomto případě nabývají hodnot 4, 1, 10, 5, 20, 18, 0, 3, 16 a 24. Očekávané hodnoty nabývají konkrétně hodnot 2.4752, 2.5248, 7.4257, 7.5743, 18.812, 19.188, 1.4851, 1.5149, 19.802 a 20.198. Pokud by se výše uvedená hypotéza H0 potvrdila, a mezi sledovanými kvalitativními znaky neexistovala závislost, tak by ani mezi těmito četnostmi neexistoval statisticky významný rozdíl.

The SAS System

The FREQ Procedure

Frequency Expected	Table of ICT_orientace by Zajem_mobilni_platby		
	Zajem_mobilni_platby(Zajem_mobilni_platby)		
ICT_orientace(ICT_orientace)	ano	ne	Total
Na profesionální úrovni (admin, programátor, správce sítě apod.).	4 2.4752	1 2.5248	5
Odborný uživatel (Uživatel s určitou odbornou IT specializací.)	10 7.4257	5 7.5743	15
Pokročilý uživatel	20 18.812	18 19.188	38
Začátečník	0 1.4851	3 1.5149	3
Základní uživatel	16 19.802	24 20.198	40
Total	50	51	101

Obrázek 39 - Empirické a očekávané četnosti (vlastní)

Na základě výše uvedeného rozsahu četností je možné určit, že pro tuto analýzu není možné použít Chí-kvadrát test (χ^2), jelikož sice byla splněna podmínka pro rozsah očekávaných četností větší než 20, avšak nebyla splněna podmínka nižšího než 20% výskytu očekávaných četnostní menších 5. V tomto případě je k hodnocení závislosti nutné využít Fisherův test.

Fisher's Exact Test	
Table Probability (P)	1.586E-04
Pr <= P	0.0919

Obrázek 40 - Výsledky Fisherova testu (vlastní)

Na základě výše uvedené p-hodnoty Fisherova testu, která konkrétně nabývá hodnoty 0.0919, je na základě vztahu $p<0.05$ možné určit, že nulová hypotéza H0 byla potvrzena a mezi sledovanými znaky neexistuje závislost na hladině významnosti $\alpha = 5\%$.

6.3 Vícekriteriální analýza variant

Druhá část analytického zpracování dat získaných z dotazníkového šetření je zaměřena na oblast nabízených funkcionalit mobilních bankovních aplikací, s ohledem na preference uživatelů jak dané banky, tak i v souhrnném pohledu. Konkrétní řešení je cíleno na získání přehledu o prioritách uživatelů mezi nabízenými funkcionalitami a případný vliv jejich absence v dané bankovní aplikaci. Rovněž je v rámci této části práce určen normalizovaný přínos pro uživatele, na základě kterého je určeno pořadí aplikací dle maximalizačního kritéria.

Pro zápis hodnocených variant je využitá kriteriální matice, jejíž sloupce udávají hodnocení *p*-tého kritéria a řádky *n*-té varianty, které jsou mezi sebou srovnávány. Kompletní množina všech variant je následně označena A = {a1, a2, … an}.

$$\mathbf{Y} = \begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1p} \\ y_{21} & y_{22} & \cdots & y_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n1} & y_{n2} & \cdots & y_{np} \end{pmatrix}$$

Obrázek 41 - Kriteriální matice (58)

Stanovení vah nabízených funkcionalit vychází z dotazníkového šetření, v rámci kterého respondenti určovali na maximalizační bodové škále 1 až 5 své preference u jednotlivých funkcí. Z těchto výpovědí byla získána data o uživatelských preferencích, ze kterých byla v případě filtrace respondentů jednotlivých bank a následným provedením skalárního součinu četností pro naměřené hodnoty preferencí, jejichž souhrnným součtem byly děleny jednotlivé hodnoty vypočtené skalárním součinem za jednotlivá kritéria, získána informace o vahách pro jednotlivé oblasti dle uživatelů dané finanční instituce.

V případě aplikování stejného postupu na celý soubor získaných dat bylo umožněno získat informace o vahách souhrnně za všechny respondenty. Získané hodnoty

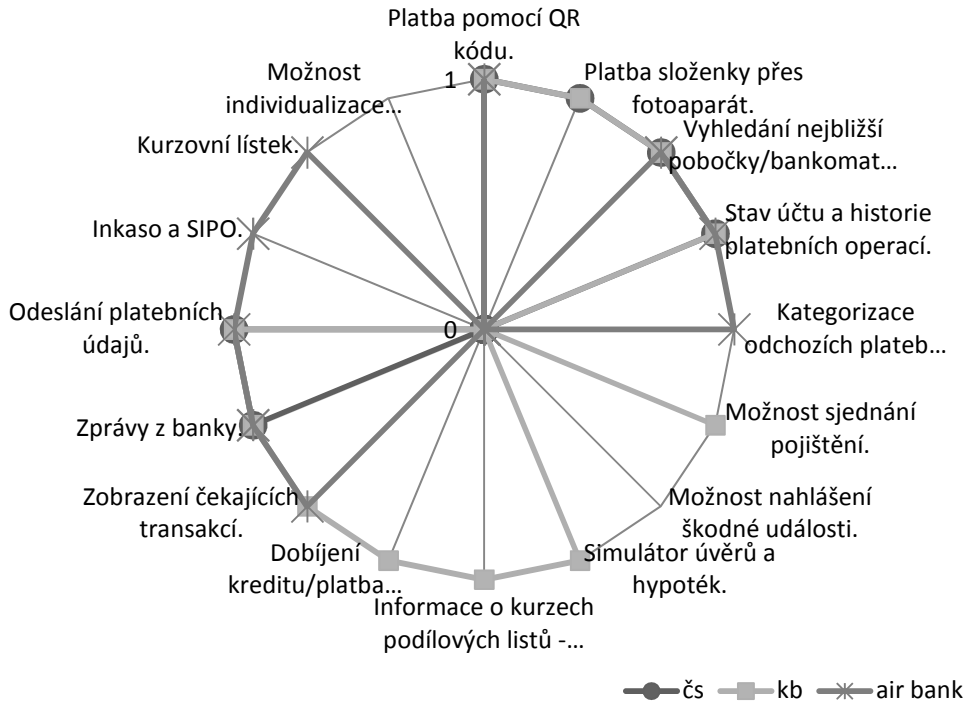
vah poté byly zaneseny do vektoru, jenž byl násoben maticí výskytu nabízených funkcí u jednotlivých finančních institucí, které jsou souhrnně uvedené v následující tabulce 6. V této tabulce jsou přidány 2 funkce, kterými dané aplikace nedisponují, avšak autor práce je považoval za zajímavé. Konkrétně se jedná o možnost nahlášení škodné události a možnost individualizace aplikace.

Tabulka 6 - Funkcionality vybraných smartbanking aplikací (vlastní)

Funkce/Banka	ČS	KB	Air Bank
Platba pomocí QR kódu.	ano	ano	ano
Platba složenky přes fotoaparát.	ano	ano	ne
Vyhledání nejbližší pobočky/bankomatu (popř. s naplánováním trasy).	ano	ano	ano
Stav účtu a historie platebních operací.	ano	ano	ano
Kategorizace odchozích plateb pro vedení osobního účetnictví.	ne	ne	ano
Možnost sjednání pojištění.	ne	ano	ne
Možnost nahlášení škodné události.	ne	ne	ne
Simulátor úvěrů a hypoték.	ne	ano	ne
Informace o kurzech podílových listů - IKS, AMUNDI.	ne	ano	ne
Dobíjení kreditu/platba faktur za telefon.	ne	ano	ne
Zobrazení čekajících transakcí.	ne	ano	ano
Zprávy z banky.	ano	ano	ano
Odeslání platebních údajů.	ano	ano	ano
Inkaso a SIPO.	ne	ne	ano
Kurzovní lístek.	ne	ne	ano
Možnost individualizace aplikace.	ne	ne	ne

Vzhledem k povaze výchozí matice výskytu nabízených funkcí, jež je transponovanou podobou tabulky 6, by hledání ideální a bazální varianty postrádalo smysl, jelikož jsou zde pouze logické hodnoty „ano“ a „ne“. Na tyto hodnoty byla v rámci dané matice aplikována bodovací metoda, která v případě výskytu dané funkcionality má přidělenu hodnotu 1, takže dostupnost či nedostupnost funkcionalit reprezentují hodnoty 1 a 0, což zároveň splňuje požadavky na maximalizaci kritérií. Nicméně z pohledu na dilema rozhodování uživatele, jakou bankovní aplikaci zvolit pouze na základě nabízených funkcí, je vhodné provést analýzu dominance podle stavu okolností, která vychází z jednotlivých řešení.

Jak je již z tabulky 6 patrné, tak žádná z variant není dominující, ani dominovaná, jelikož sice bylo splněno maximalizační kritérium, avšak žádná z variant a_1 až a_3 nesplňuje požadavek na dominanci $y_{i1} > y_{j1}$ alespoň jednoho z kritérií k_1 až k_{16}, za splnění podmínky $(y_{i1}, y_{i2}…., y_{ip}) \geq (y_{j1}, y_{j2}, …., y_{jp})$. (58) Skutečnost, že žádná z variant není dominující, je rovněž možné ověřit na grafickém znázornění níže.



Obrázek 42 – Dominance mezi nabízenými funkcemi (vlastní)

Dále byl realizován krok, kdy na základě skalárního součinu vypočteného vektoru vah od všech respondentů a matice výskytu nabízených funkcí, byl vypočten normalizovaný přínos pro uživatele jednotlivých variant.

Při využití vypočtených vah od všech respondentů a následném vynásobení tohoto vektoru s maticí výskytu nabízených funkcí je nutné vzít v potaz skutečnost, že vypočtený normalizovaný přínos pro uživatele by se mohl odvíjet od počtu nabízených funkcionalit, nicméně stále s ohledem na vliv uživatelských preferencí, které jsou pro výsledný přínos

rozhodující. Pro lepší přehlednost, vzhledem k počtu sledovaných kritérií, je tabulka vložena v transponované podobě. Přidané funkcionality možnost nahlášení škodné události a možnost individualizace aplikace zde mají hodnoty vah 0,061771058 a 0,073218143.

Tabulka 7 – Váhy jednotlivých kritérií dle všech respondentů (vlastní)

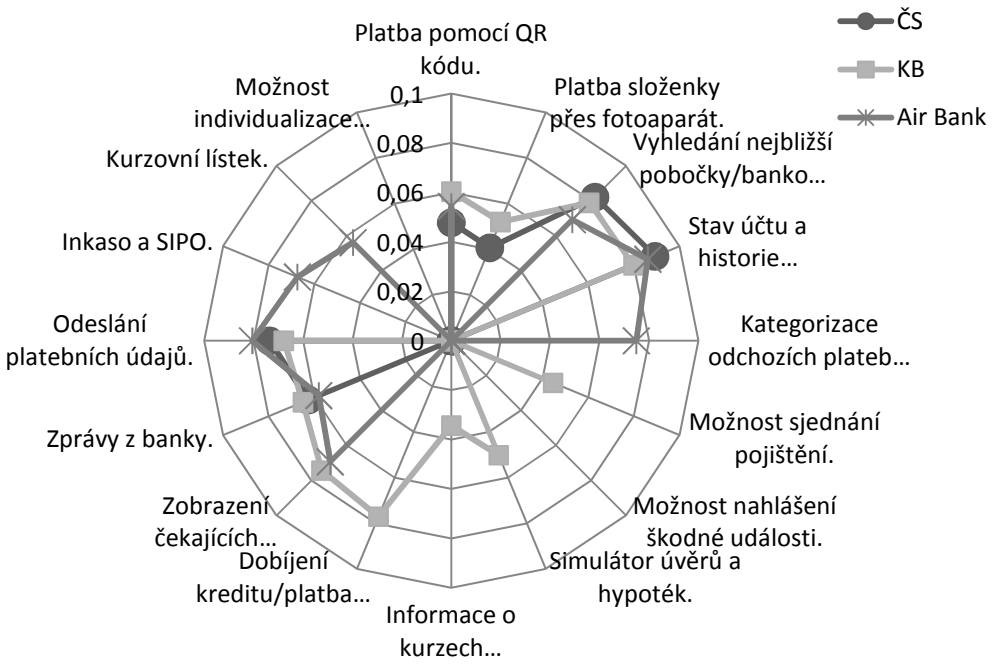
Funkce/Banka	ČS	KB	Air Bank
Platba pomocí QR kódu.	0,0594	0,0594	0,0594
Platba složenky přes fotoaparát.	0,05184	0,05184	0
Vyhledání nejbližší pobočky/bankomatu (popř. s naplánováním trasy).	0,07862	0,07862	0,07862
Stav účtu a historie platebních operací.	0,08445	0,08445	0,08445
Kategorizace odchozích plateb pro vedení osobního účetnictví.	0	0	0,06998
Možnost sjednání pojištění.	0	0,04557	0
Možnost nahlášení škodné události.	0	0	0
Simulátor úvěrů a hypoték.	0	0,04795	0
Informace o kurzech podílových listů - IKS, AMUNDI.	0	0,03823	0
Dobíjení kreditu/platba faktur za telefon.	0	0,073	0
Zobrazení čekajících transakcí.	0	0,06803	0,06803
Zprávy z banky.	0,06091	0,06091	0,06091
Odeslání platebních údajů.	0,07257	0,07257	0,07257
Inkaso a SIPO.	0	0	0,06436
Kurzovní lístek.	0	0	0,05011
Možnost individualizace aplikace.	0	0	0
Normalizovaný přínos pro uživatele	**0,40778**	**0,68056**	**0,60842**

Na základě provedených výpočtů je možné určit pořadí bankovních aplikací na základě výše normalizovaného přínosu pro uživatele dle maximalizačního kritéria, který je v tomto případě značen $u(a_i)$.

$$u(a_i) = \begin{matrix} \check{C}S \\ Air\ Bank \\ KB \end{matrix} \begin{pmatrix} \mathbf{0,40778} \\ \mathbf{0,60842} \\ \mathbf{0,68056} \end{pmatrix}$$

6.3.1 Dle preferencí jednotlivých uživatelských skupin a dostupných funkcionalit

Na základě zjištění, že mezi sledovanými variantami není dominované řešení, by bylo možné hledat variantu kompromisní, nicméně autor práce upřednostnil alternativu, kdy byl opakován stejný postup jako v předchozím případě, avšak s využitím vypočtených vah dle jednotlivých skupin respondentů založených na skutečnosti, které finanční instituce jsou klienty. Vypočtené váhy byly do kriteriální matice, jež je pro lepší přehlednost zobrazena v transponované podobě, opět zadány vynásobením vypočtených vektorů vah za jednotlivé skupiny uživatelů s maticí výskytu nabízených funkcí. Následně byl určen i normalizovaný přínos pro uživatele dle jednotlivých variant.



Obrázek 43 - Dominance dle uživatelských skupin a nabízených funkcí (vlastní)

Rovněž je možné uvést, že žádná varianta není dominující dle stavu okolností a vyskytují se zde pouze varianty nedominované.

Tabulka 8 - Preference dle klientů dané banky (vlastní)

Funkce/Banka	ČS	KB	Air Bank
Platba pomocí QR kódu.	0,04777	0,06035	0,05431
Platba složenky přes fotoaparát.	0,04072	0,052	0
Vyhledání nejbližší pobočky/bankomatu (popř. s naplánováním trasy).	0,08222	0,07892	0,06929
Stav účtu a historie platebních operací.	0,08927	0,07985	0,08614
Kategorizace odchozích plateb pro vedení osobního účetnictví.	0	0	0,07491
Možnost sjednání pojištění.	0	0,04457	0
Možnost nahlášení škodné události.	0	0	0
Simulátor úvěrů a hypoték.	0	0,05014	0
Informace o kurzech podílových listů - IKS, AMUNDI.	0	0,03435	0
Dobíjení kreditu/platba faktur za telefon.	0	0,07707	0
Zobrazení čekajících transakcí.	0	0,07428	0,06929
Zprávy z banky.	0,06265	0,065	0,05805
Odeslání platebních údajů.	0,07361	0,06778	0,08052
Inkaso a SIPO.	0	0	0,06742
Kurzovní lístek.	0	0	0,05618
Možnost individualizace aplikace.	0	0	0
Normalizovaný přínos pro uživatele	**0,39624**	**0,68431**	**0,6161**

Na základě realizovaného postupu je opět možné určit přínos pro uživatele dle jednotlivých variant. Při využití vah vycházejících z preferencí jednotlivých skupin došlo ke změnám hodnot přínosu pro uživatele, avšak pořadí bankovních aplikací se nezměnilo.

$$u(ai) = \begin{matrix} \check{C}S \\ Air\ Bank \\ KB \end{matrix} \begin{pmatrix} \mathbf{0,39624} \\ \mathbf{0,6161} \\ \mathbf{0,68431} \end{pmatrix}$$

6.3.2 Dle preferencí jednotlivých uživatelských skupin a všech funkcionalit

Na základě zjištění, že mezi referenčními skupinami se nevyskytovalo dominující řešení, byl celý postup opakován, avšak se změnou, v rámci které by dané finanční instituce pouze v hypotetické rovině nabízely veškeré sledované funkcionality, takže každá

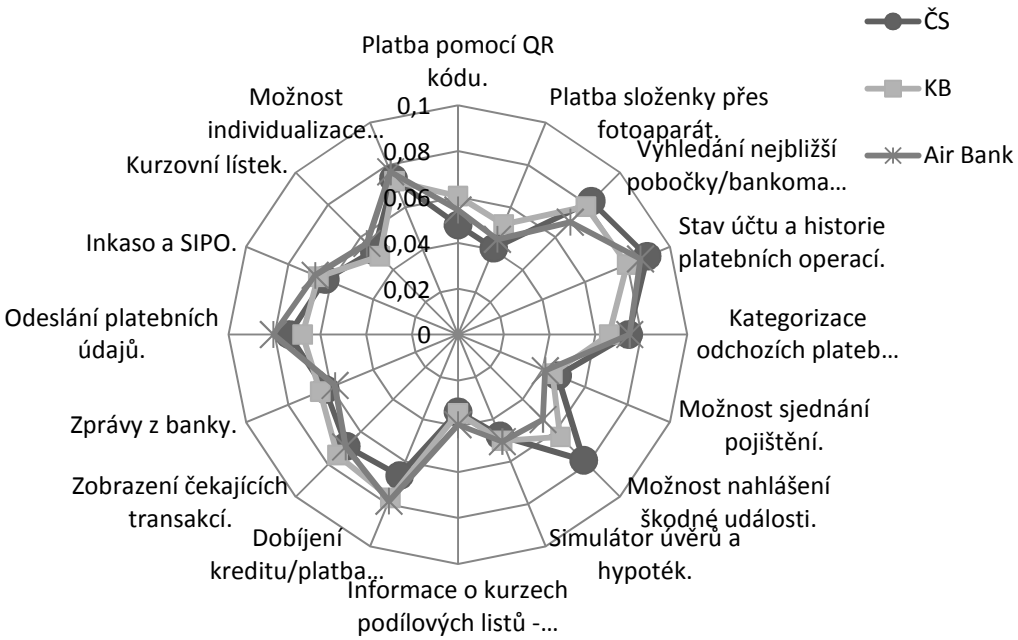
varianta matice výskytu nabízených funkcí má k dispozici bodovou hodnotu 1 pro každé kritérium. Váhy pro jednotlivá kritéria však stále vychází z preferencí jednotlivých uživatelských skupin. Tento postup sice nepřinese informaci o normalizovaném přínosu pro uživatele, jelikož při sledování všech kritérií je jeho hodnota naplněna do maximální úrovně, kterou vyjadřuje horní mez intervalu pro normalizovaný přínos od 0 do 1, konkrétně tedy 1. Účelem této analýzy je určit, jak rozdílné jsou postoje jednotlivých uživatelských skupin bez ohledu na to, zdali jejich banka danou funkci nabízí, či nikoliv. Kriteriální matice je opět kvůli přehlednosti uvedena v transponované podobě.

Tabulka 9 - Celkové preference dle uživatelských skupin (vlastní)

Funkce/Banka	ČS	KB	Air Bank
Platba pomocí QR kódu.	0,04777	0,06035	0,05431
Platba složenky přes fotoaparát.	0,04072	0,052	0,04494
Vyhledání nejbližší pobočky/bankomatu (popř. s naplánováním trasy).	0,08222	0,07892	0,06929
Stav účtu a historie platebních operací.	0,08927	0,07985	0,08614
Kategorizace odchozích plateb pro vedení osobního účetnictví.	0,07439	0,06592	0,07491
Možnost sjednání pojištění.	0,04699	0,04457	0,0412
Možnost nahlášení škodné události.	0,07753	0,06314	0,05243
Simulátor úvěrů a hypoték.	0,04777	0,05014	0,05056
Informace o kurzech podílových listů - IKS, AMUNDI.	0,03367	0,03435	0,03933
Dobíjení kreditu/platba faktur za telefon.	0,06656	0,07707	0,07865
Zobrazení čekajících transakcí.	0,06891	0,07428	0,06929
Zprávy z banky.	0,06265	0,065	0,05805
Odeslání platebních údajů.	0,07361	0,06778	0,08052
Inkaso a SIPO.	0,06265	0,06592	0,06742
Kurzovní lístek.	0,05168	0,04828	0,05618
Možnost individualizace aplikace.	0,07361	0,07242	0,07678

Následně by byla opět primárně hledána přítomnost dominovaného řešení, což však není možné, jelikož součet všech preferencí udává horní hranici naplnění přínosu pro uživatele, tedy 1. Tuto skutečnost je možné pozorovat i z grafu níže a dále vzhledem ke skutečnosti, že žádná varianta tuto hranici nepřekračuje. Nicméně na tomto grafu je patrné, že se uživatelské preference nabízených funkcí nijak zásadně na základě jejich banky

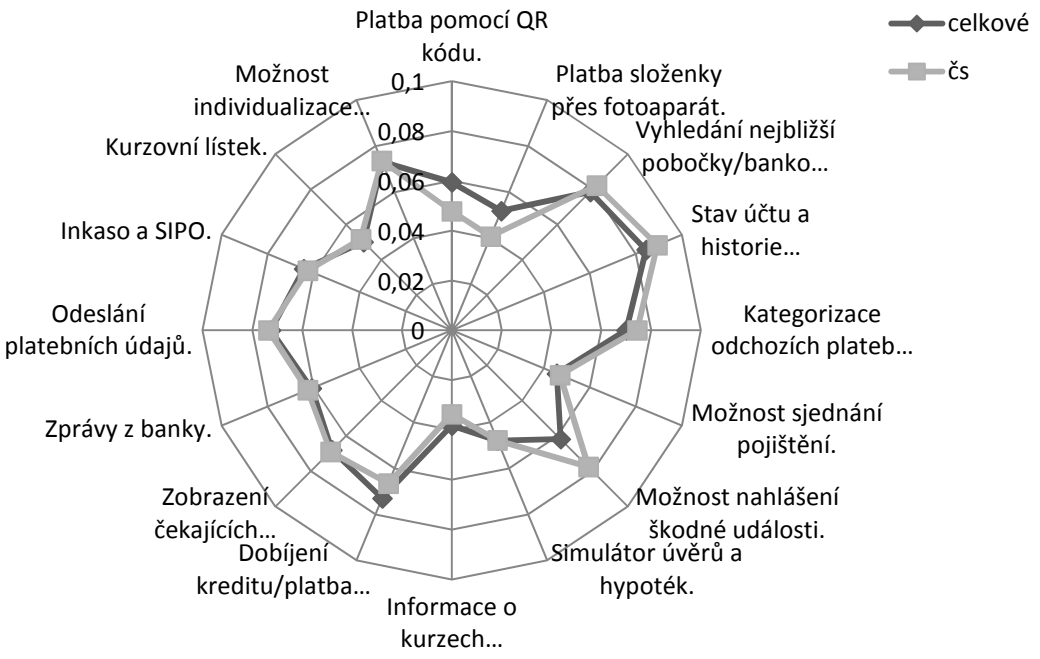
neliší, avšak vzhledem k jejich rozložení není možné případně přímo určit kompromisní variantu.



Obrázek 44 - Dominance dle uživatelských skupin a všech funkcí (vlastní)

6.3.3 Preference dle uživatelů České spořitelny

Pro lepší přehled o postojích uživatelských skupin k jednotlivým funkcionalitám jsou uvedeny získané výstupy vyobrazením rozdílů mezi vahami vypočtenými dle preferencí všech respondentů a vahami vypočtenými dle preferencí jednotlivých uživatelských skupin, v tomto případě konkrétně uživatelů České spořitelny.

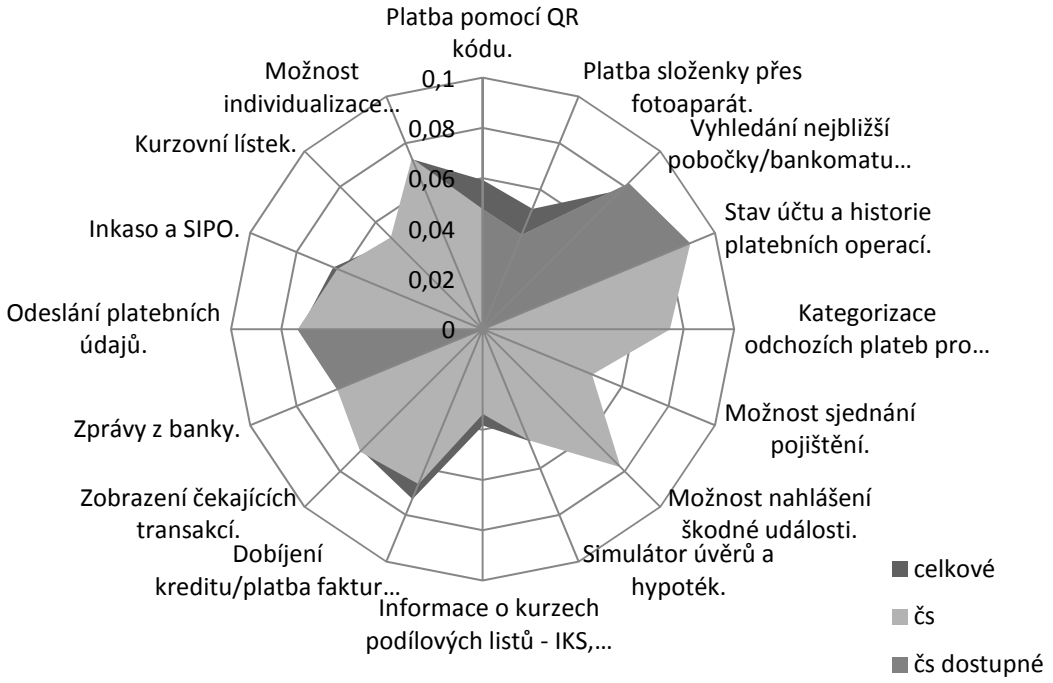


Obrázek 45 – Váhy funkcionalit dle preferencí uživatelů České spořitelny (vlastní)

K získání lepší představy o rezervách mezi dostupnými funkcemi daných bankovních aplikací, vzhledem k přínosu pro uživatele, slouží následující graf, kde nejnižší vrstvu tvoří váhy kritérií vypočtené z preferencí všech respondentů, jelikož jejich nižší preference nemá vliv na konkrétní uživatelskou skupinu, takže je tato varianta skryta pod množinou vypočtených vah kritérií z preferencí uživatelů České spořitelny. Pokud však některé z vah kritérií vypočtených na základě preferencí všech respondentů přesáhnou hranici stanovenou uživateli České spořitelny, čímž jeho zobrazení přesáhne prostřední vrstvu, tak lze následně určit, které z nabízených funkcí nejsou pro uživatele České spořitelny, na rozdíl od celkového pohledu, tak podstatné. Nejvyšší vrstvu tvoří váhy kritérií vypočtené na základě preferencí uživatelů České spořitelny, avšak s ohledem na dostupné funkce v aplikaci Servis 24.

Z tohoto grafu je zcela patrné, že z nabízených funkcí uživatelská skupina České spořitelny dává nižší kriteriální váhu platbě pomoci QR kódu a platbě složenky přes fotoaparát oproti vypočteným vahám kritérií z preferencí všech respondentů. Naopak mezi funkcemi, které v aplikaci chybí, by uživatelé do nejvyšší míry uvítali možnost nahlášení

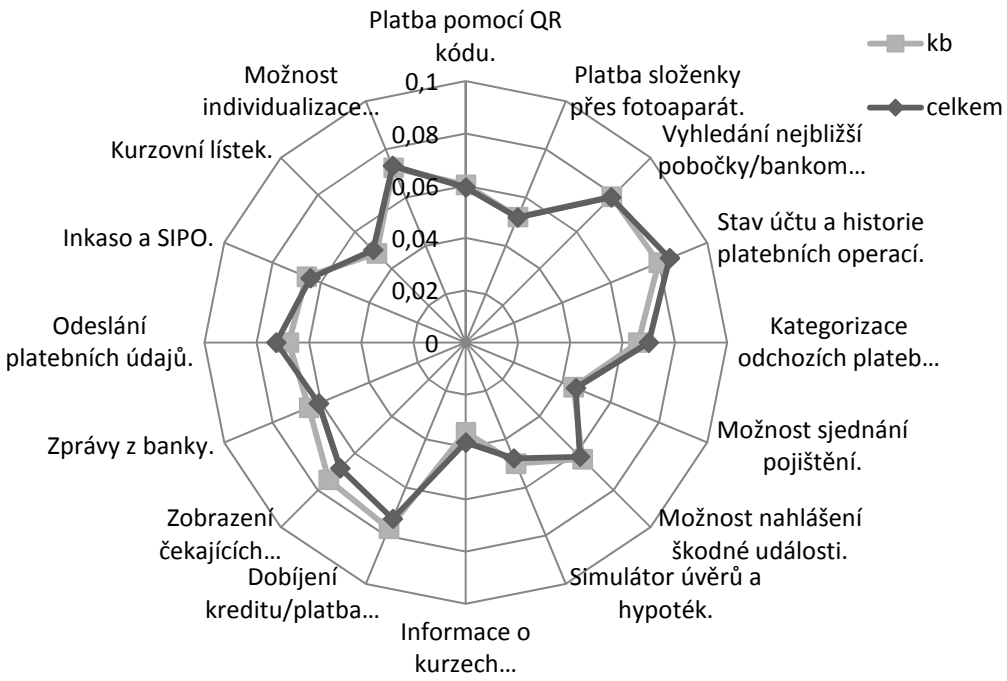
škodné události, kategorizace plateb pro vedení osobního účetnictví, možnost individualizace aplikace a zobrazení čekajících transakcí.



Obrázek 46 - Rezervy nabízených funkcionalit dle skupiny uživatelů České spořitelny (vlastní)

6.3.4 Preference dle uživatelů Komerční banky

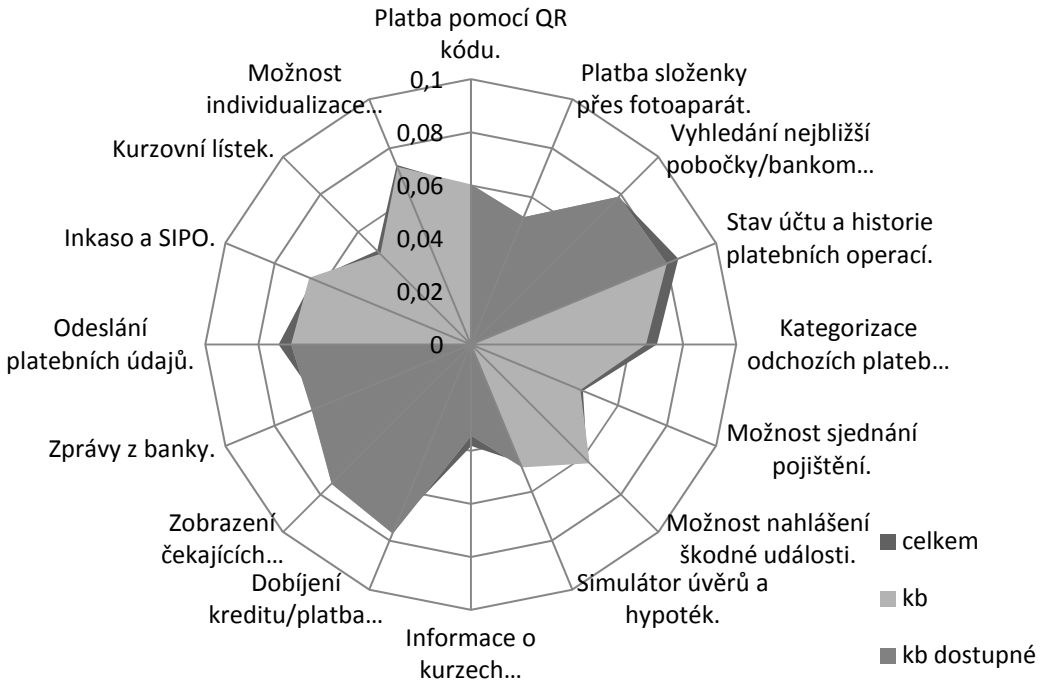
Dalším srovnáním je výčet vah vypočtených z preferencí všech respondentů vůči vahám kritérií vypočteným z preferencí skupiny uživatelů Komerční banky. Z následujícího grafu je patrné, že rozložení jednotlivých vah z preferencí uživatelů Komerční banky se natolik neliší od vah kritérií určených z preferencí všech respondentů, jako tomu bylo u České spořitelny.



Obrázek 47 - Váhy funkcionalit dle preferencí uživatelů Komerční banky (vlastní)

K získání lepší představy o rezervách mezi dostupnými funkcemi bankovní aplikace Komerční banky a vahách kritérií určených z preferencí skupiny uživatelů této banky slouží následující graf, kde nejnižší vrstvu tvoří váhy kritérií vypočtené z preferencí všech respondentů, prostřední vrstvu tvoří váhy kritérií vypočtené z preferencí uživatelů Komerční banky a nevyšší vrstvu tvoří váhy kritérií vypočtené z preferencí uživatelů Komerční banky, avšak s ohledem na dostupné funkce v aplikaci Mobilní banka 2.

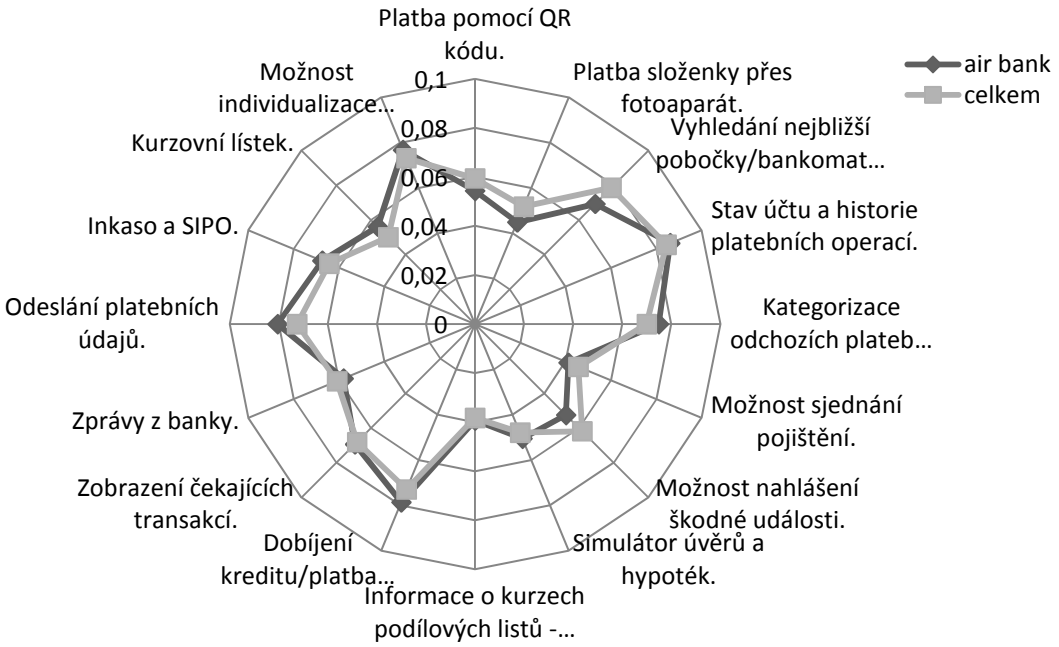
Z následujícího grafu je patrné, že bankovní aplikace Mobilní Banka 2 od Komerční banky disponuje rozsáhlejším množstvím funkcí, než aplikace Servis 24 a celkově jsou tak váhy určené z preferencí uživatelů Komerční banky oproti vahám kritérií vypočteným z preferencí všech respondentů nižší v oblasti odesílání platebních údajů a zobrazení stavu účtu s historií platebních operací. Naopak jisté rezervy v absenci dostupných funkcí jsou v rámci vah z preferencí uživatelů Komerční banky patrné především u možnosti individualizace aplikace, kategorizaci plateb pro vedení osobního účetnictví, inkasa a SIPO a možnosti nahlášení škodné události.



Obrázek 48 - Rezervy nabízených funkcionalit dle preferencí uživatelů Komerční banky (vlastní)

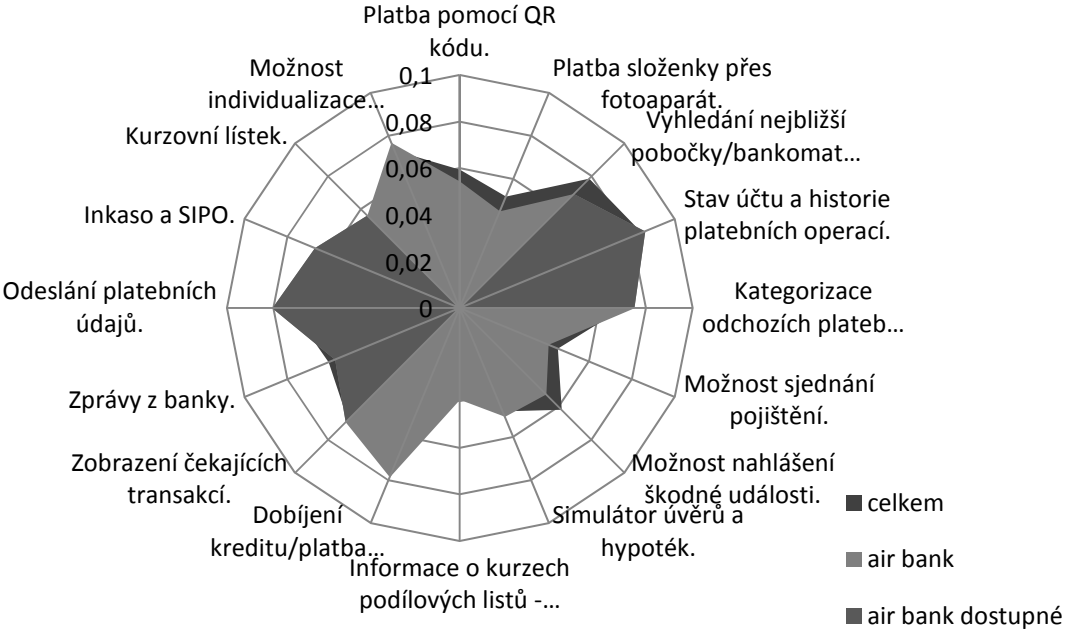
6.3.5 Preference dle uživatelů Air Bank

Posledním ve srovnání jsou váhy kritérií vypočtené z preferencí skupiny uživatelů Air Bank, kde mobilní bankovní aplikace Mobilní Bankovnictví Air Bank nedisponuje tolika funkcemi, jako aplikace Komerční banky, avšak nabízí jich více, než aplikace České spořitelny. Na následujícím grafu jsou patrné nejpodstatnější rozestupy mezi vahami kritérií určenými z preferencí všech uživatelů a vahami kritérií vypočtenými z preferencí uživatelské skupiny Air Bank. Nicméně rozestupy nejsou tak podstatné co do jejich výše, jako tomu bylo u České spořitelny, ale z hlediska jejich četnosti.



Obrázek 49 - Váhy funkcionalit dle preferencí uživatelů Air Bank (vlastní)

Mezi respondenty uživatelské skupiny Air Bank jsou podstatně nižší kriteriální váhy pro oblasti vyhledání nejbližší pobočky/bankomatu či v zájmu o zobrazení zpráv z banky. Naopak dle vah stanovených z preferencí uživatelské skupiny Air Bank jsou zcela patrné rezervy v absenci možnosti dobíjení kreditu či provedení platby faktur za telefon, v možnosti individualizace aplikace, možnost nahlášení škodné události a platbě složenky přes fotoaparát.



Obrázek 50 - Rezervy nabízených funkcionalit dle preferencí uživatelů Air Bank (vlastní)

7. Diskuse výsledků

7.1.1 Diskuse výsledků analýz závislosti kvalitativních znaků

V rámci provedených analýz závislosti kvalitativních znaků byla doložena závislost kvalitativních znaků mezi zájmem uživatelů o provádění plateb za pomoci mobilního zařízení vzhledem k znalosti pojmu smartbanking. Z doložené nízké až středně silné závislosti těchto dvou kvalitativních znaků vyplývá, že zájem o mobilní platby je přímo závislý na znalosti mobilních bankovních aplikací. Na základě tohoto výstupu je možné určit, že zvýšení počtu uživatelů těchto aplikací je závislé na jejich dostatečné propagaci, která dle vlastního dlouhodobého pozorování autora práce není příliš rozmanitá, přičemž i případné informační materiály přímo na pobočkách banky rovněž zpravidla nejsou příliš vhodně umístěny.

Další analyzovaná závislost kvalitativních znaků byla doložena na středně silné až podstatné úrovni u vlivu využívání internetového bankovnictví na znalost pojmu smartbanking. Z tohoto vztahu je tedy zcela patrné, že pokud zájem o provádění plateb za pomoci mobilního zařízení závisí na znalosti těchto aplikací a následně znalost těchto aplikací se odvíjí od využívání internetového bankovnictví, tak je vhodné růst uživatelské základny cílit na propagaci přes internetové bankovnictví, což je i celkem logickým krokem, jelikož uživatelé internetového bankovnictví, kteří aplikace neignorují z případného konzervativnějšího přístupu, jsou stěžejní cílovou uživatelskou skupinou pro mobilní bankovní aplikace.

Nejen slabá propagace je příčinou relativně nízkého počtu uživatelů mobilních bankovních aplikací, jelikož méně než polovina respondentů, kteří již pojem smartbanking znají, tuto aplikaci aktivně využívají. Jedním z teoretických předpokladů je nízká informační gramotnost a z toho plynoucí obavy z případných bezpečnostních rizik. Z tohoto důvodu byla sledována další závislost, a to konkrétně vlivu orientace respondentů v oblasti ICT na zájem o provádění platebních operací za pomoci mobilního zařízení. Výsledně se však v provedené analýze závislost těchto dvou kvalitativních znaků nepotvrdila, což naopak podporuje tvrzení autora této práce o nejednoznačné,

kontroverzní, pomalu až zavádějící povaze předávaných informací o bezpečnostních rizikách platformy Android OS.

7.1.2 Diskuse výsledků vícekriteriální analýzy variant

V rámci vícekriteriální analýzy variant byly určeny váhy kritérií z preferencí uživatelů pro jednotlivé funkcionality, které jak z celkového pohledu, tak i v rámci uživatelských skupin nevykazovaly žádné extrémní výchylky a je možné určit, že postoje uživatelů vůči nabízeným funkcionalitám jsou si velmi blízké. Rovněž se z obou provedených výpočtů normalizovaných přínosů pro uživatele potvrdilo pořadí, v rámci kterého nejvyšší přínos udává Mobilní banka 2 od Komerční banky, následně v druhém pořadí se v obou případech vyskytla aplikace Mobilní bankovnictví Air Bank a na třetím místě aplikace Servis 24 od České spořitelny. Tato skutečnost opět potvrzuje předpoklad autora práce, že absence dostupných funkcionalit v mobilní bankovní aplikaci má přímý vliv na normalizovaný přínos pro jejich uživatele. Konkrétní chybějící funkcionality jsou uvedeny v sestupném pořadí dle důležitosti:

Česká spořitelna: možnost nahlášení škodné události, kategorizace plateb pro vedení osobního účetnictví, možnost individualizace aplikace a zobrazení čekajících transakcí.

Komerční banka: možnosti individualizace aplikace, kategorizaci plateb pro vedení osobního účetnictví, inkasa a SIPO a možnosti nahlášení škodné události.

Air Bank: možnosti individualizace aplikace, možnost nahlášení škodné události a platbě složenky přes fotoaparát.

Vzhledem k tomu, že se nejedná o běžný konfesní software a s odkazem na skutečnost, jak jsou obecně aplikace pro Android OS vyvíjeny, není úprava aplikace či přidání funkcionalit problematikou absence technického řešení, ale spíše otázkou postoje dané finanční instituce, která by byla nucena investovat do vývoje. V pohledu na vybrané finanční instituce by investice do vývoje neměla být hlavní překážkou, jelikož v případě jejich zařazení do velké zahraniční skupiny, by investice do vývoje nebyla vztažena pouze pro uživatele ČR, ale po vytvoření dalších knihoven lokálních jazykových mutací, by byla použitelná i pro další státy.

8. Závěr

V souhrnném pohledu je možno říci, že využívání mobilních bankovních aplikací je dle informací o aktuálním počtu uživatelů a objemu prováděných finančních transakcí uvedených v kapitole 3.4 na vzestupu, avšak vzhledem ke konzervativnějším postojům uživatelů je potřeba tento trend podpořit. Dále je možné určit, že na základě využívání mobilního zařízení ke správě finančních prostředků se následně logicky mění i postoje a návyky uživatelů. Nejen totiž s odkazem na tuto kapitolu, ale i v rámci analytické části práce bylo v kapitole 6.3.1 prokázáno, že pro uživatele je dle nejvyšší vypočtené preference velmi podstatná možnost sledovat zůstatky a zobrazit si historii platebních operací. Tato skutečnost je v praxi podložena častějším přístupem do mobilní bankovní aplikace, než tomu bylo u běžného internetového bankovnictví. Se změnou návyků uživatele je rovněž možné očekávat i vyšší požadavky na nabízené funkce a služby v mobilních bankovních aplikacích, přičemž tento předpoklad byl zároveň potvrzen i v rámci vypočtených normalizovaných přínosů pro uživatele z vícekriteriálních analýz variant v kapitolách 6.3 a 6.3.1.

Prostor pro rozšíření řad uživatelů se tedy otevírá v samotných možnostech mobilních bankovních aplikací. Mezi sledované preference funkcionalit tak byly autorem práce přidány 2 funkcionality.

V prvním případě se jednalo o možnost nahlášení škodné události. Vzhledem ke skutečnosti, že aplikace Komerční banky nabízí možnost sjednání pojištění, se na základě nabízených služeb možnost nahlášení škodné události autorovi práce jeví logickým požadavkem. Tato funkce se dle vah kritérií určených z preferencí respondentů pohybovala v blízkosti aritmetického průměru všech vah, takže je možné hovořit o prakticky neutrálním postoji všech respondentů vůči její absenci, což má střední vliv na normalizovaný přínos pro uživatele.

Druhá přidaná funkcionalita, kterou byla možnost individualizace bankovní aplikace, dle vah kritérií stanovených z preferencí všech uživatelů, jež jsou uvedeny

v kapitole 6.3, získala stěžejnější třetí místo ze všech sledovaných funkcionalit. Její absence tedy má velmi silný vliv na normalizovaný přínos pro uživatele.

Rovněž by se jejím přidáním vyřešil i případný problém s přehledností aplikace po přidání dalších funkcí, jelikož by si uživatel mohl v ideálním případě sám navolit, které funkce se mu zobrazí. Aplikace by tak nativně obsahovala veškeré funkcionality a individualizace by spočívala pouze v jejich zobrazování. Případně se zde nabízí alternativa v podobně možnosti uspořádat si funkce do pořadí dle individuálních potřeb uživatele, který by tak měl v horní části aplikace k dispozici jen ty funkce, jež jsou pro něj rozhodující. Tato úprava by mohla být například řešena za pomoci funkce drag and drop.

Návrhem na rozšíření počtu uživatelů s ohledem na oblast bezpečnostních rizik, která dle autora práce má s touto problematikou přímou souvislost, tkví především v určitých komunikačních bariérách, problematice informační gramotnosti a případně konzervativním přístupu uživatelů. Řešení se zde otevírá na straně finančních institucí, jelikož očekávání, že uživatelé budou aktivně prohlubovat svoji informační gramotnost, není příliš reálná. Ideální formou je začít u předávání informací, kdy v případě prokázané závislosti kvalitativních znaků u zájmu o provádění platebních operací za pomoci mobilního zařízení vůči využívání internetového bankovnictví řešené v kapitole 6.2.1, by mohlo dojít k umístění informačního banneru přímo do dané webové bankovní aplikace s tím, že by se uživateli například zobrazila po přihlášení a musel ji aktivně zavřít. Celkově byla v kapitole 6.2.2 potvrzena závislost kvalitativních znaků mezi znalostí mobilních bankovních aplikací a zájmem o mobilní platby, čímž by daná banka zároveň získala zpětnou vazbu o tom, že uživatel předávanou informaci alespoň uviděl. U komunikace prostřednictvím funkce zprávy z banky není zaručeno, že uživatel tyto zprávy vybírá a banka tak zároveň nemá žádný nástroj, jak uživatele k přijetí zprávy přimět. Dále propagací v multimédiích či za pomoci online marketingových nástrojů, které by mohly oslovit i konzervativnější uživatele, jelikož automatizace platebních operací zároveň přímo snižuje náklady na zpracování platebních příkazů, což je další přínos pro každou finanční instituci.

Jednoznačný prostor pro zvýšení počtu uživatelů tedy autor práce spatřuje v oblasti bezpečnostních rizik a informovanosti klientů o vhodném bezpečném používání zařízení na platformě Android OS, které je aktuálně velmi sporadické.

Vhodným řešením by bylo vytvoření partnerského programu s jedním z vývojářů antivirových aplikací, který vyšel z provedených testů řešených v kapitolách 5.7.1 a 5.7.2 s nejvyšším hodnocením a následné distribuce dané aplikace, či umístění odkazu do Obchod Play, přímo na stránky dané banky, čímž by dané řešení bylo důvěryhodně komunikováno přímo oficiálním informačním kanálem. Vzhledem ke skutečnosti uvedené v kapitole 5.7.2, že mezi sedmi nejlépe hodnocenými aplikacemi bylo pět aplikací z oblasti freeware, by tak dané finanční instituci nevznikaly téměř žádné dodatečné náklady a vývojář by toto řešení zcela jistě uvítal, jelikož by se mu zvýšil počet uživatelů pro případnou dodatečnou nabídku placené verze. Paralelně by tak finanční instituce pasivně zvyšovala bezpečnost svých klientů a poskytla případně prostor k předání informací o zanedbatelném vlivu antivirové aplikace na výdrž baterie či hardware zátěž daného zařízení, jak také vyplývá i z výše uvedených kapitol o testování antivirových aplikací.

Další vhodné řešení, vycházející z kapitoly 5.8, se nalézá v poskytnutí garance pro danou aplikaci, která samozřejmě může být podmíněna nutností instalace antivirové aplikace a disponováním zařízení bez přidělených práv superuživatele. Na základě kapitoly 5.5 bylo potvrzeno, že práva superuživatele v daném zařízení jsou vzhledem k bezpečnostním rizikům zcela nežádoucí. Dále vzhledem ke zjištěným skutečnostem z kapitol 5.3 a 5.4, že i přes případnou důkladnou pozornost uživatele vůči přidělovaným právům při instalaci aplikace mohou některé nákazy proniknout i do oficiálního zdroje aplikací Obchod Play, aniž by je podchytil analytický nástroj Google Security a zároveň jsou schopné obejít několikavrstvou ochranu systému, se využití antivirové aplikace rovněž stává prakticky nezbytnou. V případě instalace aplikací třetích stran se stává dle zpracované problematiky přítomnost antivirové aplikace zcela zásadní.

Řešení tohoto typu by výsledně přineslo vyšší účinek, než pouhé snahy o rozšiřování informační gramotnosti. Poskytnutím garance dává finanční instituce najevo důvěru ve vlastní softwarový produkt, která je přenášena na klienta.

Samozřejmě je však stále potřeba rozvíjet i informační gramotnost vzhledem k rizikům podvodných technik uvedených v kapitole 5.2, které si kladou za cíl na základě nepozornosti uživatele získat jeho citlivé uživatelské údaje. V této oblasti nejsou rizika až tak vysoká, jako tomu je v případě internetového bankovnictví, avšak nejen malware pro Android OS dle kapitol 5.1 a 5.6 prochází rychlým vývojem, a tak i tyto podvodné techniky jsou rychle modifikovány pro oblast mobilních telefonů, jak i vyplynulo z kapitol 5.2.1, 5.2.3, 5.2.4, 5.2.5 a 5.2.7.1.

Značné ohrožení autor práce spatřuje v útoku typu DoubleDirect, který lze eliminovat vypnutím ICMP přesměrování paketů, což je však pro uživatele spjato s pro tuto oblast zcela nežádoucími právy superuživatele. Východisko autor práce spatřuje v diskusi s vývojáři, aby byla funkce ICMP Redirect volitelná v GUI Android OS. Možnost volby deaktivace funkce přesměrování paketů by tak zamezila útokům typu DoubleDirect. Vyšší hrozbu autor práce spatřuje v útocích typu Keylogger, a to na základě běžného rozložení softwarové klávesnice či případně ve zneužití Keyloggeru, který byl na zařízení instalován za účelem tzv. rodičovské kontroly. Zde se otevírá prostor k nabídce krátkých interaktivních demo náhledů z aplikace obsahující bezpečnostní doporučení a nabídce konzultací bezpečnostních rizik prostřednictvím Helpdesku či zákaznických linek.

9. Zdroje

9.1 Citovaná literatura

1. **IDC Research, Inc.** Smartphone OS Market Share, 2015 Q2. *Http://www.idc.com.* [Online] 2015. [Citace: 12. září 2015.] http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

2. **Statista.** Distribution of Android operating systems used by Android phone owners in October 2015, by platform version. *Statista - The Statistic Portal.* [Online] 2015. [Citace: 29. říjen 2015.] http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/.

3. **Era.** Era portál – nové internetové bankovnictví. *Https://www.erasvet.cz.* [Online] 2015. [Citace: 12. září 2015.] https://www.erasvet.cz/fyzicke-osoby/ostatni/stranky/internetove-bankovnictvi/co-je-nutne-k-zalozeni.aspx.

4. **ING.** Mezi Čechy je oproti zbytku Evropanů jen velmi málo uživatelů mobilního bankovnictví. *Http://www.ingbank.cz.* [Online] 2015. [Citace: 13. září 2015.] http://www.ingbank.cz/tiskove-centrum/zpravodaj-ing-bank/clanky/mezi-cechy-je-oproti-zbytku-evropanu-jen-velmi-malo-uzivatelu-mobilniho-bankovnictvi.html.

5. **Zemen, Jakub.** *Internetové bankovnictví.* Praha : Česká zemědělská univerzita v Praze, 2012. Bakalářská práce. Vedoucí práce Ing. Jan Jarolímek, Ph.D..

6. **ČNB.** Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví. *Https://www.cnb.cz.* [Online] ČESKÁ NÁRODNÍ BANKA, 2015. [Citace: 13. září 2015.] https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html.

7. 8. METODY A TECHNIKY SBĚRU DAT. *Http://management-marketingu.blogspot.com.* [Online] 2015. [Citace: 15. září 2015.] http://management-marketingu.blogspot.com/2010/09/8-metody-techniky-sberu-dat.html.

8. **Vojtíšek, Petr.** Výzkumné metody - Metody a techniky výzkumu a jejich aplikace v absolventských pracích vyšších odborných škol. [Online] 2012. [Citace: 15. září 2015.] Studijní text. http://skoly.praha.eu/files/=84121/Skripta++-+Výzkumné_metody.pdf. ISBN 978-80-905109–3-7.

9. **Kohoutek, Rudolf.** Dotazník jako průzkumná metoda. *Psychologie v teorii a praxi.* [Online] 2010. [Citace: 15. září 2015.] http://rudolfkohoutek.blog.cz/1002/dotaznik-jako-pruzkumna-metoda.

10. **Kábrt, Milan.** Test chí-kvadrát nezávislosti v kontingenční tabulce. *Aplikovaná statistika.* [Online] 2011. [Citace: 8. září 2015.] http://www.milankabrt.cz/testNezavislosti/.

11. **Petr Mareš, Ladislav Rabušic.** LEKCE09 MĚŘENÍ (SÍLY) ASOCIACE MEZI DVĚMA SPOJITÝMI PROMĚNNÝMI: KORELAČNÍ KOEFICIENTY A GRAFY . *https://is.muni.cz.* [Online] 2012. [Citace: 4. říjen 2015.] https://is.muni.cz/el/1423/podzim2004/SOC418/SPSS_8_korelace.pdf.

12. **Brožová Helena, Tomáš Šubrt, Milan Houška.** *Modely pro vícekriteriální rozhodování.* Praha : Credit, 2014. ISBN 978-80-213-1019-3.

13. **ČNB.** ČESKÁ NÁRODNÍ BANKA. *Slovník pojmů ČNB.* [Online] [Citace: 12. říjen 2015.] http://www.cnb.cz/cs/obecne/slovnik/e.html.

14. **Máče, Miroslav.** *Platební styk: klasický a elektronický.* Praha : Grada, 2006. ISBN 80-247-1725.

15. **Schlossberger, Otakar.** *Elektronické platební prostředky.* Praha : Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.

16. **Chvátal, Dalibor Z.** Mobilní bankovní SIM Toolkit je odsouzen k zániku, je staromódní. *měšec.cz.* [Online] 4. duben 2015. [Citace: 19. říjen 2015.] http://www.mesec.cz/clanky/mobilni-bankovnictvi-bude-pohodlne-ale-mene-bezpecne/.

17. **Sovová, Eva.** Banka v mobilu začíná ovlivňovat nákupní a finanční chování Čechů. *iDnes.cz/Finance.* [Online] 9. leden 2015. [Citace: 9. září 2015.] http://finance.idnes.cz/analyza-banka-v-mobilu-a-vyuzivani-aplikaci-fky-/viteze.aspx?c=A150108_110432_viteze_sov.

18. **Bubák, Zdeněk.** Začínáme seriál o mobilním bankovnictví v Česku. Postupně představíme aplikace vybraných bank. *Finparáda.* [Online] 27. březen 2015. [Citace: 22. říjen 2015.] http://www.finparada.cz/2665-Zaciname-serial-o-mobilnim-bankovnictvi-v-Cesku.aspx.

19. **Schwarzmann, Marek.** Banku v mobilu používá více než 1,1 milionu Čechů. *E15.cz.* [Online] 19. říjen 2015. [Citace: 29. říjen 2015.] http://e-svet.e15.cz/technika/banku-v-mobilu-pouziva-vice-nez-1-1-milionu-cechu-1237524.

20. **mBank.** Mobilní aplikace. Jednoduchá, intuitivní a pohodlná. *mBank.* [Online] mBank, 2015. [Citace: 28. říjen 2015.] http://www.mbank.cz/firemni/sluzby/mobilni-aplikace/.

21. **ING, Bank.** GENERAL REGULATIONS. *https://www.ing.be.* [Online] 18. srpen 2013. [Citace: 22. listopad 2015.] https://www.ing.be/xpedio/groups/transaction/@transaction/@ibe/@homebank/documents/portalcontent/060776_en.pdf.

22. **Bank, UniCredit.** Služby a parametry GWS. *UniCredit Bank.* [Online] 1. červen 2015. [Citace: 28. říjen 2015.] https://www.unicreditbank.cz/files/download/prime_bankovnictvi/Sluzby_a_parametry_GWS.pdf.

23. **Kuinam J. Kim, Naruemon Wattanapongsakorn.** *Mobile and Wireless Technology 2015.* Berlin : Springer, 2015. ISBN 978-3-662-47668-0.

24. **SocialCompare Collaborative comparsion, engine.** Android versions comprasion. *SocialCompare Collaborative comparsion engine.* [Online] 13. říjen 2015. [Citace: 16. říjen 2015.] http://socialcompare.com/en/comparison/android-versions-comparison.

25. **Sarah Mitroff, Jessica Dolcourt.** The Android era: From G1 to Lollipop. *CNET.* [Online] 8. květen 2014. [Citace: 16. říjen 2015.] http://www.cnet.com/news/history-of-android/.

26. **Air Bank, a. s.** Mobilní bankovnictví. *Google Play.* [Online] 2015. [Citace: 17. říjen 2015.] https://play.google.com/store/apps/details?id=cz.airbank.android&hl=cs.

27. **KB.** Mobilní banka. *Komerční banka.* [Online] Komerční banka, 2015. [Citace: 17. říjen 2015.] http://www.kb.cz/cs/lide/obcane/mobilni-banka-2.shtml.

28. **ČS.** SERVIS 24 Mobilní banka. *Česká spořitelna.* [Online] Česká spotřitelna, 2015. [Citace: 17. říjen 2015.] http://www.csas.cz/banka/nav/osobni-finance/servis-24-mobilni-banka/o-produktu-d00024634.

29. **UniCredit, Bank.** Smart Banking. *UniCredit Bank.* [Online] 2015. [Citace: 30. říjen 2015.] https://www.unicreditbank.cz/web/obcane/online-sluzby/smart-banking.

30. **Anmol Misra, Abhishek Dubey.** *Android Security: Attacks and Defenses.* New York : CRC Press, 2013. ISBN 9781439896471.

31. **SocialCompare.** Mobile OSes: developer comparsion. *SocialCompare Collaborative comparsion engine.* [Online] 28. duben 2015. [Citace: 18. říjen 2015.] http://socialcompare.com/en/comparison/mobile-os-comparison-developer-view.

32. **TechTerms.** Android Definition. *TechTerms.* [Online] 4. leden 2010. [Citace: 15. říjen 2015.] http://techterms.com/definition/android.

33. **Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, Muttukrishnan Rajarajan.** Android Security: A Survey of Issues, Malware Penetration and Defenses. *ResearchGate.* [Online] 30. srpen 2015. [Citace: 11. říjen 2015.] http://www.researchgate.net/publication/274013709_Android_Security_A_Survey_of_Issues_Malware_Penetration_and_Defenses. ISSN 1553-877X.

34. **Google, Inc.** Security. *android.* [Online] 2015. [Citace: 10. září 2015.] https://source.android.com/devices/tech/security/.

35. **Google, Inc.** The Android Source Code. *android.* [Online] 2015. [Citace: 17. říjen 2015.] http://source.android.com/source/index.html.

36. **Tišnovský, Pavel.** Architektura mikrořadičů s jádry ARM Cortex-M3. *Root.cz.* [Online] 6. září 2015. [Citace: 30. říjen 2015.] http://www.root.cz/clanky/architektura-mikroradicu-s-jadry-arm-cortex-m3/.

37. **Suhas Holla, Mahima M Katti.** ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY. *http://www.internationaljournalssrg.org/.* [Online] 2012. [Citace: 3. říjen 2015.] http://ijcttjournal.org/Volume3/issue-3/IJCTT-V3I3P130.pdf. ISSN: 2231-2803.

38. **Sebastian Neuner, Victor van der Veen, Martina Lindorfer, Markus Huber, Georg Merzdovnik, Martin Mulazzani, Edgar Weippl∗.** Enter Sandbox: Android Sandbox Comparison. *Cornell University Library.* [Online] 28. listopad 2014. [Citace: 7. září 2015.] http://arxiv.org/ftp/arxiv/papers/1410/1410.7749.pdf.

39. **Šlik, Jáchym.** „Vývojáři mobilních antivirů jsou šarlatáni a podvodníci," uvedl expert z Google. *ANDROID MARKET.* [Online] 2011. [Citace: 14. říjen 2015.] http://androidmarket.cz/ruzne/vyvojari-mobilnich-antiviru-jsou-sarlatani-a-podvodnici-uvedl-expert-z-google/.

40. **Shankland, Stephen.** Googler: Android antivirus software is scareware from 'charlatans'. *http://www.cnet.com/.* [Online] 18. listopad 2011. [Citace: 16. říjen 2015.] http://www.cnet.com/news/googler-android-antivirus-software-is-scareware-from-charlatans/.

41. **Kilián, Karel.** Nové škodlivé aplikace objeveny v Android Marketu. *SVĚT ANDROIDA.* [Online] 12. červenec 2011. [Citace: 12. září 2015.] http://www.svetandroida.cz/nove-skodlive-aplikace-objeveny-v-android-marketu-201107.

42. **Golson, Jordan.** Phil Schiller Tweets Link to Mobile Malware Report That Slams Android. *MacRumors.* [Online] 7. březen 2013. [Citace: 4. říjen 2015.] http://www.macrumors.com/2013/03/07/phil-schiller-tweets-link-to-mobile-malware-report-that-slams-android/.

43. **Selinger, Markus.** 35 Android Protection Apps Put to a 6-Month Endurance Test. *AV.TEST - The Independent IT-Security Institute.* [Online] 17. prosinec 2014. [Citace: 28. září 2015.] https://www.av-test.org/en/news/news-single-view/35-android-protection-apps-put-to-a-6-month-endurance-test/.

44. **Zetter, Kim.** Hacker Lexicon: What Are Phishing and Spear Phishing? *WIRED.* [Online] 4. červenec 2015. [Citace: 18. září 2015.] http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/.

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

46. **Keylogger, Android.** Android Keylogger – 2015 Best Keylogger App for Android. *Android Keylogger.* [Online] 2015. [Citace: 19. říjen 2015.] http://www.android-keylogger.net/.

47. **Coob, Michael.** Mobile keyloggers: Defense measures against mobile keystroke logging. *TechTarget - SearchSecurity.* [Online] červen 2014. [Citace: 3. říjen 2015.] http://searchsecurity.techtarget.com/answer/Mobile-keyloggers-Defense-measures-against-mobile-keystroke-logging.

48. **Cherian, Blessen.** Preventing DDoS Attacks. *LinuxSecurity.com.* [Online] 2015. [Citace: 6. říjen 2015.] http://www.linuxsecurity.com/content/view/121960/49/.

49. **Asaf Shabtai, Dudu Mimran, Yuval Elovici.** Evaluation of Security Solutions for Android Systems. *Cornell University Library.* [Online] 17. únor 2015. [Citace: 28. září 2015.] http://arxiv.org/ftp/arxiv/papers/1502/1502.04870.pdf.

50. **Weber, Johannes.** IPv6 Security - An Overview. *RIPE NCC.* [Online] 18. červen 2013. [Citace: 13. září 2015.] https://labs.ripe.net/Members/johannes_weber/ipv6-security-an-overview.

51. **Paganini, Pierluigi.** DoubleDirect MitM Attacks are targeting users worldwide. *security affairs.* [Online] 22. listopad 2014. [Citace: 8. říjen 2015.] http://securityaffairs.co/wordpress/30417/cyber-crime/doubledirect-mitm-attacks.html.

52. **COMPUTERWORLD.** Computerworld.cz. *O bezpečnosti aplikací pro Android si můžeme nechat zdát.* [Online] 11. březen 2013. [Citace: 15. duben 2014.] http://computerworld.cz/securityworld/o-bezpecnosti-aplikaci-pro-android-si-muzeme-nechat-zdat-49594.

53. **Havryluk, Michal.** Bezpečnost Androidu v číslech. Ještě lepší než jsme doufali. *Mobil.idnes.cz.* [Online] 2014. [Citace: 15. duben 2014.] http://mobil.idnes.cz/bezpecnost-androidu-0lm-/mob_tech.aspx?c=A131102_160512_mob_tech_ham.

54. **Stloukal, Ivan.** Android a bezpečnost - Google zveřejnil data. *Dotekomanie.cz.* [Online] 2014. [Citace: 15. duben 2014.] http://dotekomanie.cz/2013/10/google-uverejnuje-informace-jak-je-ve-skutecnosti-bezpecnosti-androidu/.

55. **GmbH, AV-TEST.** AV TEST - The Independent IT-Security Institute. *The best antivirus software for Android.* [Online] 2014. [Citace: 15. duben 2014.] http://www.av-test.org/en/tests/mobile-devices/android/sep-2013/.

56. **Nápravník, Jiří.** Největší hrozbou internetového bankovnictví není uživatel. *měšec.cz.* [Online] 11. květen 2015. [Citace: 24. září 2015.] http://www.mesec.cz/clanky/nejvetsi-hrozbou-internetoveho-bankovnictvi-neni-uzivatel/.

57. **Horáček, Filip.** Průměrná mzda v Česku stoupla na 26 287 korun, firmám chybí lidi. *iDnes.cz/Ekonomika.* [Online] 4. září 2015. [Citace: 7. listopad 2015.] http://ekonomika.idnes.cz/prumerna-mzda-v-cesku-stoupla-na-26-287-korun-fi8-/ekonomika.aspx?c=A150904_092018_ekonomika_fih.

58. **Dvořák, Jiří.** Vícekriteriální rozhodování. *SlidePlayer.* [Online] 2007. [Citace: 7. listopad 2015.] http://slideplayer.cz/slide/3032309/#.

59. **Miroslav Haluza, Jan Macháček.** Využití multikriteriální analýzy (MCA) pro hodnocení inteligentních elektroinstalací. *tzbinfo.* [Online] Fakulta elektrotechniky a komunikačních technologií VUT v Brně, 14. červenec 2011. [Citace: 9. listopad 2015.] http://elektro.tzb-info.cz/inteligentni-budovy/7651-vyuziti-multikriterialni-analyzy-mca-pro-hodnoceni-inteligentnich-elektroinstalaci.

60. **ČNB.** Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví. *ČESKÁ NÁRODNÍ BANKA.* [Online] 2015. [Citace: 17. říjen 2015.] http://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html.

9.2 Seznam obrázků

9.3 Seznam tabulek

10. Přílohy

Dotazník – na přiloženém CD

Data získaná z dotazníkového šetření - na přiloženém CD