Česká zemědělská univerzita v Praze
Provozně ekonomická fakulta
Katedra informačních technologií

Bakalářská práce
Bezpečnost dat na Internetu

Filip Malý

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Filip Malý

Informatika

Název práce

Bezpečnost dat na Internetu

Název anglicky

Data security on the Internet

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku bezpečnosti dat na Internetu. Hlavním cílem práce je identifikovat možnosti zabezpečení dat na Internetu v oblasti realokace finančních prostředků mezi elektronickými systémy.
Dílčím cílem bakalářské práce je:
- analyzovat úroveň zabezpečení uživatelů na Internetu a jejich znalost problematiky bezpečnosti v prostředí Internetu.
- vytvořit UI (user interface) specifikace pro bezpečné dobíjení finančních prostředků do informačního systému vybrané organizace.
- syntetizovat výsledky práce a formulovat závěry bakalářské práce.

Metodika

Rešeršní část bakalářské práce bude založena na analýze odborných a vědeckých dokumentů. Jako základní metodický postup v praktické části práce bude použita metoda dotazníkového šetření. Pro vytvoření UI specifikace uživatelského rozhraní bude použita metoda Affective interaction design. Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

Bezpečnost na Internetu, bezpečnost dat, Internet, user interface, Affective interaction design

---

Doporučené zdroje informací

BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.

COOPER, Alan, Robert REIMANN, Dave CRONIN a Alan COOPER. About face 3. ISBN 9780470084113.

GOODWIN, Kim, Robert REIMANN, Dave CRONIN a Alan COOPER. Designing for the digital age: how to create human-centered products and services. [3rd ed.], Completely rev. Indianapolis: Wiley, c2009, xxix, 739 s. ISBN 978-0-470-22910-1.

MCBRIDE, Patrick. Secure Internet practices: best practices for securing systems in the Internet and e-Business age. Cornelius, NC: METASeS, c2002, xv, 209 p. ISBN 08-493-1239-6.

RHEE, Man Young. Internet security: cryptographic principles, algorithms and protocols. Chichester: Wiley, 2003, xvii, 405 s. ISBN 04-708-5285-2.

VANÍČEK, Jiří. Měření a hodnocení jakosti informačních systémů. Vyd. 2., přeprac. V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2004. ISBN 978-802-1312-067.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Jan Tyrychtr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 11. 03. 2016

Čestné prohlášení

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

V Praze dne 10. 3. 2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Janu Tyrychtrovi, Ph.D. za odborné vedení a rady při zpracování této práce.

Bezpečnost dat na Internetu

Data security on the Internet

Souhrn

Tato bakalářská práce se zabývá problematikou bezpečnosti dat na Internetu, zejména bezpečností uživatelů, kteří se dostávají do styku s platbou na Internetu.

Práce je rozčleněna do dvou částí – teoretické a praktické. V teoretické části jsou definovány pojmy související s bezpečností dat na Internetu. Následuje představení potřebných termínů s vysvětlením řešené problematiky. Dílčí částí teoretické části je zpracovaná analýza bezpečnosti uživatelů na Internetu a jejich znalosti problematiky bezpečnosti dat.

Praktická část se zabývá návrhem UI specifikace pro bezpečné dobíjení finančních prostředků do informačního platebního systému. Uživatelé v tomto platebním systému budou moci dobíjet finanční prostředky prostřednictvím své kreditní karty, prémiové sms zprávy a klasické hotovostní platby.

Klíčová slova: Bezpečnost na Internetu, bezpečnost dat, Internet, User Interface, Affective Interaction Design.

Data security on the Internet

Bezpečnost dat na Internetu

Summary

This thesis deals with the issue of data security on the Internet, especially the safety of users, who come into contact with the payments on the Internet.

The thesis is divided into two parts - theoretical and practical. The theoretical part defines terms related to data security on the Internet. It is followed by the introduction of necessary terms with explanations of these issues. The theoretical part includes an analysis of the safety of users of the Internet and their knowledge of the issues of data security.

The practical part deals with a design of UI specifications for a safe charging of funds into the information payment system. The users in this payment system will be able to top up funds via their credit cards, premium SMS texts and classic cash payments.

Keywords: data security on the Internet, data security, Internet, User Interface, Affective Interaction Design

Obsah

1 Úvod

Platba přes Internet je již nedílnou součástí každodenního života, šetří nám čas a ulehčuje nám život. Na Internetu lidé nejčastěji platí v internetových obchodech za zboží nebo případně za služby. Platba přes Internet je velmi rychlá a snadná, ale má i své nevýhody v možnosti zneužití údajů potřebných pro platbu a následně nechtěného finančního úbytku na svém účtu. Pro platbu přes Internet lze v současné době využít jakékoli chytřejší zařízení, ze kterého lze provést platbu.

Nejčastěji pro platbu na Internetu lidé využívají svůj osobní počítač, kde volí platbu prostřednictvím bankovního převodu nebo přímé platby pomocí bankovní karty. Dále lidé využívají další dostupné prostředky pro platbu, u kterých se snaží vyvarovat zadávání hodnot ze své primární karty. Tyto prostředky například mohou být dvojité kreditní karty, kde jedna je přímo určená na platby přes Internet, nebo virtuální platební karty typu PayPal. V poslední době také přibývá mnoho plateb prostřednictvím mobilních telefonů. Tyto přístroje mají většinou nainstalované speciální programy distribuované jejich bankou, které jim umožní provádět platby skrze jejich mobilní telefon a také spravovat jejich mobilní bankovnictví.

Velmi oblíbeným prostředkem pro platbu je bankovní převod přes internetové bankovnictví. Lidé tuto možnost velmi rádi využívají, protože je velmi jednoduchá a dobře zabezpečená. Pro přístup do internetového bankovnictví lze využít v současnosti velké množství zařízení, která mají přístup na Internet. Výhodou této platební metody je, že uživatel přesně ví, kolik finančních prostředků má aktuálně na svém účtu.

V současnosti existuje velké množství problémů v návrhu těchto systémů v kontextu bezpečnosti a UI specifikace. Tato práce se zabývá právě touto problematikou.

1.1 Cíl práce

Bakalářská práce je tematicky zaměřena na problematiku bezpečnosti dat na Internetu. Hlavním cílem práce je identifikovat možnosti zabezpečení dat na Internetu v oblasti realokace finančních prostředků mezi elektronickými systémy. Dílčím cílem bakalářské práce je:

- analyzovat úroveň zabezpečení uživatelů na Internetu a jejich znalost problematiky bezpečnosti v prostředí Internetu,
- vytvořit UI (user interface) specifikace pro bezpečné dobíjení finančních prostředků do informačního platebního systému,
- syntetizovat výsledky práce a formulovat závěry bakalářské práce.

1.2 Metodika práce

Metodika řešení využívaná v této práci je založena na studiu odborných a vědeckých dokumentů, které jsou zaměřeny na danou problematiku, a jejich následné zpracování. Jako základní postup v praktické části práce budou použity metody pro tvorbu UI specifikace. Pro vytvoření UI specifikace uživatelského rozhraní bude použita metoda User Interface design. (1) (2)

Metoda User Interface design je podmnožinou oboru studia nazývaného Human Computer Interaction (HCI), v českém překladu Interakce člověk počítač. Jedná se o studii, plánování a design, jak lidé a počítače pracují dohromady, aby byly lidské potřeby co nejvíce uspokojeny. (3)

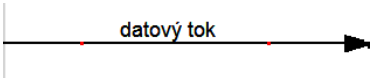
Metoda Affective Interaction design v překladu znamená citový interakční design. Princip metody spočívá v celém procesu návrhu interakce, kde si projektanti musí být vědomi klíčových aspektů svých návrhů, které mají vliv na emociální reakce u cílových uživatelů. (4) (5)

Pro tvorbu UI specifikace v praktické části jsou použity Diagramy datových toků (Data Flow Diagram) a UML schémata (Unified Modeling Language) vytvořené v programu MetaEdit+. DFD je graf datových toků od jejich vzniku v objektu přes jejich zpracování, které je transformuje pro potřebu jiného objektu. (6) DFD obsahuje procesy, datové toky, datastory a aktory (terminátory). Níže uvedené symboly reprezentují tyto termíny.

Symbol 1 proces (vlastní zpracování)

Symbol 2 aktor (vlastní zpracování)

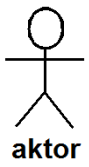
Symbol 3 datastore (vlastní zpracování)



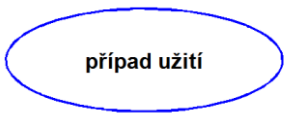
Symbol 4 datový tok (vlastní zpracování)

Sjednocený modelovací jazyk (UML) je druh grafické notace, podporovaný nezávislým meta-modelem, který umožňuje popisovat a navrhovat softwarové systémy, konkrétně systémy budované využitím objektově orientované metodiky. (7)

Případ užití (Use Case) je metodou pro zachycení funkčních požadavků na systém. Případy užití popisují typické interakce mezi uživateli systému a samotným systémem, a předkládají nám příběh o tom, jak je systém používaný. (7) Případy užití se skládají ze scénářů a účastníků (aktérů). Níže uvedené dva symboly reprezentují tyto termíny.



Symbol 5 Use Case aktor (vlastní zpracování)



Symbol 6 případ užití (vlastní zpracování)

2 Přehled řešené problematiky

V této kapitole autor popisuje základní řešenou problematiku této bakalářské práce. Autor zde uvádí nezbytné pojmy pro lepší porozumění této práce.

2.1 Data versus informace

Pod pojmem data si můžeme představit surovou informaci, která potřebuje dále zpracovat, abychom jí dostatečně porozuměli. Ve světě počítačové vědy byla data používána, jako pro označení čísla, textu, zvuku, obrazu a dalších smyslových vjemů vhodných pro zpracování počítačem. (8) Z hlediska práce s daty lze data členit na strukturovaná a nestrukturovaná.

2.1.1 Strukturovaná data

Tato data explicitně zachycují fakta, atributy, objekty a další objekty, přičemž významným rysem je existence určitých elementů dat. Klasickým příkladem je ukládání dat pomocí relačních databázových systémů, ve kterých se obvykle používá hierarchie elementů pole→ záznam→ relace→ databáze. Díky tomuto uskupení lze snadno vybírat jen ta data, která jsou zapotřebí k řešení nějakého informačního problému. (8)

2.1.2 Nestrukturovaná data

Tyto data jsou vyjádřena jako „tok bytů“ bez dalšího rozlišení, může jít například o obrázky, videonahrávku nebo textový řetězec. (8)

2.2 Bezpečnost informací

Informace existuje na našich počítačích v elektronické podobě, jako jsou dokumenty, fotografie, programy, obrázky, e-maily a další soubory. Tato informace je přepravována mezi počítači a je snadno a rychle duplikovatelná nebo vysílaná. Je ji možné kopírovat, distribuovat a zničit ve vteřině, tyto její vlastnosti ztěžují její ochranu. Přestože informace existují v elektronické podobě, v přenosu, na pevném disku nebo na paměťovou kartě, musíme je chránit před činnostmi, jako jsou krádež, zničení, podvod, neoprávněné užití nebo neoprávněné zveřejnění. Informace musí být chráněny proti útoku zvenčí, útoku zevnitř a nevinných chyb od uživatelů. Informace jsou chráněny proti hrozbám s využitím

protiopatření, jako jsou antiviry a různé firewally, dále lze informace zašifrovat a tím zvýšit jejich neporušitelnost. (9)

2.3 Nástroje zabezpečení na Internetu

V následující podkapitole budou autorem této práce popsány základní nástroje pro zabezpečení na Internetu.

2.3.1 Autentizace

Autentizace je proces, který nastává před začátkem datové výměny. Má na starost zjistit, kdo je komunikačním partnerem, znamená to tedy identifikování subjektu v daném okamžiku. (10)

2.3.2 Autorizace

Autorizace je proces, který nastává po autentizaci. Tento proces ověřuje přístupová práva subjektu k informačnímu systému. Pro zajištění bezpečnostních požadavků se aplikuje několik bezpečnostních mechanismů. (10)

2.3.3 Ověřovací protokoly

Jedním z hlavních problémů spojených se stávajícími TCP / IP sítěmi je snadný přenos dat po síti, která mohou být zachycena a analyzována. Tento problém souvisí se způsobem fungování protokolů v LAN síti. Údaje posílané jako prostý text v sítích TCP / IP jsou vystaveny nebezpečí, proto jakýkoli ověřovací mechanismus, který bude vycházet z jasných textových hesel, nebo předvídatelných hesel není bezpečný. Zabezpečení síťových zařízení pomáhá zlepšit bezpečnost přenosu pomocí TCP/ IP, ale problém je, že třetí osoby mohou používat štěnice a podobné nástroje. Zamezit zneužití lze s využitím standardních protokolů ověřování. Nejznámější protokol, který se využívá, je SSL protokol pro bezpečnou relaci, tento protokol bude popsán detailněji v samostatné kapitole. (11)

2.3.4 Ověřování autorizačními servery

Autentizační servery slouží k ověřování v síťovém prostředí. Tyto servery jdou ještě o krok dále tím, že uchovávají privilegia nebo přístupová práva pro ověření identity. Autentizační a autorizační servery poskytují příslušné služby pro řadu klientů v architektuře

klient-server. Jsou schopny zajistit bezpečnost všech vrstev softwaru, tak dlouho, dokud klient má vhodné rozhraní a je správně nakonfigurován. (11)

2.3.5 Síťová integrita pomocí síťových skenerů

Zabezpečení pomocí síťových skenerů je založeno na podobném principu jako hostitelské bezpečnostní skenery. Jejich účelem je skenování sítě, hledání věcí, které by tam neměly být, a v neposlední řadě odhalení potenciální zranitelnosti. I nejjednodušší síťové skenery vykonávají mnohem více, než pouze mapování zařízení, které se v síti nachází. Využívají k tomu jednoduchých sond, jako jsou například Internet Control Message Protocol (ICMP) nebo echo request zprávy (běžně známé jako ping). O úroveň výš z jednoduchých nástrojů příkazového řádku jsou nástroje schopné vykonávat mapování portů. Sondováním individuální TCP nebo User Datagram Protocol (UDP), mohou tyto nástroje zmapovat síť a určit, které síťové služby jsou v provozu. Nejlepší jsou komerční nástroje, které při použití podobných technik využívají databázi obsahující informace o známých zranitelnostech. (11)

2.3.6 Firewall

Firewall je zařízení, nebo kombinace zařízení, která řídí přístup mezi dvěma nebo více síťovýma segmenty. Firewally povolují nebo zakazují připojení z jedné sítě do druhé na základě souboru pravidel vyjádřených daty v protokolu. Tato data jsou převzata z vrstev 3 až 7 modelu OSI. U TCP / IP modelu jsou v aplikační vrstvě. Moderní komerční firewally obsahují funkce pro autentizaci uživatelů, což je důležitým krokem vpřed, protože nám umožňují připojení k síti na osobu, nikoli na síťovou adresu. (11)

2.3.7 Proxy server

Proxy server funguje podobným způsobem jako firewally aplikaci-brány. Rozdíl je v tom, že firewally řídí přístup k síti pro příchozí i odchozí provoz, zatímco proxy servery slouží pro kontrolu spojení, která vznikají v rámci podniku. Proxy servery vyžadují autentizaci koncového uživatele, omezují komunikaci na definovanou sadu protokolů, které uplatňují omezení řízení přístupu a starají se o audit a protokolování. (11)

2.3.8 Webové filtry

Webové filtry se používají pro řízení přístupu zaměstnanců na externí webové stránky. Tyto nástroje umožňují administrátorovi selektivně blokovat přístup na určité typy webů na základě místní dohody. Filtrováním webového obsahu lze povolit nebo zablokovat přístup do externích internetových zdrojů. Ve skutečnosti se tyto nástroje používají pro zvýšení produktivity zaměstnanců a zvýšení bezpečnosti webu. Webové filtry chrání tím, že zabraňují uživatelům v přístupu na stránky, které by mohly hostit nevhodný obsah nebo škodlivý kód. (11)

2.4 Šifrování

Šifrování je mocným nástrojem k utajování zpráv, dokumentů nebo souborů. Návrhem a implementací šifrovacích systémů se zabývá kryptografie. Údaje se dělí uživatelům na srozumitelný otevřený text a na jeho tajný ekvivalent šifrový text. Dále k těmto informacím patří šifrovací klíč. Šifry se dělí na dva základní principy symetrické a asymetrické. (12)

2.4.1 Symetrické šifrování

Této metodě šifrování se obecně přezdívá klasická nebo konvenční. U těchto šifer je využíván jeden klíč pro zašifrování a dešifrování souboru. Tyto šifry mají výhodu ve snadné implementaci a časové náročnosti, ale proti tomu mají nevýhodu ve snadnějším prolomení hesla. Příklad jednoduché symetrické šifry může být Caesarova šifra, která využívala posunu písmen o určitou délku n. (12)

Moderní šifrovací algoritmy nepracují s písmeny, ale s bity. Nejpoužívanější kódovací tabulkou je kód ASCI, který vytváří z posloupnosti bitů bitové řetězce. Šifry se poté dělí na proudové, kdy je šifrován jeden bit po druhém a blokové, kde se bity sdružují do bloků předem dané velikosti. (13) Mezi blokové šifry patří: AES (14), Blowfish (14), Des (15), Gost (15), IDEA (16), RC2 (16), RC5 (16), Triple DES (15), Twofish (16) a Skipjack (16). Mezi proudové šifry patří FISH a RC4 (17).

2.4.2 Asymetrické šifrování

Asymetrická kryptografie, která je mladší než symetrická, se jinak nazývá moderní kryptografie. Tato metoda šifrování využívá dva odlišné klíče pro šifrování a dešifrování. Nazývají se veřejný a soukromý klíč. Veřejný klíč je určen k šifrování a tajný soukromý je pouze pro dešifrování. Klíče jsou navrhovány tak, že v rozumném čase nesmí být možné z jednoho odvodit druhý. Asymetrická kryptografie je bezpečnější, ale časové náročnější než symetrická kryptografie. (12) Příklady asymetrických šifer jsou: RSA (18), ElGamal (19), Diffie-Hellman (14), DSA (14) a Merkle-Hellman (20).

2.4.3 Hash otisk

Dalším způsobem zabezpečení je využití hashovací funkce, pomocí které lze vytvořit otisk zprávy – hash. Vstupem této funkce je libovolně dlouhá zpráva, ale výstupem je otisk, který má pevnou délku. To v praxi znamená, že pokud změníme i jediný znak, dostaneme na výstupu úplně jiný otisk. Hash se využívá převážně k vytvoření elektronického podpisu. Nejdříve se použije hash funkce a poté se soubor zašifruje veřejným klíčem. Příjemce si soubor pak otevře pomocí svého privátního klíče. (21) Nejznámější hash otisky jsou SHA-1, (22) a MD5. (22)

3 Interakce člověk počítač

Interakce člověk počítač (Human Computer Interaction, dále jen HCI) představuje oblast výzkumu a praxe, která se zrodila počátkem 80. let 20. století. Původně to byla specializace v rámci jedné počítačové vědy, zahrnující kognitivní vědu a ergonomii. Zkoumání interakce člověka s počítačem se rychle rozrostlo mimo původní rámec a tento vědní obor se neustále vyvíjí. V současnosti oblast HCI do značné míry představuje spojení oblastí výzkumu a praxe v rámci informatiky zaměřené na člověka. (23)

Podstata HCI spočívá v inovaci této oblasti tak, aby se lidské hodnoty a priority prostřednictvím nových technologií dále rozvíjely a neupadaly. HCI je otevřený koncept, který nemůže být nikdy zredukován na předem danou osnovu nebo oblast. (23)

3.1 Základní teorie

Základní teorii lze rozdělit do těchto tří základních etap teorií:

1. teorie nahlíží na interakci člověka s počítačem jako na zpracování informací,
2. teorie chápe interakci jako iniciativu uživatele jak má realizovat svoje úkoly a projekty,
3. teorie interakci neodděluje od sociálního a materiálního kontextu okolního světa.

3.1.1 Tři základní směry HCI

U HCI lze rozlišit tyto tři základní přetrvávající směry:

1. směr tradičních stále širších aplikací a hlubších základních teorií,
2. směr vývoje místních teorií v rámci konkrétních návrhářských oblastí,
3. směr využívání návrhářského přístupu jako zprostředkovatelské úrovně pro popis mezi základní vědou a designérskou praxí.

Při tvorbě návrhu musí návrhář zvažovat mnoho faktorů, například co lidé chtějí a předpokládat jaké jsou jejich fyzické možnosti a schopnosti. Návrhář také musí brát v potaz technickou stránku zařízení a limity počítačů a softwaru. (3)

Více o oboru HCI se lze dočíst v těchto publikacích: Hci Theory: Classical, Modern, and Contemporary od autora Yvonne Rogers (24), Human-Computer Interaction od autorů DIX,

Alan, Janet Finlay, Gregory D. Abowd a R. Beale (25). O tomto oboru existuje mnoho dostupné literatury, autor práce v tomto odstavci uvádí pouze pár nejznámějších publikací.

3.2 Interakční design

Tento druh designu byl představen kolem roku 1985 pány Billem Moggridgem a Billem Verplankem. Do roku 1990 zůstává nevyužitý, až do doby, kdy Gillian Crampton-Smith zahájil výuku a praktické využití na Royal College of Art (RCA) v Londýně pod názvem Computer-Related Design. (5)

Interakční design v sobě zahrnuje tyto části:

- cílově orientovaný design,
- persony,
- kognitivní dimenze,
- citový interakční design.

3.2.1 Cílově orientovaný design

V originále nazývaný Goal-Oriented Design lze přeložit do českého jazyka jako design směřovaný k efektivnímu dosažení uživatelského cíle. Snahou je umožnit uživateli zajistit splnění jeho uživatelského cíle (business goal) co nejrychleji, s vynaložením minimálního úsilí. V tomto odvětví pracoval Alan Cooper. Tvrdil, že musíme skutečně pochopit cíle uživatele (osobní i objektivní), a následně vyřešit problém nejlepším možným způsobem. Dále uváděl, že současný přístup k řešení problémů je hodně orientován na řešení jednotlivých problémů z pohledu podnikání či jiné zúčastněné strany. (24) (5)

3.2.2 Persony (aktéři)

Persony se v originále nazývají Personas, lze je přeložit do českého jazyka jako uživatele, kteří budou se systémem, věcí pracovat. Tato část v sobě zahrnuje personifikace uživatelů. Modeluje vzorové archetypy, pro které je finální návrh směřován. Cílem person je popsat přesný charakter našeho uživatele a jeho cíle, kterého si přeje dosáhnout. Nejlepší způsob je dát uživatelům jména a krátké příběhy, které pak budou představovat reálné uživatele daného produktu. Důvodem pro tvorbu příběhů pro uživatele je, aby tyto postavy

byly věrohodné, aby tak mohly být považovány za skutečné lidi a jejich potřeby mohly být uskutečněny. (26) (5)

3.2.3 Poznávací dimenze

Poznávací dimenze se v originálním znění nazývá Cognitive Dimension. Jedná se o přístup k analýze a kvalitě výsledného designu. Je to společný slovník pro diskuzi o mnoho faktorech v notaci UI, poskytuje odbornou slovní zásobu pro hodnocení a změny v konkrétním řešení designu. Tyto přístupy jsou navrženy jako lehký přístup k analýze kvality designu. Věnují se především popisu, který má být podrobný a na vysoké úrovni a má popsat jak s UI uživatelé pracují. (27) (5)

3.2.4 Citový interakční design

Citový interakční design se v originálním překladu nazývá Affective Interaction Design. V tomto případě se přistupuje k tvorbě návrhu, kdy si musí být designéři vědomi klíčových aspektů řešení a jejich vzorů. Jedná se o aspekty, které ovlivňují emocionální reakce cílových uživatelů. U finálního produktu by člověka mělo těšit jeho používání, produkt by jej neměl dělat hloupým, neporušovat jeho model. V programech se využívají například dynamické ikony, animace a zvuk. Tyto prostředky nám mohou pomoci pochopit stav provozu, vytvářet pocit interaktivity a zpětné vazby. (4) (5)

3.3 Princip tvorby specifikace uživatelského rozhraní

Specifikace uživatelského rozhraní je formalizovaný postup popisu chování, které vychází z principů interakčního designu (dále jen ID). Snahou uživatelského rozhraní (dále jen UI) je dodržet základní hlediska interakce člověka s počítačem. Dalším cílem UI specifikace je vytvořit uživatelskou přívětivost a použitelnost. Posledním důležitým aspektem je zahrnutí efektivního použití. (5)

4 Protokoly na bázi SSL

SSL je bezpečnostní protokol z dílen firmy Netscape. Protokol vznikl počátkem roku 1994, se záměrem vyvinout bezpečnou komunikaci mezi serverem a webovým prohlížečem. Jeho specifikace byla navržena tak, aby mohla pracovat i s dalšími aplikacemi, jakou jsou TELNET nebo FTP. Protokol SSL má řadu využití zejména v transakční sféře, kde je potřeba chránit data z platebních karet a mít tak bezpečné a kvalitní šifrované spojení. (28) Nejčastější využití tohoto protokolu je u:

- internetových obchodů, které přijímají objednávky a platby pomocí platebních karet,
- zabezpečení a uchování hesel a přihlašovacích údajů na webových portálech,
- obchodní komunikace s partnery (výměna důvěrných informací),
- chráněný přístup do vlastních emailů,
- uchovávání a zpracování citlivých osobních údajů,
- zabezpečené přenosy regulačních ustanovení legislativy.

Zejména kvůli prvnímu bodu, zabezpečení internetových obchodů a platebních karet, bude autor této práce tento protokol v širším smyslu rozebírat.

4.1 Verze SSL

Pro SSL protokol existují základní tři verze. SSL verze 1.0, která nebyla vydána pro veřejnost, verze SSL 2.0 byla poprvé použita pro veřejnost a verze SSL 3.0, která byla oficiálně oznámena v březnu 1996. (29)

4.1.1 Podprotokoly SSL

Mezi podprotokoly SSL patří tyto čtyři následující protokoly:

- Handshake Protokol (spojující protokol): zajišťuje správné navázání bezpečného a autentizovaného spojení mezi komunikujícími stranami,
- Record Layer Protokol: tento protokol zodpovídá za zapouzdření dat protokolů vyšších vrstev, například u http,
- Change Cipher Specification Protokol: tento uvedený protokol nastavuje parametry šifrování,
- Alert Protokol: slouží k podávání informací o varováních a chybách.

Zpracováno dle publikace Šifrování a biometrika. (12)

4.2 Handshake Protokol

Tento protokol tvoří hlavní komponentu celého procesu. Po jeho úspěšném proběhnutí je zajištěna autentizace klienta (nemusí být vyžadováno), autentizace serveru (toto je vždy povinné) a výměna náhodných informací pro výpočet šifrovacích klíčů. Pro popis metody Handshake je využíváno HELLO zpráv. (12). Klient zašle serveru Hello zprávu, server tuto zprávu buď přijme a založí bezpečnou komunikaci mezi serverem a klientem, nebo se může také stát, že server Hello zprávu nepřijme a nastane fatální error, který skončí nekomunikací mezi klientem a serverem. Klientova Hello zpráva a zpráva ze serveru založí tyto následující atributy: verzi protokolu, náhodné hodnoty pro server a klienta, identifikátor sezení, šifrovací metodu a kompresní metodu. (30)

4.2.1 Princip Handshake protokolu

Začátek protokolu je u klienta, který pošle serveru zprávu s těmito parametry:

- verze protokolu: v této zprávě je obsažen protokol, kterým si přeje klient komunikovat v průběhu akce. Většinou se používá nejvyšší verze disponovaná klientem,
- náhodná hodnota: jedná se o klientem vygenerovanou náhodnou strukturu znaků o délce 28 bytů,
- identifikátor sezení: jedná se o identifikaci spojení. Klient může zaslat dva privátní stavy serveru. Prvním je nenulová hodnota, která znamená, že klient chce změnit parametry spojení nebo vytvoření nového spojení v tomto spojení. Nulová hodnota značí přání klienta začít nové spojení s novými hodnotami,
- šifrovací metoda: klient pošle seřazený list šifrovacích metod, které podporuje. Šifry jsou prioritně seřazeny sestupně. Server jednu vybere a obnoví spojení s klientem,
- kompresní metoda: jedná se také o prioritně seřazený list kompresních metod podporovaných klientem.

Když server zprávu přijme, tak odešle zprávu s odpovědí, kde jsou vybrány přijatelné algoritmy pro oba účastníky. Jakmile ale server nenajde shodu mezi vlastními sadami a klientovými, odešle klientovi chybné hlášení, které obsahuje výpis parametrů a

podrobnosti o chybách. Nejčastější chyby jsou v neaktuálnosti protokolu na straně klienta. (30)

Následně po Hello zprávách server začíná fázi posílání vlastních certifikátů. Server může také vyžadovat klientův certifikát. Celý tento proces na straně serveru končí zasláním Hello done zprávy, dle které klient zjistí, že je řada na něm. Jestliže server zaslal žádost o klientův certifikát, klient jej musí poskytnout. (12)

Po obdržení Hello done zprávy klientem, klient zašle nazpět tyto zprávy: ClientKeyExchange, Certificate a CertificateVerify. Tyto typy zpráv budou popsány v následujícím seznamu:

- ClientKeyExchange: tato zpráva obsahuje tzv. PremasterSecret klíč. Z tohoto klíče se později vypočítá MasterSecret, které je označováno jako sdílené tajemství. PreMasterSecret je standardně šifrován veřejným klíčem,
- Certificate: je klientův certifikát. Může být vyžadován, ale nemusí. V případě, že není vyžadován, klient komunikuje se serverem anonymně,
- CertificateVerify: Jedná se o potvrzovací certifikát, na jehož základě může server ověřit totožnost klienta.

4.2.2 Finální fáze Handshake protokolu

Poslední fází Handshake protokolu je finální zpráva Change Cipher Specification. Tato zpráva slouží k ověření, že použité klíče a autentizace mezi dvěma subjekty byly úspěšné. Poslední jmenovaná zpráva je vlastně první zprávou chráněnou vybranou šifrou a klíči. (28). Názornou ukázku fáze Hanshake lze nalézt v příloze 1 obrázek 1 Handshake protokol.

4.2.3 Obnovení relace Handshake protokolu

První zmíněný postup se odehrává výhradně pro nastavení spojení. Když už jsme se serverem spojeni přenos mezi klientem a serverem probíhá rychleji. Pro obnovení relace se používají tyto čtyři základní principy.

1) Klient opět pošle serveru zprávu ClientHello, která obsahuje všechny výše uvedené atributy a navíc přidá identifikátor obnovované relace.
2) Server odpovídá klientovi také zprávou ServerHello, kde se opět nachází již zmíněné atributy a dále je zde taky použit identifikátor obnovované relace.

3) Server potvrzuje zvolení nových šifrovacích klíčů zprávou ChangeCipherSpec a pak ihned odešle poslední, již šifrovanou zprávu Finished.
4) Klient ukončí obnovení relace také zasláním zpráv ChangeCipherSpec a Finished. (12)

4.3 Record Layer Protocol

SSL Record Protocol přijímá data z nejvyšších vrstev SSL subprotokolů a fragmentovaných adresovaných dat o kompresi, autentizaci a šifrování. Protokol si bere jako vstupy bloky dat neurčité velikosti a produkuje na výstupu sérii SSL data fragmentů. Konečný SSL Record Protocol tedy obsahuje:

- content type: tento proces definuje nejvyšší vrstvu protokolu, která musí být použita,
- protocol version number: definuje, jaká verze protokolu má být použita (v současnosti se nejvíce používá 3.0),
- length: síla zabezpečení, jaké jsou vybrány metody (MD5, SHA),
- data payload: doprovodná data,
- MAC: Message Authentication Code, slouží k ověření neporušitelnosti zprávy. Obvykle je tvořen pomocí hashovací funkce například SHA. (29)

Jakákoli chyba při dešifrování zprávy (např. nesprávný MAC) znamená ukončení spojení.

4.4 Alert Protocol

Tento protokol se využívá v případě, že dojde k chybě v komunikaci. Díky tomuto protokolu má jedna strana možnost sdělit druhé, že je něco v nepořádku. Ve verzi SSL 3 a TLS 1 existují základní dva stupně upozornění:

- varující (1): SSL našlo problém, který není fatální a lze jej řešit,
- fatální (2): SSL našlo fatální error a okamžitě ukončuje přímé spojení.

Přehled základních upozornění pro SSL verzi 3 a TLS verzi 1 lze najít v publikaci SSL and TLS: Theory and Practice od autora Oppligera Rolfa. (28)

4.5 Certifikát X.509

Certifikát X.509 je mezinárodní forma, která definuje strukturu certifikátu. Předepisuje co má takovýto certifikát obsahovat:

1) verze certifikátu: číslo s verzí certifikátu,
2) sériové číslo: unikátní číslo certifikátu,
3) doba platnosti: od kdy do kdy certifikát platí,
4) veřejný klíč: většinou je délky 1204 bitů,
5) informace o certifikační autoritě,
6) informace o subjektu, jemuž je certifikát vydáván,
7) identifikace algoritmu, který bude používán pro podepisování.

Zde v tomto výpisu, jsou uvedené jen nejběžnější atributy certifikátu, v praxi dovoluje norma definovat řadu dalších položek a rozšíření. (12) Pro lepší představu jak certifikáty vypadají v praxi, jsou v příloze 1 této práce přiloženy dva obrázky, obrázek 2 certifikát ČSOB a obrázek 3 certifikát AirBank se stavem ke dni 14. 11.2015.

4.6 TLS

TLS protokol bývá označován jako nástupce SSL. Je konstrukčně shodný: je to klient /server protokol. Protokol TLS 1.0 vyšel v roce 1999 a je prakticky srovnatelný s protokolem SSL 3.0. (28) V praxi je více rozšířený protokol SSL.

4.7 OpenSSL

OpenSSL je kryptografická knihovna, která nabízí implementaci nejvíce doporučovaných algoritmů. Obsahuje algoritmy jako 3DES, AES, RSA a také hashovací a autentizační algoritmy. Jádro knihovny je napsané v programovacím jazyce C. Tato knihovna je distribuována jako open source a je dostupná pro většinu operačních systémů Unixovského tipu (Solaris, Mac OS X, BSD), OpenVMS a Microsoft Windows. (14)

4.7.1 Využití OpenSSL

OpenSSL se používá ke generování privátního klíče a CSR žádosti o vystavení SSL certifikátů. Disponuje však celou řadou užitečných funkcí, díky kterým můžeme například porovnat MD5 hash certifikátu a privátního klíče a zjistit jestli k sobě "sedí". Pomocí knihovny OpenSSL také můžeme ověřit správnost naší instalace SSL certifikátu na server.

4.7.2 Nejčastější typy OpenSSL certifikátů

Typy nejčastějších OpenSSL certifikátů jsou názorně zobrazeny v této tabulce. Tabulka popisuje formáty SSL certifikátů, způsoby uložení, nejčastější přípony souborů, servery využívající tuto službu a další informace.

4.8 Zobrazení certifikátu v různých prohlížečích

Na závěr této kapitoly autor odkazuje na čtyři přílohy snímků obrazovky nejběžnějších internetových prohlížečů, které jsou používány v Evropě. Na těchto snímcích jsou znázorněny ikony HTTPS, které značí použití šifrovaného zabezpečení pomocí TLS nebo SSL. Pro prezentaci snímků obrazovky autor použil stránku českého prodejce elektroniky www.alza.cz. Snímky jsou v příloze 1 označeny čísly 4-7.

5 Platební systémy

Platba přes Internet se stává nedílnou součástí našeho života. Usnadňuje nám každodenní činnosti a zejména nám šetří čas. V České republice je v průměru 53% lidí, kteří nakupují přes Internet, většina z nich volí platbu online platební kartou, nebo využívají pro platbu bankovní převod. Poměr plateb přes Internet můžete vidět v grafu, který je v příloze 1 označen jako obrázek číslo 8. Graf je převzat z Českého statistického úřadu (dále jen ČSU). Tato kapitola se bude zabývat platebními systémy pro platbu přes Internet.

5.1 Platba

Platba znamená převod prostředků od plátce k příjemci platby. Platba se může realizovat těmito způsoby:

- oběživem (hotové peníze),
- bankovní platbou (prostřednictvím vkladů na bankovních běžných účtech),
- kombinací oběživa a bankovní platby. (32)

5.2 Platební systém

Platební systém se jinými slovy nazývá systém převodu peněz nebo likvidity (Funds Transfer System, FTS). Může být provozován dvěma způsoby. První je založen na principu zúčtování a vypořádání jednotlivých položek při současné kontrole jejich krytí, druhý zase na principu zúčtování rozdílů sald vypočtených ze vzájemných pohledávek a závazků účastníků systému. Právně se hovoří o formální dohodě založené na soukromém kontraktu nebo na zákoně. Dohoda se vyznačuje vícenásobným členstvím, společnými pravidly a standardizovaným uspořádáním pro převod a vypořádání pohledávek a závazků mezi členy tohoto systému. (32)

5.2.1 Mezibankovní platební systém

Mezibankovní platební systém neboli systém mezibankovních převodů prostředků (Interbank Payment System, zkráceně IFTS) je systém, u kterého většinu nebo všechny přímé účastníky představují banky. Tento systém funguje na principu korespondenčního bankovnictví, prostřednictvím nostro a vostro účtů. Běžnou praktikou u těchto systému je, že měna těchto účtů je shodná s domácí měnou banky, u které je účet veden. Systém nostro

a vostro účtů znamená, že banky mají určitou banku či speciální nebankovní jednotku, která má vlastní zúčtovací centrum. (32)

Centrální mezibankovní platební systém funguje na základě převodu prostředků z účtu banky plátce na účet banky příjemce. Tyto převody probíhají v zúčtovacím centru centrální banky. Platby jsou prováděny u bank na základě příkazu svých klientů, předávaných formou písemných dokladů jako jsou příkazy k úhradě nebo třeba šeky, klienti mohou využít také technické prostředky, jako například datový nosič, počítač propojený elektronicky s bankou, hlasově běžným telefonem, zvláštní mobilní bankovní aplikací a v neposlední řadě lze využít i platební karta. Pokud probíhá platba v rámci jedné banky, tak banka využívá svoje vlastní zúčtovací centrum a neodkazuje se na centrální banku. (32)

Platby přes internet lze provádět pomocí:

- platební karty,
- bankovního převodu,
- mobilního telefonu,
- virtuální platební karty,
- dalších technologií.

5.3 Platební karta

Platební karta představuje moderní nástroj bezhotovostního platebního styku, využívaný zejména k úhradě spotřebních výdajů a výběru hotovosti. Platební karty slouží k rozšíření osobních běžných a úvěrových účtů bank a mají snahu překonat nedostatky šekového a zejména hotovostního platebního styku. Mají za cíl umožnit komitentům snadnější a bezpečnější dispozici jejich finančních prostředků. (21)

5.3.1 Náležitosti platební karty

Vzhled platebních karet a jejich formální i obsahové náležitosti jsou v mezinárodním měřítku standardizovány. Přehled základních náležitostí zobrazuje tabulka 1.

Údaje na kartě	
Označení vydavatele	název a logo příslušné banky
Číslo platební karty	16 - 19 číselných znaků (2 označí druh karty, 5 značí identifikaci banky, zbytek čísel identifikuje držitele)
Část čísla BIN	4 znaky identifikující banku (Bank Identification Number)
Platnost platební karty	udává začátek a konec platnosti karty
Jméno držitele	Obsahuje jméno držitele, může mít max 27 znaků
Podpisový proužek	vzor podpisu držitele, obvykle bývá na zadní straně
Záznam dat	dle typu karty, čipové, magnetické a laserové

Tabulka 1 Náležitosti platební karty (21)

5.3.2 Ověřovací údaje karty

Card Verification Value (CVV) je číselná hodnota na kreditní kartě, vynalezená pro masivní boj proti podvodům s platebními kartami. Existují dva základní typy CVV, které jsou často zaměňovány. První typ je zahrnut v magnetickém pásku karty a druhý typ, který je označován jako CVV2 je natisknut na zadní straně karty. Kód CVV2 je využíván pro platby přes Internet. Rozdíly mezi CVC a CVV2 jsou popsány v následujících tabulkách. (33) V příloze 1 jsou autorem přiloženy dva náhledy platební karty, jsou to obrázky 9 a 10.

Společnost	Kód	Jméno (anglicky)	Umístění	Délka
American Express	CSC	Card Security Code	Magnetický pásek	3
Discover	CVV	Card Verification Value	Magnetický pásek	3
JCB	CAV	Card Authentication Value	Magnetický pásek	3
MasterCard	CVC	Card Validation Code	Magnetický pásek	3
Visa	CVV	Card Verification value	Magnetický pásek	3

Tabulka 2 kódy CVV (32)

Společnost	Kód	Jméno (anglicky)	Umístění	Délka
American Express	CID	Card Identification Number	Přední strana karty	4
Discover	CID	Card Identification Number	Zadní strana karty	3
JCB	CAV2	Card Authentication Value 2	Zadní strana karty	3
MasterCard	CVC2	Card Validation Code 2	Zadní strana karty	3
Visa	CVV2	Card Verification value 2	Zadní strana karty	3

Tabulka 3 kódy CVV2 (32)

5.4 Internetové bankovnictví

Internetové bankovnictví nám umožňuje být 24 hodin denně 7 dní v týdnu ve spojení se svojí bankou. Prostřednictvím Internetu může uživatel převádět finanční prostředky do jiné banky, kontrolovat svoje odchozí a příchozí platby a spravovat svůj účet. Internetové bankovnictví šetří čas, odpadá nutnost uživatele chodit na pobočku svojí banky a provádět změny osobně. Existují základní tři typy spojení uživatele s bankou přes Internet: (34)

- internetově založené, používají standartní webový prohlížeč, přístup do banky je pomocí osobního účtu a online stránek banky,
- bankovní software, jedná se o speciální software, který si uživatel nainstaluje na svůj osobní PC, software vytvoří zabezpečené spojení přes Internet do klientovy banky,
- osobní finanční software, tento druh software dovoluje vyměňovat finanční informace s bankou, nejedná se o software vydaný bankou, ale jiným dodavatelem například Microsoftem, software není přímo spjatý s konkrétní bankou. (34)

5.4.1 Bankovnictví prostřednictvím mobilního telefonu

V poslední době přibývá uživatelů využívající mobilní telefon pro přístup k Internetovému bankovnictví. Pro přístup k internetovému bankovnictví lze využít prohlížeč mobilního telefonu anebo speciální aplikace distribuované bankami. Pomocí aplikace lze spravovat účet, odesílat platby a vykonávat mnoho dalších akcí v závislosti na druhu aplikace. (35) V České republice lze využít tyto mobilní aplikace (zobrazeny pouze nejznámější v rámci ČR): ČSOB SmartBanking, Mobilní bankovnictví od Air Bank, SERVIS 24 Mobilní banka od České spořitelny, Mobilní banka od komerční banky, Fio banka Smartbanking, Raiffeisen Smart Mobile a další. (zdroj https://play.google.com/store/apps)

5.4.2 Využívání QR kódů

V současné době se pomalu začíná pro platby používat čárový QR kód, který v sobě zahrnuje asymetrickou kryptografii s veřejným klíčem. Princip funkce spočívá na serveru, který bezpečně získá spolehlivě dva klíče a platební informace k zašifrování, poté vytvoří QR kód. Dále server odešle zákazníkovi QR kód s podklady pro platbu. Zákazník kód otevře nebo naskenuje vlastním zařízením. Speciální aplikace rozšifruje QR kód, vyplní uživateli

všechny náležitosti pro platbu a uživatel je pak jen potvrdí. Informace se odešlou nazpátek na server se zašifrovanou informací o úspěšné platbě. (35) Prvním průkopníkem této metody byla banka Raiffeisenbank, v současné době podporuje QR kódy v ČR již většina bank.

6 Zabezpečení plateb přes Internet

Pro zabezpečení plateb přes Internet vybral autor této práce dvě základní procedury platební bránu a 3D Secure. Dále zde autor popisuje alternativní možnosti a platby na Internetu.

6.1 Platební brána

Platební brána je on-line analogie fyzického zpracování terminálu kreditní karty, které můžeme najít ve většině maloobchodních prodejnách. Jejím úkolem je zpracovat údaje o kreditní kartě a vrátit výsledky zpět do uložiště systému. Můžete si představit, platební bránu jako prvek mezi internetovým obchodem a sítí kreditních karet. (36) Umístění a funkce platební brány je vidět na obrázku 11 v příloze 1.

6.1.1 Stavy při nákupu přes Internet pomocí kreditní karty

1) Zákazník po naplnění nákupního košíku s produkty úspěšně vstoupí do pokladny. Poté zákazník zadá informace o kreditní kartě a klikne na tlačítko zaplatit.
2) Nyní strana obchodníka pošle zabezpečené informace spolu s celkovou částkou na platební bránu.
3) Platební brána začne vykonávat několik rutinních procesů. Předá informace bankovnímu procesoru obchodníka, kde byl účet otevřen již dříve.
4) Všechny tyto informace jsou pak tímto procesorem odeslány do sítě kreditních karet. Visa a MasterCard jsou dvě z nejznámějších a nejpoužívanějších sítí kreditních karet.
5) Síť kreditních karet zpracovává platnosti kreditní karty a odesílá informace z kreditní karty do banky, pod kterou je karta zákazníka registrována.
6) Ve výsledku banka odmítne nebo schválí transakci a posílá informace zpět do sítě kreditní karty prostřednictvím stejného směrování, ale v opačném směru. Výsledná informace je nakonec převedena se speciálním kódem zpět do internetového obchodu. To vše se děje v několika sekundách a tok informací od platební brány je izolován od zákazníka i obchodníka. To znamená, že se nemusíme vypořádávat s tím, co se děje s daty po odeslání informací do platební brány. Stejně jako obchodník potřebujeme vědět jen výsledek transakce.

Po zpracování informací v síti kreditní karty v kroku šest, jsou prostředky transakce převedeny na účet obchodníka do sítě kreditních karet. Dále si obchodník může převést

finanční prostředky na svůj bankovní účet automaticky. (36) Toto je obecný princip pro platby kartou na Internetu.

6.2 3D Secure

3D Secure rozděluje internetovou transakci do množství koncepčních domén. Ve skutečnosti existují tři oblasti tak, že každá osoba nebo systém jsou v jedné nebo více doménách. Domény jsou obchodník, zákazník a banka. (37)

6.2.1 Princip 3D Secure

Po přihlášení se k 3D Secure e-commerce ve své bance je držitel karty připraven nakupovat v kterémkoli obchodním místě, kde má obchodník integrované 3D Secure. Obchodníkův server je integrován do serveru banky, která je schopna získat informace o držiteli karty a mít přístup k serveru emitenta. Ten potvrdí účast karty ve službě. Poté co držitel karty klikne na "Koupit", obchodníkův server plug-in odešle zprávu do platebního systému, kterým může být Visa nebo MasterCard. Systém obsahuje číslo účtu držitele karty. Prostřednictvím výměny zpráv na značce adresář a kontrola přístupu, server může určit, zda je držitel karty zapsán do 3D Secure. Zpráva je vrácena do obchodníkova serveru plug-in. V případě, že držitel karty je zapsán do systému 3D Secure a pokus o ověřování je k dispozici, zpráva obsahuje adresu URL příslušného serveru banky. Pokud není v systému 3D Secure, transakce proběhne klasicky bez zabezpečení 3D secure. (38)

Pokud je vše v pořádku obchodníkův server plug-in odešle požadavek na ověření přístupu k serveru prostřednictvím prohlížeče držitele karty. Server banky provádí rutinní ověřování definované vydavatelem karty. Může například vyžadovat, aby držitel karty zadal heslo, které může být fixní nebo OTP One Time Password (jednorázové heslo), které je generováno na jedno použití, nejčastěji přijde držiteli formou sms na mobilní telefon. Server banky odešle výsledky ověření do obchodníkova serveru Plug-in. Pokud zpráva s odpovědí obsahuje úspěšnou autentizaci, obchodníkův server Plug-in vrátí ověřovací odpověď obchodníkovi a transakce je hotová. (38)

Ve většině případů se využívá ještě zprostředkovatel, který přenáší data mezi bankou a obchodníkem. Výhodou tohoto principu je, že obchodník nezíská údaje z držitelovy karty. Celý princip je znázorněn v příloze 1 obrázkem 12.

6.3 Alternativní platby

Jiné platební metody než platba kreditní kartou se nazývají alternativní platby. Alternativní platební metody nabízí obchodníkům nové platební možnosti, které mohou nabídnout svým spotřebitelům, a které nevyžadují využití jedné z hlavních kreditních společností karet. Obchodníci a spotřebitelé využívají tyto alternativní typy plateb z mnoha důvodů. Základními hledisky jsou cena, bezpečnost/důvěra a snadnost použití. Nejznámější alternativní typ platby je služba PayPal, která se exponenciálně rozrostla a stává do značné míry tradičním způsobem platby. (39)

6.3.1 PayPal

PayPal je jedním z nejpopulárnějších a nejjednodušší systémů pro přijímání kreditních karet v internetovém obchodě. Účet v systému si lze představit jako běžný bankovní účet, který se dá ovšem přímo napojit na miliony internetových obchodů po celém světě a přesun peněz z účtu na účet probíhá téměř okamžitě. Dá se tak říci, že na internetu mají všichni tzv. „stejnou banku“. PayPal má dva hlavní produkty:

- PayPal Webová Platba Standard (Website Payment Standart),
- PayPal Webová Platba Pro (Website Payment Pro). (39)

Obě tyto platební metody poskytují jak platební bránu, tak i funkční obchodní účet. Rozdíl je ale v poplatcích za provedenou transakci. U prvního typu obchodník platí z každé započaté transakce určité procento, u druhého typu platí předem stanovenou taxu. Výhoda využití služby PayPal pro zákazníka je v rychlosti platby a vyvarováním se použitím při platbě kreditní kartou. Tím můžeme snížit riziko jejího zneužití. (39)

6.3.2 Virtuální internetová karta

Virtuální karta slouží pro platby na Internetu. Klient má přidělené speciální číslo platební karty. Číslo může být vytištěno na papíře anebo vyryto na kartě. Virtuální karta může existovat vedle skutečné platební karty a mít i vlastní výpis, nebo mohou být transakce

převáděny na účet hlavní karty. Tyto karty jsou v bezpečnostním žebříčku na předposledním místě za klasickou platební kartou využívanou pro platby přes Internet, ale přesto zajišťují vysokou bezpečnost. (40) V současné době se již moc nepoužívají. V Čechách se můžeme setkat s virtuální kartou u těchto společností:

- Komerční banka,
- Ebanka,
- GE money bank,
- Cetelem,
- a další.

6.3.3 Bitcoin

Bitcoin je decentralizovaná digitální měna. To znamená, že není osoba nebo instituce, která by mohla měnu podpořit nebo ji ovládat. Není kryta fyzickým zbožím, ani drahými kovy, protože Bitcoin je jen počítačový program. Pro platby se využívá soukromý a veřejný klíč, kdy plátce šifruje svým soukromým klíčem. Je tedy využita asymetrická kryptografie. V malém měřítku začínají firmy používat bitcoiny pro malé platby, wikipedie například přijímá sponzorské dary v bitcoinech pro provoz webu. (41) V Čechách se můžeme s bitcoiny setkat na burze nebo ve speciálních směnárnách, kde se dají bitcoiny směnit za jinou měnu.

Na závěr této kapitoly autor přikládá citaci o nebezpečí platby kartou z pohledu uživatele ve prospěch obchodníka. „Lidé, kteří si zvyknou platit platební kartou, utratí při koupích mnohem více peněz, než při platbě hotovostí. Většina obchodníků využívá psychologického poznatku, že peníze, které člověk nevidí, utratí snáze než hmatatelnou hotovost. S tímto poznatkem jsou obchodníci dobře obeznámení a jsou proto ochotni platit bankám vydávající karty nemalé poplatky za zprostředkování platby.“ (32)

7 Analýza zabezpečení uživatelů na Internetu

Tato část bakalářské práce se skládá z rešeršní analýzy pěti různých zdrojů. První dva zdroje jsou konkrétně zdroje britské a americké. Zbylé tři zdroje jsou od českých distributorů, dva jsou od českého statistického úřadu a poslední je z portálu www.dobryweb.cz. V následujících odstavcích autor podrobně popíše použité zdroje.

První analýza vychází z odborné publikace Assessing the Security Perceptions of Personal Internet Users od autorů: S.M. Furnella , P. Bryanta a A.D. Phippen. Tato analýza prezentuje výsledky z průzkumu od 415 domácích uživatelů z Velké Británie. Sbírání dat od respondentů probíhalo v roce 2006, a to od května do srpna formou dotazníků zaslaných emailem a zveřejněním na webových stránkách. Analýza vycházela z poznatků, že uživatelé internetu stále více zjišťují bezpečnostní hrozby při používání domácích počítačů.

Druhá použitá analýza vyhází z odborné publikace Anonymity, Privacy, and Security Online z roku 2013. Tento průzkum lidí na Internetu byl vytvořen na Carnegie Mellon Univerzitě ve Spojených státech amerických. Metoda získání respondentů, byla založena na telefonickém dotazování. Ankety se zúčastnilo 1002 dospělých jedinců starších 18 let. Dotazování probíhalo v období 11. až 14. června pomocí databáze čísel na pevné linky a mobilní telefony uživatelů. Výsledkem z dotazů na uživatele Internetu a mobilních telefonů bylo 792 dotázaných s odchylkou měření ±3,8%.

Pro porovnání se dvěma předešlými analýzami autor využil publikaci od portálu dobrýweb, ze které autor této práce využil tři zpracované otázky z celkových dvou okruhů. Sběr dat pro tuto analýzu probíhal 14 dní na známých českých webových serverech. Šetření se zúčastnilo 2894 respondentů.

Pro finální porovnání využil autor dvě zpracované práce z českého statistického úřadu (dále ČSU). První se nazývá Internetovými dovednostmi v Evropské Unii a v České republice. Zdrojové data jsou z Eurostatu pro rok 2015. Druhá publikace z ČSU má název Češi a Internet od paní Romany Malečkové.

7.1 Porovnání analýz

Všechny na rešerši použité analýzy využívají základní soubor respondentů ve věkové hranici od 16 let pro ČSU a od 18 pro zbylé analýzy. Největší věkové zastoupení bylo u respondentů ve věku 16-40 let a druhá nejvýraznější skupina byla s respondenty nad 50 let.

První otázka pro srovnání se týká využívání Internetu respondenty pro určité činnosti. Pro přehlednost autor přikládá zpracované grafy, které lze naleznout v příloze 2 pod označením obrázek 13-16. Z porovnání grafů vyplývá, že uživatelé Internetu nejvíce používají Internet k posílání e-mailů, hledání informací, nákupu zboží a v neposlední řadě k používání sociálních sítí. U sociálních sítí je vidět největší nárůst uživatelů, jak je zobrazeno na obrázku 14 v porovnání s obrázky 15 a 16, tento nárůst se týká spíše mladých lidí.

7.2 Citlivost a ochrana soukromí

Další část porovnání se věnuje citlivosti uživatelů na vlastní data a mapování jejich stopy na Internetu. První graf v příloze 2 s označením obrázek 17 nám znázorňuje míru zabezpečení uživatelských účtů k určité věkové hranici. Obrázek 17 popisuje důležitost autorizace k určitým činnostem na Internetu. Druhý graf s označením v příloze 2 obrázek 18 nám popisuje, jak se uživatelé snaží docílit větší bezpečnosti v prostředí Internetu a skrytí své identity. Z porovnání obou grafů lze vyčíst, že uživatelé Internetu jsou si vědomi hrozeb a snaží se zabránit sledování činností, které na Internetu vykonávají.

7.3 Analýza bezpečnosti uživatelů

Závěr této kapitoly patří analýze znalosti bezpečnostních pojmů uživateli na Internetu. Pro tuto analýzu není srovnání z více zdrojů, a proto vychází z poznatků pouze jedné publikace stavějící na odpovědích respondentů ve Velké Británii. První graf se týká problematiky znalosti pojmů ze světa Internetu, nalezneme ho v příloze 2 s označením obrázek 19. Z grafu je zřejmé, že většina uživatelů zná nejznámější ustálené pojmy. Největší potíže dělaly uživatelům pojmy phishing (podvodné emaily vydávající se za uživatelovu banku) (42) (43), spyware (program pro odesílaní dat o uživateli) (44) (45), červ (program, který se rozesílá sám a přebírá kontrolu nad pc) (44) (46) a trojský kůň (skrytý program, se kterým uživatel nesouhlasí) (44) (46) . Druhý graf nám znázorňuje míru využívání

bezpečnostních programů uživateli, tento graf nalezneme v příloze 2 pod obrázkem 20. Z průzkumu vyšlo najevo, že většina uživatelů používá pro zabezpečení nejvíce antivirové programy a bránu firewall. Poměrně velké zastoupení mají i antispyware programy se 77% a antispamové programy s 60%.

Poslední část této kapitoly patří grafu, který nalezneme v příloze 2 pod označením obrázek 21. Graf je zaměřen na míru uživatelů, kteří pravidelně aktualizují své bezpečnostní programy. Z výzkumu je zřejmé, že uživatelé neberou vážně hrozby číhající na Internetu a velmi málo často aktualizují jejich bezpečnostní programy. Nejvíce uživatelů se snaží mít aktuální databázi u antivirového programu 63%, dále se snaží bránit proti spyware 47%. Nejhůře dopadli aktualizace operačního systému 38% a firewallu s 37%.

7.4 Shrnutí analýz

Na závěr této kapitoly by autor chtěl říct, že by mělo být provedeno nové šetření přímo zaměřené na problematiku plateb na Internetu a znalosti hrozeb při těchto platbách. Z analýz grafů uvedených v této kapitole vyplývá, že se objevuje určitá neznalost speciálních termínů, u kterých má část uživatelů nedostatečné znalosti. Dále je z grafů viditelné, že Internet se stává nepostradatelnou součástí každodenního života a je potřeba se na něm chránit.

8 Praktická část

V této části bakalářské práci bude vytvořen návrh UI specifikace bezpečného dobíjení finančních prostředků do platebního systému (dále jen PS) z pohledu uživatele a administrátora. Pro návrh systému bude využita UI specifikace popsaná v samostatné části této bakalářské práce.

8.1 Návrh platebního systému

Pomocí UI specifikace bude nastíněn model systému s databází, do kterého se mohou dobíjet finanční prostředky. Pro dobíjení do PS lze využít klasickou přepážku s pokladnou, platební automaty pro dobíjení, mobilní telefon s aktivovanými prémiovými sms zprávami a zařízení s přístupem na Internet, ze kterého lze provést bankovní převod nebo zaplatit kartou online.

Každý uživatel PS bude mít k přístupu do systému vlastní účet, do kterého se bude moci dostat pomocí svého uživatelského jména a hesla. K přihlašovacím údajům bude mít dále každý uživatel čipovou kartu a možnost mít i čipovou samolepku, kterou může nalepit na oblíbený přívěšek nebo mobilní telefon. Pro placení v rámci organizace půjde využít pouze čipových zařízení. Placení lze využít u všech zařízení a služeb, které budou tento typ transakce podporovat, nejčastěji se bude jednat o nápojové automaty a stravovací zařízení.

Kvůli větší bezpečnosti a menší míře zneužití půjdou finanční prostředky vybrat ze systému pouze na klientském centru PS, kde bude moci uživatel využít vrácení peněz hotově nebo na účet. Tímto opatřením lze docílit zamezení míry zneužití účtu na Internetu, kde bude možné finanční prostředky pouze dobíjet.

Platební systém bude tvořen vnitřní sítí s omezeným přístupem na Internet. Pro komunikaci s uživateli je v systému implementována Internetová aplikace, která je zabezpečena nejnovějším firewallem a SSL protokolem. Data uchovávaná o uživatelích v rámci systému jsou zašifrována. V příloze 3 pod označením obrázek 22 je přiložený kontextový diagram pro lepší představení systému.

8.2 Persony (aktéři)

Persony jsou autorem blíže popsány v této práci v samostatné kapitole. Pro tento návrh UI specifikace byly vymodelovány autorem tyto persony, mají určené archetypy tak, aby se co nejvíce přiblížili PS. Lidé pracující s tímto systémem budou různého charakteru a věku. Jako vzorové osobnosti byly vybrány dvě osobnosti (aktéři), kteří budou se systémem pracovat.

8.2.1 Aktér 1

Jméno a příjemní: Zuzana Křečková.

Věk: 23.

Povolání: studentka 3. ročníku na univerzitě.

Frekvence využívání PS: 3x týdně.

Role v systému: klasický registrovaný uživatel.

Stručný popis aktéra 1

Zuzana je studentkou třetího ročníku vysoké školy. PS využívá pouze pro placení obědů ve školní menze. Zuzana je občas zapomnětlivá a nestíhá si pravidelně dobíjet svůj interní účet. Proto velmi často využívá funkci dobití pomocí sms zprávy nebo dobíjí platební kartou.

Normální den aktéra 1

Zuzky normální den začíná snídaní, následně se vydává do školy na ranní přednášky. V poledne chodí na oběd do školní menzy, zde platí interní čipovou kartou. Odpoledne chodí na cvičení a přednášky. Na univerzitě si kupuje občerstvení z automatu. Po 17 hodině chodí domů odpočívat a trávit zbylý volný čas hraním online her. V dny, kdy Zuzana nechodí na univerzitu, se snaží docházet na brigády.

8.2.2 Aktér 2

Jméno a příjmení: Radim Brzobohatý

Věk: 42.

Povolání: pracovník organizace s PS.

Frekvence využívání PS: 5x týdně.

Role v systému: administrátor.

Stručný popis aktéra 2

Radim je administrátorem v organizaci využívající tento PS. Pracuje v klientském centru PS. Je ve styku s uživateli, provádí základní úkony se systémem, přidává uživatele, zakládá účty, konfiguruje platební čipové karty a udržuje plynulý chod systému.

Normální den aktéra 2

Radimův normální den začíná v 7 hodin ráno, po snídani vyráží na své pracoviště v klientském centru. Zde má normální pracovní 8 hodinovou směnu. Radim je ve styku s klienty a platebním systémem, řeší každodenní rutinní operace v systému.

8.3 Případy užití (Use Case)

V této části jsou vytvořeny případy užití. Pro tyto případy užití je vytvořeno UML schéma, které můžeme nalézt v příloze 4 pod označením obrázek 23.

8.3.1 **Případ užití 1:** dobití prostředků v automatu

Krátký popis: Use Case umožňuje dobití finančních prostředků pomocí automatu.

Podmínky pro spuštění

Uživatel musí být přihlášen v systému a dobíjet prostřednictvím automatu.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	vygeneruje formulář pro výběr typu dobití	s tlačítky hotově a kartou
2	uživatel	zvolí jeden typ dobití a potvrdí kliknutím	
3	systém	umožní uživateli provést zvolenou metodu dobíjení	
4	uživatel	dobije finanční prostředky	kartou nebo hotově
5	systém	uloží data a připíše uživateli prostředky	po dokončení zobrazí zůstatek

Tabulka 4 Use Case 1 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
3.I	uživatel	mění metodu platby	použije tlačítko zpět
3.II	systém	vrátí uživatele na úvodní formulář	tok pokračuje krokem 2

Tabulka 5 Use Case 1 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
3.I	uživatel	zadá špatné heslo u dobíjení kartou	
3.II	systém	upozorní uživatele a nechá ho zadat platné heslo	
3.III	uživatel	zadá platné heslo	tok pokračuje krokem 4

Tabulka 6 Use Case 1 alternativní tok 2 (vlastní zpracování)

Alternativní tok 3

Krok	Role	Akce	Poznámka
1.I	uživatel	odebere předčasně čtecí zařízení	
1.II	systém	uživatele odhlásí a neuloží data	

Tabulka 7 Use Case 1 alternativní tok 3 (vlastní zpracování)

Podmínky pro dokončení

Dobíjená částka bude připsána na účet uživatele.

8.3.2 **Případ užití 2:** dobití prostředků kartou online

Krátký popis: Use Case umožňuje dobití finančních prostředků pomocí karty online.

Podmínky pro spuštění

Uživatel musí být přihlášen v internetové aplikaci systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	zobrazí uživateli stránku pro kartu online	
2	systém	nechá uživatele zadat dobíjenou částku	nesmí být záporná
3	uživatel	zadá částku a odešle požadavek na zpracování	
4	systém	přesměruje uživatele na poskytovatele online platby	
5	uživatel	dobije prostředky v externím systému	
6	systém	získá data ze sítě platebních karet	
7	systém	uloží data a připíše uživateli prostředky	

Tabulka 8 Use Case 2 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
5.I	externí systém	zašle data o neúspěšné platbě	
5.II	systém	přesměruje uživatele na zadání nové platby	
5.III	uživatel	zadá novou částku	tok pokračuje krokem 3

Tabulka 9 Use Case 2 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
4.I	uživatel	zadá neplatné údaje z karty	
4.II	externí systém	upozrní uživatele a vyzve k zadání správných hodnot	
4.III	uživatel	zadá platné hodnoty	tok pokračuje krokem 5

Tabulka 10 Use Case 2 alternativní tok 2 (vlastní zpracování)

Alternativní tok 3

Krok	Role	Akce	Poznámka
1.I	uživatel	neprovede v průběhu 10 minut žádnou akci	
1.II	systém	odhlásí uživatele z externí webové aplikace	

Tabulka 11 Use Case 2 alternativní tok 3 (vlastní zpracování)

Podmínky pro dokončení

Dobíjená částka bude připsána na účet uživatele.

8.3.3 **Případ užití 3:** dobití prostředků převodem na účet

Krátký popis: Use Case umožňuje dobití finančních prostředků pomocí klasického bankovního převodu z účtu na učet.

Podmínky pro spuštění

Uživatel musí být přihlášen v internetové aplikaci systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	zobrazí informace pro platbu převodem na účet	
2	uživatel	zadá platební údaje do internetového bankovnictví	u banky dle uživatele
3	systém	čeká na potvrzení z banky	
4	systém	uloží data a připíše uživateli prostředky	

Tabulka 12 Use Case 3 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
1.I	uživatel	zná platební údaje	pokračuje rovnou na tok 2

Tabulka 13 Use Case 3 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
1.I	uživatel	neprovede v průběhu 10 minut žádnou akci	
1.II	systém	odhlásí uživatele z externí webové aplikace	

Tabulka 14 Use Case 3 alternativní tok 2 (vlastní zpracování)

Podmínky pro dokončení

Dobíjená částka bude připsána na účet uživatele.

8.3.4 **Případ užití 4:** dobití prostředků sms zprávou

Krátký popis: Use Case umožňuje dobití finančních prostředků pomocí sms zprávy.

Podmínky pro spuštění

Uživatel musí být přihlášen v internetové aplikaci systému a vlastnit mobilní telefon.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	zobrazí informace pro sms platbu	
2	uživatel	napíše sms zprávu s definovanými parametry	uživatelské jméno
3	uživatel	odešle zprávu na předem stanovené číslo	konec čísla dle velikosti částky
4	systém	získá potvrzení od mobilního operátora	sms zprávou
5	systém	uloží data a připíše uživateli prostředky	

Tabulka 15 Use Case 4 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
3.I	uživatel	zašle na špatné číslo nebo napíše špatný tvar zprávy	
3.II	mobilní operátor	zašle sms o špatném tvaru sms nebo čísla	
3.III	uživatel	upraví sms zprávu a odešle	pokračuje rovnou na tok 3

Tabulka 16 Use Case 4 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
1.I	uživatel	zná údaje pro sms platbu	pokračuje rovnou na tok 2

Tabulka 17 Use Case 4 alternativní tok 2 (vlastní zpracování)

Alternativní tok 3

Krok	Role	Akce	Poznámka
1.I	uživatel	neprovede v průběhu 10 minut žádnou akci	
1.II	systém	odhlásí uživatele z externí webové aplikace	

Tabulka 18 Use Case 4 alternativní tok 3 (vlastní zpracování)

Podmínky pro dokončení

Dobíjená částka bude připsána na účet uživatele

8.3.5 **Případ užití 5:** zjištění aktuálního stavu účtu.

Krátký popis: Use Case umožňuje zobrazení aktuálního stavu účtu.

Podmínky pro spuštění

Uživatel musí být přihlášen v internetové aplikaci systému nebo v dobíjecím automatu.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	zobrazí uživateli aktuální zůstatek	
2	uživatel	vytiskne účtenku	

Tabulka 19 Use Case 5 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
1	uživatel	nechce vytisknout účtenku	
2	systém	stornuje tisk účtenky	

Tabulka 20 Use Case 5 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
1.I	uživatel	neprovede v průběhu 10 minut žádnou akci	
1.II	systém	odhlásí uživatele z externí webové aplikace	

Tabulka 21 Use Case 5 alternativní tok 2 (vlastní zpracování)

Podmínky pro dokončení

Zobrazení aktuálního stavu účtu uživateli.

8.3.6 **Případ užití 6:** platba v systému

Krátký popis: Use Case umožňuje uživateli platbu v rámci systému.

Podmínky pro spuštění

Uživatel musí být přihlášen v systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	odešle data o uživateli	
2	pokladní systém	čeká na provedení platby	
3	uživatel	provede platbu	
4	systém	uloží změny a odečte uživateli zvolenou částku	
5	pokladní systém	vytiskne uživateli účtenku	

Tabulka 22 Use Case 6 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
1.I	uživatel	odebere předčasně čtecí zařízení	
1.II	systém	uživatele odhlásí a neuloží data	

Tabulka 23 Use Case 6 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
3.I	uživatel	nemá dostatečnou částku na účtu	
3.II	systém	neprovede platbu a upozorní uživatele	
3.III	systém	zobrazí zůstatek a umožní změnit transakci	
3.IV	uživatel	změní položky v transakci	pokračuje na tok 2

Tabulka 24 Use Case 6 alternativní tok 2 (vlastní zpracování)

Podmínky pro dokončení

Systém odepíše uživateli finanční prostředky z účtu.

8.3.7 **Případ užití 7:** přidání uživatele do systému

Krátký popis: Use Case umožňuje administrátorovi dělat úpravy v rámci systému. Administrátor může přidat uživatele do systému.

Podmínky pro spuštění

- Administrátor musí být přihlášen v systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	umožní administrátorovi provádět změny	
2	systém	umožní přidat nového uživatele	
3	administrátor	zadá údaje o novém uživateli	
4	systém	uloží záznam do databáze	
5	administrátor	nastaví přihlašovací údaje a čip	
6	systém	uloží změny do databáze	účet je ihned aktivní

Tabulka 25 Use Case 7 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
1.I	administrátor	zadá existujícího uživatele	
1.II	systém	upozorní a vyzve k opravení hodnot	pokračuje na tok 2

Tabulka 26 Use Case 7 alternativní tok 1 (vlastní zpracování)

Podmínky pro dokončení

Systém uloží nového uživatele.

8.3.8 **Případ užití 8:** odebrání uživatele ze systému

Krátký popis: Use Case umožňuje administrátorovi dělat úpravy v rámci systému. Administrátor může odebrat uživatele ze systému.

Podmínky pro spuštění

- Administrátor musí být přihlášen v systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	umožní administrátorovi provádět změny	
2	systém	umožní odebrat uživatele	
3	administrátor	vybere uživatele	dle ID, čipu
4	systém	vymaže uživatele ze systému	

Tabulka 27 Use Case 8 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
3.I	administrátor	maže uživatele s nenulovým zůstatkem	
3.II	systém	upozorní uživatele na zůstatek	
3.III	systém	nepovolí uživatele vymazat	přesměruje na tok 1

Tabulka 28 Use Case 8 alternativní tok 1 (vlastní zpracování)

Alternativní tok 2

Krok	Role	Akce	Poznámka
3.I	administrátor	chce smazat aktuální přihlášený účet administrátora	nelze mazat svůj účet
3.II	systém	upozorní a zobrazí výtrahu	
3.III	systém	nepovolí smazat účet	přesměruje na tok 1

Tabulka 29 Use Case 8 alternativní tok 2 (vlastní zpracování)

Podmínky pro dokončení

Systém odebere uživatele z databáze.

8.3.9 **Případ užití 9:** úprava uživatele v systému

Krátký popis: Use Case umožňuje administrátorovi dělat úpravy v rámci systému. Administrátor může upravit uživatele v systému.

Podmínky pro spuštění

- Administrátor musí být přihlášen v systému.

Základní tok

Krok	Role	Akce	Poznámka
1	systém	umožní administrátorovi provádět změny	
2	systém	umožní upravovat uživatele	
3	administrátor	vybere uživatele	dle ID, čipu
4	systém	načte uživatele	
5	administrátor	upraví hodnoty	
6	systém	uloží vytvořené změny	

Tabulka 30 Use Case 9 základní tok (vlastní zpracování)

Podmínky pro dokončení

Systém upraví uživatele v databázi.

8.3.10 **Případ užití 10:** vrácení finančních prostředků uživateli

Krátký popis: Use Case umožňuje administrátorovi vrátit peněžní prostředky uživateli. Peníze mohou být vráceny hotově z pokladny nebo zaslány na účet uživatele.

Podmínky pro spuštění

- Administrátor musí být přihlášen v systému.

- Uživatel musí být přihlášen do systému

Základní tok

Krok	Role	Akce	Poznámka
1	systém	umožní provádět změny na účtu uživatele	pouze pro administrátory
2	uživatel	zvolí částku pro výběr a metodu výběru	
3	administrátor	zkontroluje a zadá hodnoty do systému	
4	systém	odešle data do pokladního systému	
5	administrátor	vrátí peníze hotově, nebo vytvoří příkaz k úhradě	
6	pokladní systém	vytiskne účtenku a vrátí data do systému	
7	systém	odečte uživateli částku a uloží do databáze	dle ID

Tabulka 31 Use Case 10 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
2.I	uživatel	zvolí větší částku, než disponuje	
2.II	systém	upozorní uživatele a zobrazí zůstatek	
2.III	systém	nepovolí výběr	přesměruje na 2 krok

Tabulka 32 Use Case 10 alternativní tok 1 (vlastní zpracování)

Podmínky pro dokončení

Vrácení peněz uživateli.

8.3.11 **Případ užití 11:** zaslání potvrzení emailem

Krátký popis: Use Case systém umožňuje odeslat potvrzení o proběhlé platbě.

Podmínky pro spuštění: vykonání alespoň jedné z těchto akcí.

- Dobití prostředků v automatu.
- Dobití prostředků kartou online.
- Dobití prostředků převodem na účet.
- Dobití prostředků sms zprávou.

Základní tok

Krok	Role	Akce	Poznámka
1	uživatel	provedl platbu	
2	systém	vygeneruje zprávu a odešle uživateli	
3	systém	zaznamená událost do databáze	

Tabulka 33 Use Case 11 základní tok (vlastní zpracování)

Alternativní tok 1

Krok	Role	Akce	Poznámka
2.I	uživatel	má zadaný špatný email	
2.II	systém	systém dostane zprávu o nedoručení	
2.III	systém	odešle zprávu administrátorovi	
2.IV	administrátor	zajistí změnu emailu	kontaktuje uživatele
2.V	systém	uloží záznam do databáze	

Tabulka 34 Use Case 11 alternativní tok 1 (vlastní zpracování)

Podmínky pro dokončení

Odeslání emailu uživateli.

8.4 Diagramy datových toků (DFD)

Na závěr praktické části návrhu UI specifikace platebního systému autor přikládá vytvořené DFD diagramy navazující na problematiku Use Case. Diagramy jsou popsané tabulkami, které nalezneme v příloze 5 pod označením tabulka 39-45. V tabulkách jsou vypracované datové toky pro platební systém z pohledu uživatele a administrátora. Jednotlivé grafy se nachází v příloze 6 této práce pod označením obrázek 24 – 34.

9 Závěr bakalářské práce

Hlavním cílem bakalářské práce bylo analyzovat možnosti zabezpečení dat na Internetu v oblasti realokace finančních prostředků mezi elektronickými systémy. V teoretické části byly charakterizovány vybrané pojmy a problematika, ve které se využívá realokace finančních prostředků. Dále byly popsány nezbytné metody a principy potřebné k zabezpečení dat na Internetu.

Na tvorbu rešeršní části práce byly použity odborné a vědecké zdroje v elektronické podobě. V této práci převažují zejména zahraniční tituly významných osobností. Při dohledávání kvalitních zdrojů a titulů se nejvíce osvědčily databáze Ebrary, ScienceDirect a Google Scholar.

Dílčím cílem bakalářské práce bylo analyzovat úroveň zabezpečení uživatelů na Internetu a jejich znalost problematiky bezpečnosti v prostředí Internetu. V této části bylo porovnáno pět analýz od čtyř zdrojů, které byly české a zahraniční. Analýzy se zaměřovaly především na využívání Internetu uživateli, míru citlivosti na data uživatelů v prostředí Internetu a znalost základních pojmů z bezpečnosti na Internetu. Dle průzkumů vyplynulo, že většina uživatelů si je vědoma hrozeb v prostředí Internetu a snaží se jim předcházet. Analýza problematiky zabezpečení plateb přes Internet se ukázala nedostatečná. Autor této práce by chtěl v navazující diplomové práci toto téma více rozšířit a analyzovat do hloubky.

Samotná vlastní práce byla založena na tvorbě UI specifikace z pohledu uživatele a administrátora pro bezpečné dobíjení finančních prostředků do informačního platebního systému. Prostřednictvím UML bylo vytvořeno schéma případů užití platebního systému s DFD diagramy pro popis datových toků platebního systému. V návrhu systému byla zohledněna možnost uživatele dobíjet finanční prostředky z různých zdrojů. Uživatel může dobíjet prostředky do platebního systému pomocí platební karty, prémiové sms zprávy a hotovosti. Při tvorbě UI specifikace byla využívaná metoda citově interakčního designu pro lepší koordinaci mezi uživatelem a systém. K základním funkcím dobíjení do platebního systému byly dále vytvořeny případy užití pro platbu v systému, načtení zůstatku, výběr prostředků, přidání, odebraní a editování uživatele. Tyto případy jsou také popsány datovými toky v přiložených přílohách.

10 Seznam obrázků v práci

11 Seznam obrázků v příloze

12 Seznam tabulek

13 Zdroje citací

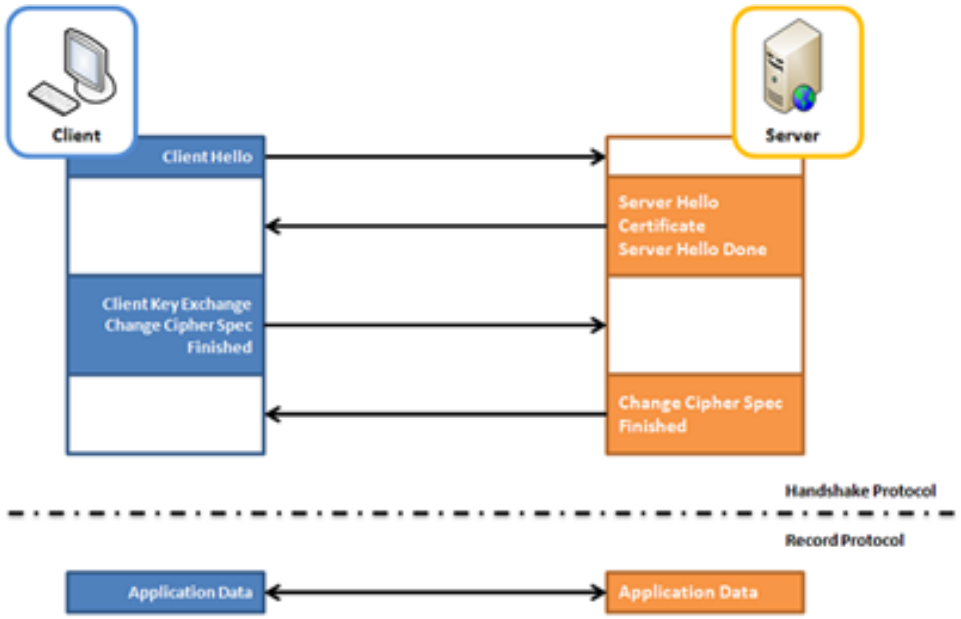
1. **Alan Cooper, Robert Reimann, David Cronin, Christopher Noessel.** *About Face: The Essentials of Interaction Design.* New York : John Wiley & Sons, 2014. 9781118766583.
2. **Goodwin, Kim.** *Designing for the Digital Age: How to Create Human-Centered Products and Services.* Chichester : John Wiley & Sons, 2011. 9781118079881.
3. **Galitz, Wilbert O.** *The Essential Guide to User Interface Design: An Introduction to GUI Design Principles and Techniques.* Indianapolis : Wiley Pub, 2007. 9780470146224.
4. **Jenny Preece, Yvonne Rogers, Helen Sharp.** *Interaction Design: Beyond Human-Computer Interaction.* New Jersey : John Wiley & Sons, 2015. 9781119020752.
5. **Pavlíček, Josef.** *Interakce člověk počítač [přednáška].* Praha : PEF ČZU, 2014.
6. **Ing. Ivan Vrana, DrSc.** *Projektování informačních systémů.* Praha : Credit, 2005. 80-213-0666-1.
7. **Fowler, Martin.** *Destilované UML.* Praha : Grada, 2009. 9788024720623.
8. **Sklenák, Vilém.** *Data, informace, znalosti a Internet.* Praha : C.H. Beck, 2001. 9788071794097.
9. **R. Rowlingson, Robert.** *Essential Guide to Home Computer Security.* Swindon : British Informatics Society, 2011. 9781906124694.
10. **Budiš, Petr.** *Elektronický podpis a jeho aplikace v praxi.* Olomouc : ANAG, 2008. 9788072634651.
11. **Purser, Steve.** *A Practical Guide to Managing Information Security.* Norwood : Artech House, 2004. 9781580537032.
12. **Bitto, Ondřej.** *Šifrování a biometrika.* Kralice na Hané : Computer Media s.r.o. 2005, 2005. 8086686485.
13. **Prokop, Jiří.** *Algoritmy v jazyku C a C++ - 2., rozšířené a aktualizované vydání.* Praha : Grada Publishing a.s., 2012. 9788024739298.
14. **John Viega, Matt Messier, Pravir Chandra.** *Network Security with OpenSSL: Cryptography for Secure Communications.* Sebastopol : O'Reilly Media, Inc., 2002. 9780596551971.
15. **Cobb, Chey.** *Cryptography For Dummies.* Hoboken : John Wiley & Sons, 2004. 9780764568312.
16. **Nemati, Hamid R.** *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering: Information Encryption and Cyphering.* Hershey : Information Science Reference, 2010. 9781615207848.
17. **Goutam Paul, Subhamoy Maitra.** *RC4 Stream Cipher and Its Variants.* Boca Raton : CRC Press, 2011. 9781439831359.
18. **Yan, Song Y.** *Cryptanalytic Attacks on RSA.* New York : Springer , 2007. 9780387487427.
19. **Kwangjo Kim, Tsutomu Matsumoto.** *dvances in cryptology--ASIACRYPT '96: International Conference on the Theory and Application of Cryptology and Information Security, Kyongju, Korea.* New York : Springer Science & Business Media, 1996. 9783540618720.
20. **Charles P. Pfleeger, Shari Lawrence Pfleeger.** *Security in Computing.* Upper Saddle River : Prentice Hall Professional, 2003. 9780130355485.
21. **Miroslav, Máče.** *Platební styk: klasický a elektronický.* Praha : Grada Publishing a.s., 2006. 8024717255.
22. **Boyles, Tim.** *CCNA Security Study Guide: Exam 640-553.* New York : John Wiley & Sons, 2010. 9780470636336.
23. **Ghaoui, Claude, John M. Carroll.** *Encyclopedia of Human Computer Interaction.* Hershey PA : Idea Group Inc (IGI), 2005. 9781591407980.
24. **Rogers, Yvonne.** *HCI theory: classical, modern, and contemporary.* San Rafael : Morgan & Claypool Publishers, 2012. 9781608459001.
25. **DIX, Alan, Janet FINLAY, Gregory D ABOWD a R BEALE.** *Human-computer interaction. Third edition.* Harlow : Pearson Education, 2004. 9780130461094.
26. **Cooper, Alan.** *The inmates are running the asylum.* Indianapolis : Sams, 2004. 0672326140.
27. **Green, T. R. G.** *Instructions and Descriptions: some cognitive aspects of programming and similar activities.* Leeds : University of Leeds, 2000.
28. **Oppliger, Rolf.** *SSL and TLS: Theory and Practice.* Norwood : Artech House, 2014. 9781596934481.
29. —. *Security Technologies for the World Wide Web.* Norwood : Artech House, 2003. 9781580535854.
30. **Rhee, Man Young.** *Internet Security: Cryptographic Principles, Algorithms and Protocols.* Hoboken : John Wiley & Sons, 2003. 9780470852859.
31. **Josef, Jílek.** *Finance v globální ekonomice I: Peníze a platební styk.* Praha : Grada Publishing a.s., 2013. 9788024738932.
32. **Gomzin, Slava.** *Hacking Point of Sale : Payment Application Secrets, Threats, and Solutions.* Indianapolis : John Wiley & Sons, Incorporated, 2014. 9781118810101.
33. **Verlag, Wiesbaden: Vieweg+Teubner.** *Electronic Banking: The Ultimate Guide to Business and Technology of Online Banking.* New York : Springer Science & Business Media, 2013. 9783322866271.

34. **Mejstřík, Michal, Pečená, Magda, Teplý, Petr.** *Bankovnictví v teorii a praxi: Banking in theory and practice.* Praha : Karolinum, 2014. 9788024628707.
35. **Yilmaz, Murat.** *OpenCart 1.4 Beginner's Guide : Build and manage professional online shopping stores easily using OpenCart.* Birmingham : Packt Pub, 2010. 9781849513036.
36. **Dr. Keith Mayes University of London, Konstantinos Markantonakis.** *Smart Cards, Tokens, Security and Applications.* New York : Springer Science & Business Media, 2007. 9780387721989.
37. **Verdinand, Karl C.** *Computer Science, Technology and Applications : Computer Science Research and Technology.* New York : Nova, 2011. 9781617286889.
38. **Montague, David A.** *Essentials of Online Payment Security and Fraud Prevention.* Hoboken : John Wiley & Sons, 2010. 9780470915127.
39. **Pavel, Juřík.** *Platební karty: Velká encyklopedie - 1870-2006.* Praha : Grada Publishing a.s., 2006. 8024713810.
40. **Guttmann, Benjamin.** *The Bitcoin Bible: All you need to know about bitcoins.* Norderstedt : BoD – Books on Demand, 2013. 9783732284320.
41. **Markus Jakobsson, Steven Myers.** *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* Hoboken : John Wiley & Sons, 2006. 9780470086094.
42. **Rachael Lininger, Russell Dean Vines.** *Phishing: Cutting the Identity Theft Line.* Hoboken : John Wiley & Sons, 2005. 9780764599224.
43. **Erbschloe, Michael.** *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code.* Burlington : Butterworth-Heinemann, 2004. 9780080519685.
44. **Yang, John S.** *Spyware.* New York : Novinka Books, 2005. 9781594546488.
45. **Axelrod, Evan M.** *Violence Goes to the Internet: Avoiding the Snare of the Net.* Springfield : Charles C Thomas Publisher, 2009. 9780398079833.
46. *Assessing the security perceptions of personal Internet users.* **S.M. Furnell, P. Bryant, A.D. Phippen.** United Kingdom : Computers & Security, 7. březen 2007.
47. **Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden.** Anonymity, Privacy, and Security Online . *www.pewresearch.com.* [Online] 5. září 2013. http://www.huntonprivacyblog.com/wp-content/files/2013/09/PIP_AnonymityOnline_090513.pdf.
48. **Bill, Moggridge.** *Designing interactions.* Cambridge : MIT Press, 2007. 978-0-262-13474-3.
49. **Qi, Ershi.** *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation: Innovation and Practice of Industrial Engineering and Management.* New York City : Springer, 2015. 9789462391451.
50. **Ristic, Ivan.** *OpenSSL Cookbook: A Guide to the Most Frequently Used OpenSSL Features and Commands.* London : Feisty Duck, 2013. 9781907117053.

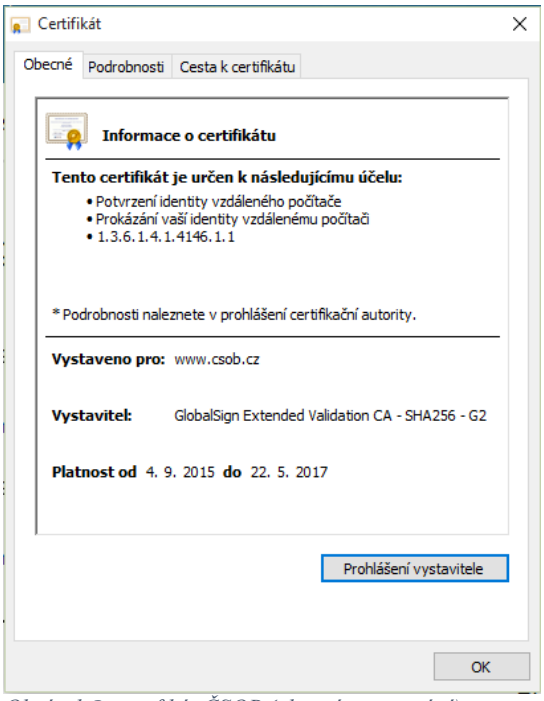
14 Přílohy bakalářské práce

V přílohách této bakalářské práce se nachází obrázky, grafy a tabulky odkazované v práci. Přílohy jsou rozdělené do pěti sekcí.

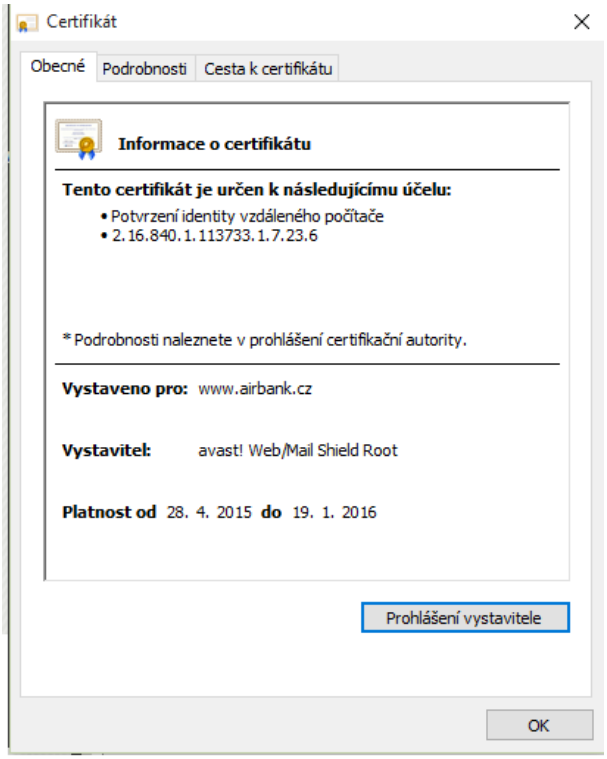
14.1 Příloha 1 obrázky



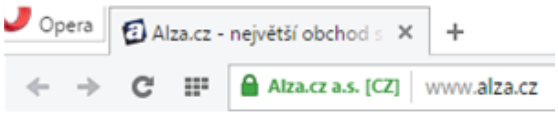
Obrázek 1 Handshake protokol (29)



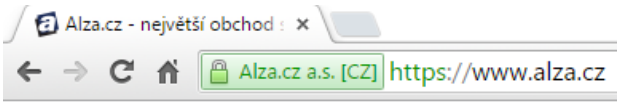
Obrázek 2 certifikát ČSOB (vlastní zpracování)



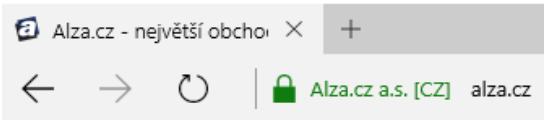
Obrázek 3 certifikát Air Bank (vlastní zpracování)



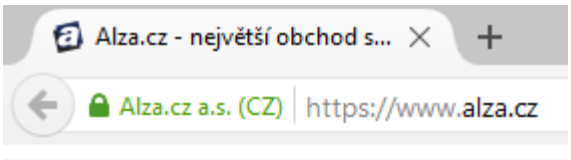
Obrázek 4 HTTPS Opera (vlastní zpracování)



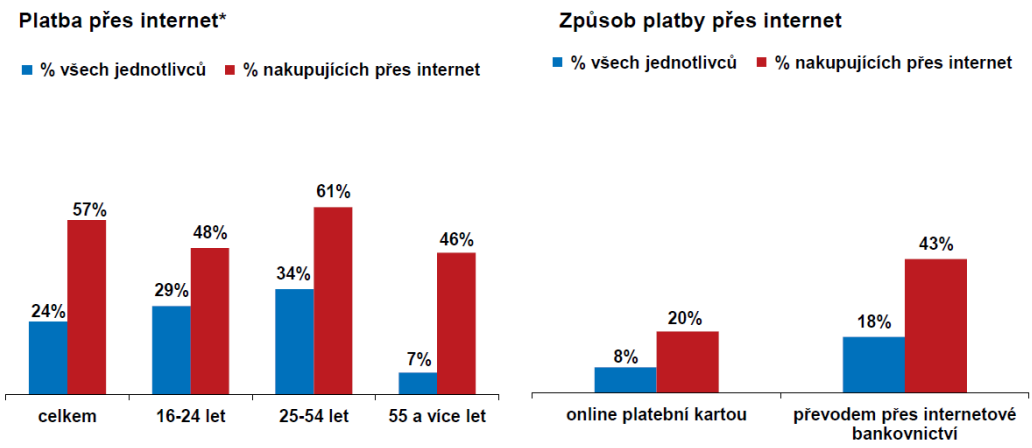
Obrázek 5 HTTPS Chrome (vlastní zpracování)



Obrázek 6 HTTPS Microsoft Edge (vlastní zpracování)



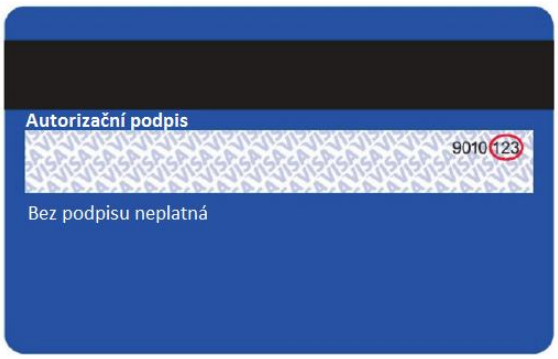
Obrázek 7 HTTPS Mozilla Firefox (vlastní zpracování)



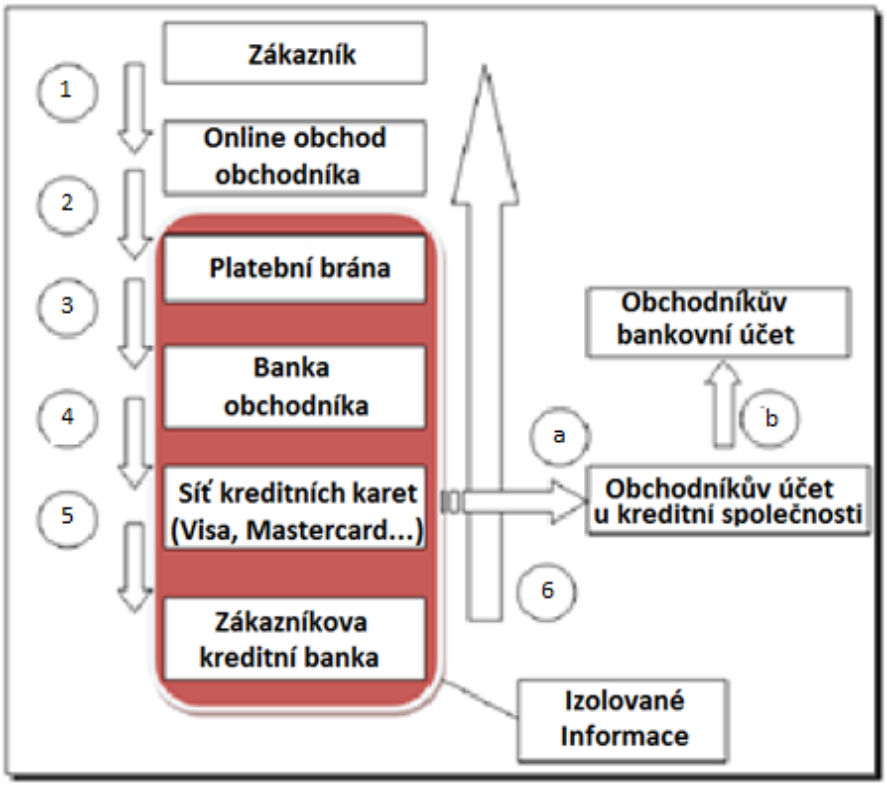
**** Zahrnuje platbu přes internet platební kartou, převodem přes internetové bankovnictví či prostřednictvím „elektronických peněženek" PayPal, PaySec, apod.***

Obrázek 8 graf míry plateb přes Internet (zdroj ČSU)

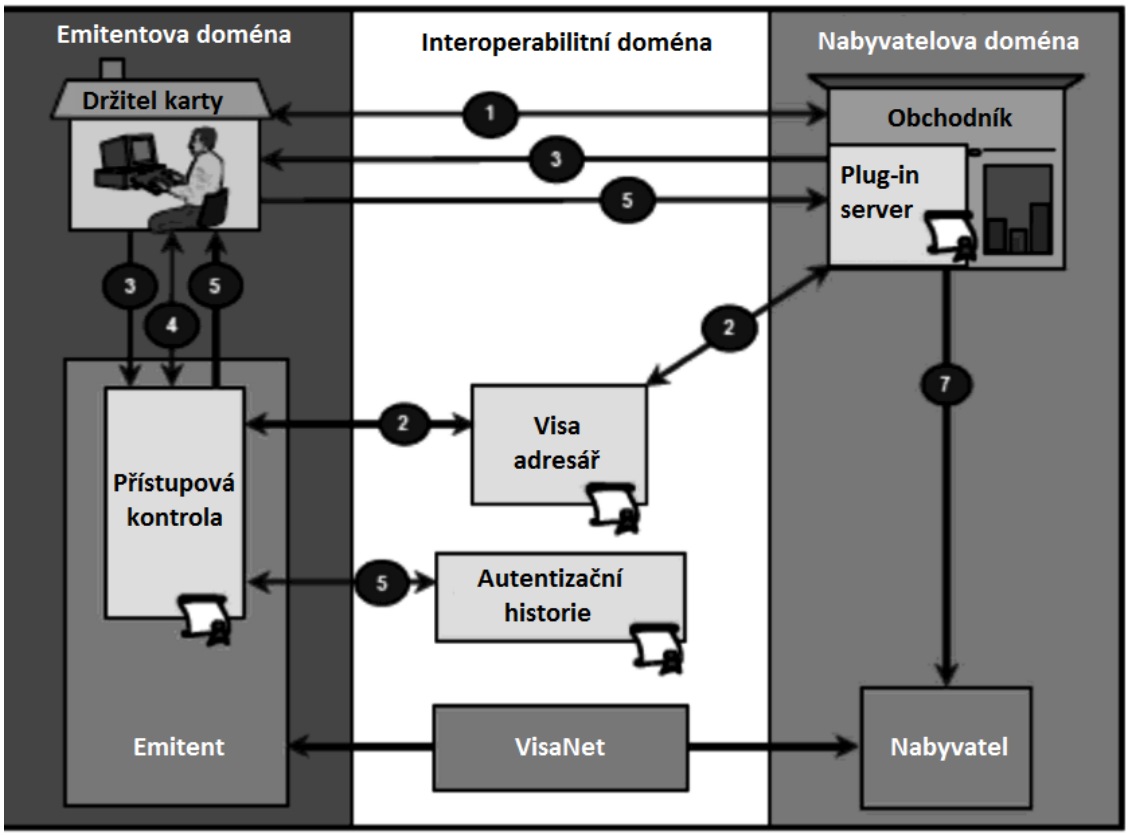
Obrázek 9 kreditní karta (34)



Obrázek 10 CVV2 na kartě (34)



Obrázek 11 Funkce platební brány (37)

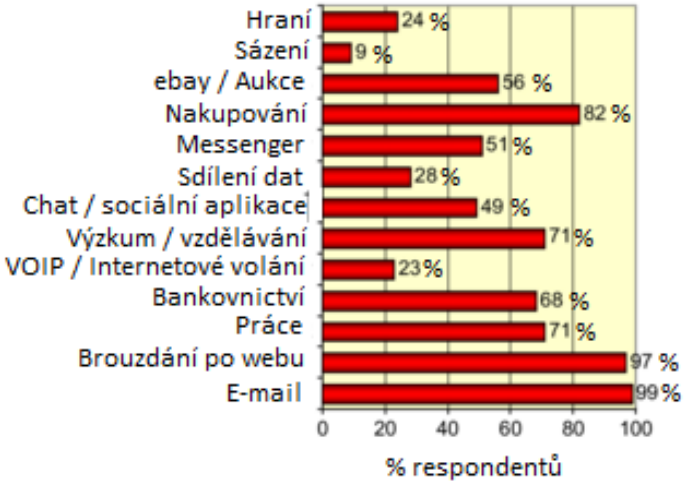


Obrázek 12 princip 3D Secure (39)

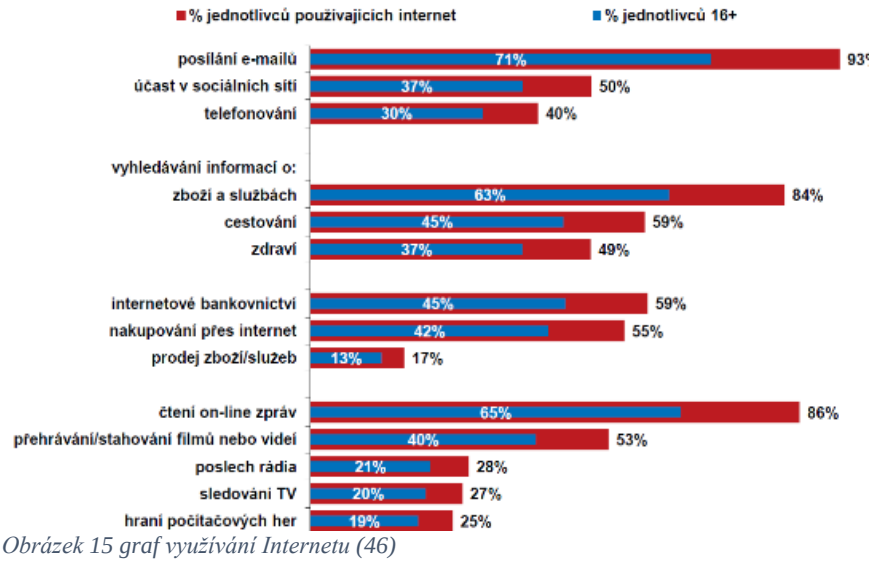
14.2 Příloha 2 grafy k analýze zabezpečení uživatelů

Služby na internetu	Absolutní četnost	Relativní četnost
Facebook	2143	74,0%
Vyhledávání	2822	97,5%
Zpravodajství	2531	87,5%
e-mail	2842	98,2%
stahování souborů	2570	88,8%
Chat	1078	37,2%
ICQ a instant messaging	1889	65,3%
nákup zboží	2401	83,0%

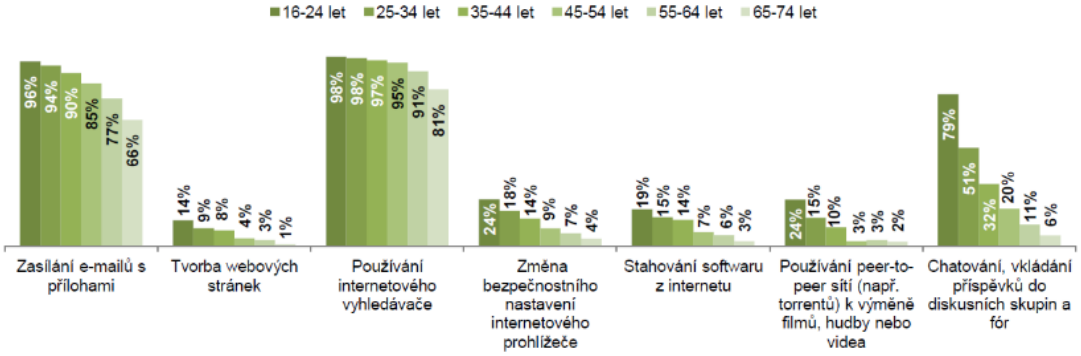
Obrázek 13 využívání Internetu (zdroj dobrýweb)



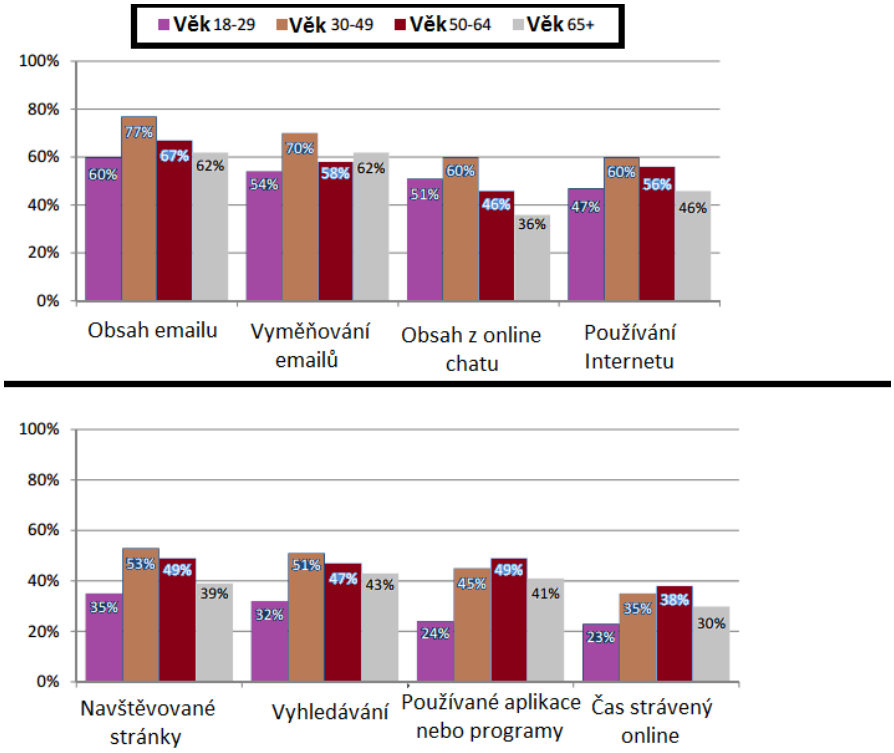
Obrázek 14 graf využívání Internetu (ČSU)



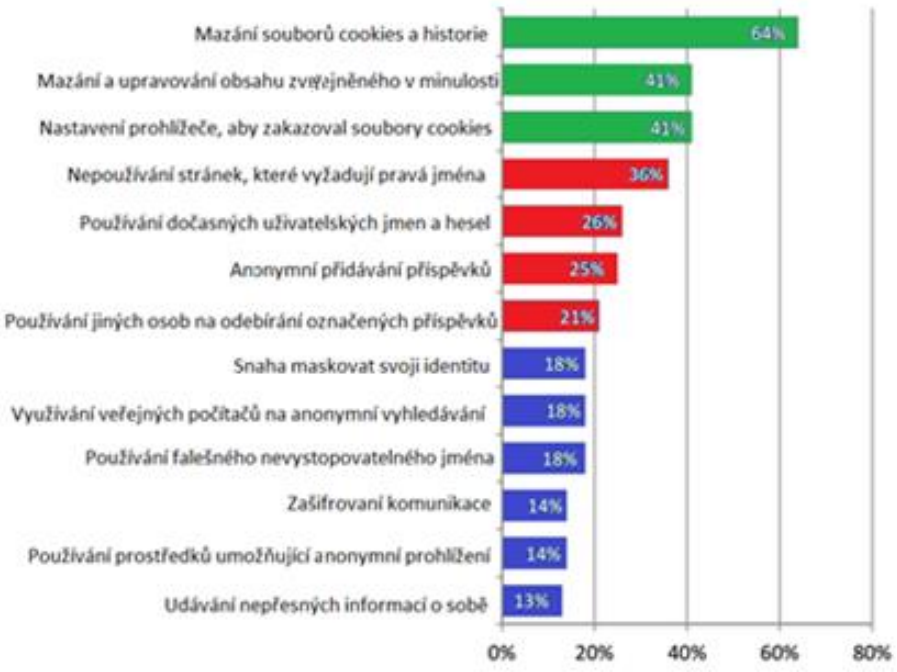
Obrázek 15 graf využívání Internetu (46)



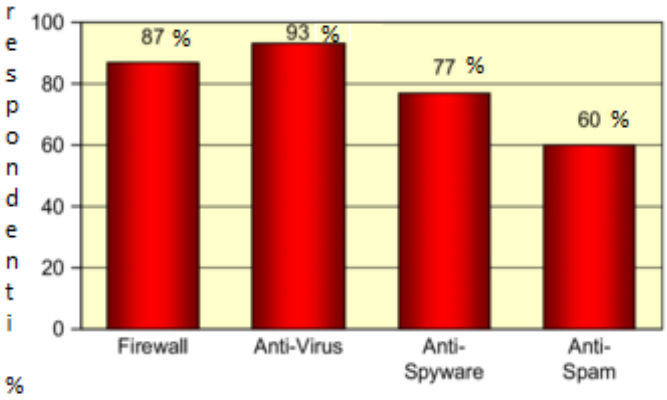
Obrázek 16 graf využívání Internetu (ČSU)



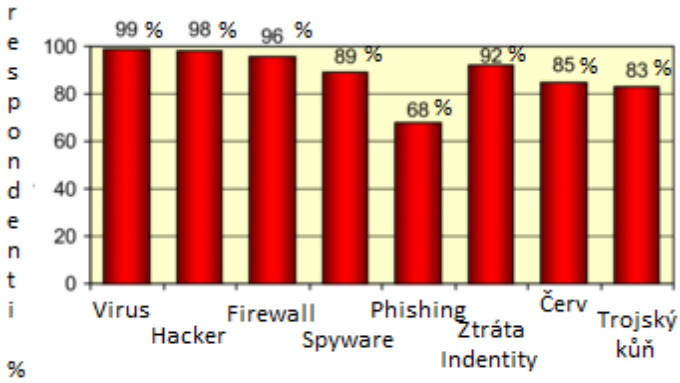
Obrázek 17 graf autorizace na Internetu (43)



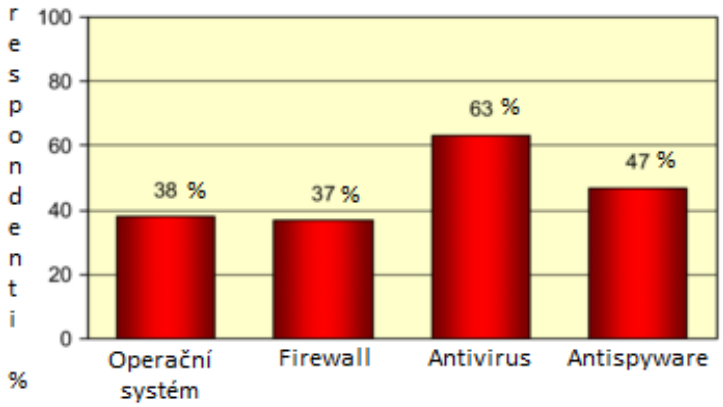
Obrázek 18 graf ochrana identity uživatelů (49)



Obrázek 19 graf míry používání bezpečnostních programů (46)

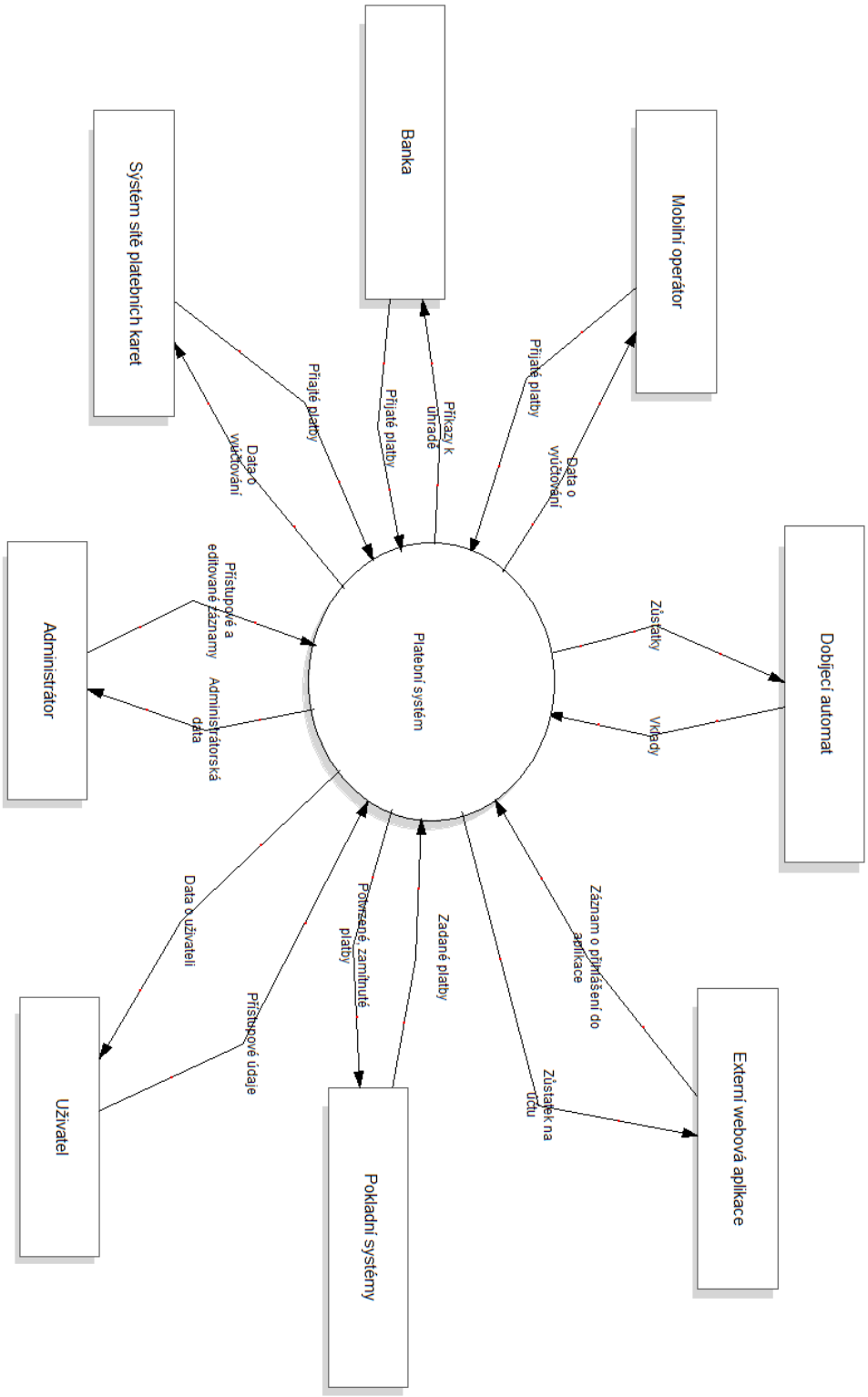


Obrázek 20 graf znalosti pojmů u uživatelů (46)



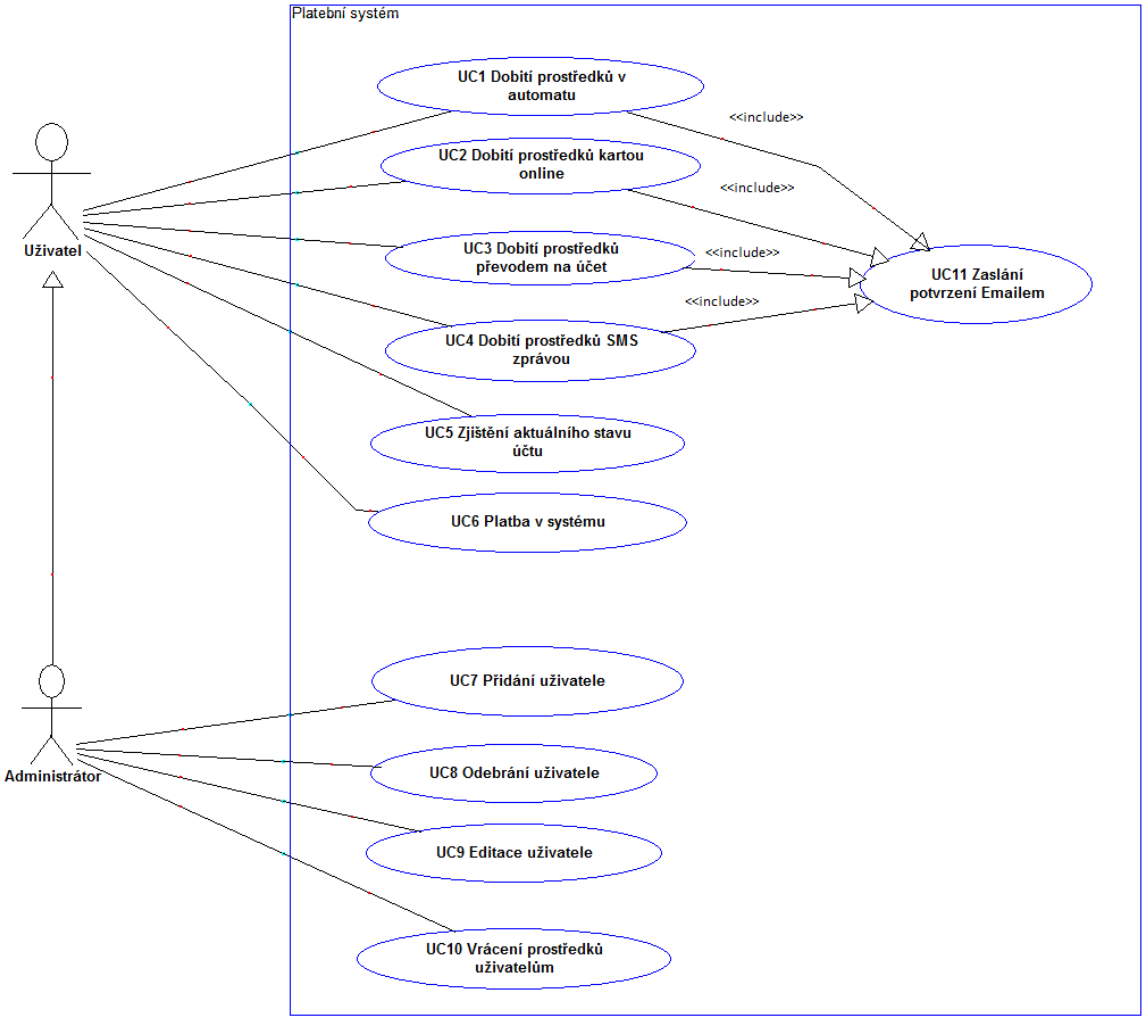
Obrázek 21 graf míry aktualizace programů uživateli (46)

14.3 Příloha 3 kontextový diagram



Obrázek 22 kontextový diagram platebního systému (vlastní zpracování)

14.4 Příloha 4 Use Case



Obrázek 23 UML schéma případů užití (vlastní zpracování)

14.5 Příloha 5 DFD tabulky

Název	Označení	Popis
uživatel	terminátor	použije dobíjecí automat
data z čipové karty	datový tok	ID uživatele
dobití kartou	proces	vklad hotovosti a výběr částky
dobití hotově	proces	vklad karty a výběr částky
pin kód	datový tok	pin z karty
data pro přepnutí platby	datový tok	příkaz pro změnu platby
kontrola pinu	proces	ověření pinu
schválený pin + částka	datový tok	ověřený pin
systém sítě platebních karet	terminátor	poskytovatel platby kartou
zamítnutá částka	datový tok	informace o zamítnutí platby
potvrzená transakce	datový tok	potvrzení od poskytovatele
potvrzení o vkladu	datový tok	potvrzení z automatu
dobití částky	proces	zpracování vkladu
dobitá částka	datový tok	dobíjená částka + ID
Databáze	datastore	uložení hodnot dle ID

Tabulka 35 dobití prostřednictvím automatu (vlastní zpracování)

Název	Označení	Popis
uživatel	terminátor	uživatel v internetové aplikaci
přihlašovací údaje	datový tok	přihlašovací jméno + heslo
zobrazení stránky karta online	proces	zobrazení stránky
dobíjená částka	datový tok	zvolená částka
platba kartou online	proces	spojení s poskytovatelem
platební údaje	datový tok	údaje z karty
systém sítě platebních karet	terminátor	poskytovatel platby kartou
zadané špatné údaje	datový tok	data se špatnými údaji
data o zamítnutí platby	datový tok	data o zamítnutí platby
potvrzená platba	datový tok	data o schválení platby
dobití prostředků	proces	zpracování platby
dobíjená částka	datový tok	dobitá částka + ID uživatele
databáze	datastore	uložení hodnot dle ID

Tabulka 36 dobití prostřednictvím kartou online (vlastní zpracování)

Název	Označení	Popis
uživatel	terminátor	uživatel v internetové aplikaci
přihlašovací údaje	datový tok	přihlašovací jméno + heslo
zobrazení stránky převod	proces	zobrazení stránky
platební údaje	datový tok	variabilní + konstantní symbol
zadání platby	proces	internetové bankovnictví
data do bankovnictví	datový tok	data pro banku
banka	terminátor	banka uživatele
potvrzená platba	datový tok	přišlá platba z banky
zpracování příchozí platby	proces	zpracování platby
dobitá částka	datový tok	velikost částky
databáze	datastore	uložení hodnot dle variabilního a konstantního symbolu

Tabulka 37 dobití prostřednictvím převodem na účet (vlastní zpracování)

Název	Označení	Popis
uživatel	terminátor	uživatel v internetové aplikaci
přihlašovací údaje	datový tok	přihlašovací jméno + heslo
zobrazení stránky sms	proces	zobrazení stránky
informace pro dobití	datový tok	tvar sms zprávy + číslo
dobití pomocí sms	proces	vytvoření sms zprávy
sms zpráva	datový tok	odeslaná sms zpráva
mobilní operátor	terminátor	poskytovatel platby
neplatná sms zpráva	datový tok	sms o neplatném tvaru
potvrzená platba	datový tok	data o potvrzení
zpracování platby	proces	zpracování dat od operátora
dobitá částka	datový tok	částka + ID uživatele
databáze	datastore	uložení dle ID uživatele

Tabulka 38 dobití prostřednictvím sms zprávy (vlastní zpracování)

Název	Označení	Popis
uživatel	terminátor	uživatel v systému
přihlašovací údaje	datový tok	data pro přístup do systému
zjištění stavu účtu	proces	požadavek na zjištění stavu
dotaz na stav	datový tok	ID uživatele
databáze	datastore	databáze v systému
aktuální stav	datový tok	data se stavem
stav účtu	datový tok	data s aktuálním stavem
tisk účtenky	proces	vytisknutí účtenky
data o tisku	datový tok	data o tisku účtenky

Tabulka 39 zjištění aktuálního stavu účtu (vlastní zpracování)

Název	Označení	Popis
uživatel	terminátor	uživatel v systému
přihlašovací údaje	datový tok	data pro přístup do systému
platba v systému	proces	zvolení položky + typ platby
data o nové transakci	datový tok	data z pokladního systému
pokladní systém	terminátor	pokladna nebo automat
zadaná platba	datový tok	částka
ověření zůstatku	proces	zjištění stavu účtu
schválená platba	datový tok	data o schválené platbě
dotaz na zůstatek	datový tok	data pro zjištění zůstatku
aktuální zůstatek	datový tok	data se zůstatkem
databáze	datastore	databáze v systému
data o transakci	datový tok	částka + položky + datum
tisk účtenky	proces	tisk transakce
data pro odečtení částky	datový tok	ID + částka

Tabulka 40 platba v systému (vlastní zpracování)

Název	Označení	Popis
administrátor	terminátor	administrátor systému
zadané hodnoty	datový tok	informace o novém uživateli
přidání uživatele	proces	požadavek na založení
data o novém uživateli	datový tok	jméno + příjmení + rodné číslo
kontrola existujícího uživatele	proces	kontrola jedinečnosti
databáze	datastore	databáze v systému
potvrzená data	datový tok	data z databáze
potvrzení o jedinečnosti	datový tok	potvrzení k založení uživatele
data o založení uživatele	datový tok	informace o uživateli
ID uživatele	datový tok	nově vytvořené ID
nastavení čipu a přihlášení	proces	nastavení nových údajů
přihlašovací údaje	datový tok	id + heslo + přihlašovací údaje

Tabulka 41 přidání uživatele do systému (vlastní zpracování)

Název	Označení	Popis
administrátor	terminátor	administrátor systému
ID uživatele	datový tok	ID z čipového zařízení
odebrání uživatele	proces	požadavek na odebrání
potvrzení o nulovém stavu	datový tok	data s potvrzením
kontrola zůstatku	proces	kontrola stavu účtu uživatele
data o uživateli	datový tok	data z databáze
databáze	datastore	databáze v systému

Tabulka 42 odebrání uživatele ze systému (vlastní zpracování)

Název	Označení	Popis
administrátor	terminátor	administrátor systému
ID uživatele	datový tok	ID z čipového zařízení
načtení uživatele	proces	požadavek pro načtení
data o uživateli	datový tok	jméno + heslo + ID + data
editace uživatele	proces	změna údajů o uživateli
upravené hodnoty	datový tok	změněné hodnoty
databáze	datastore	databáze v systému

Tabulka 43 úprava uživatele v systému (vlastní zpracování)

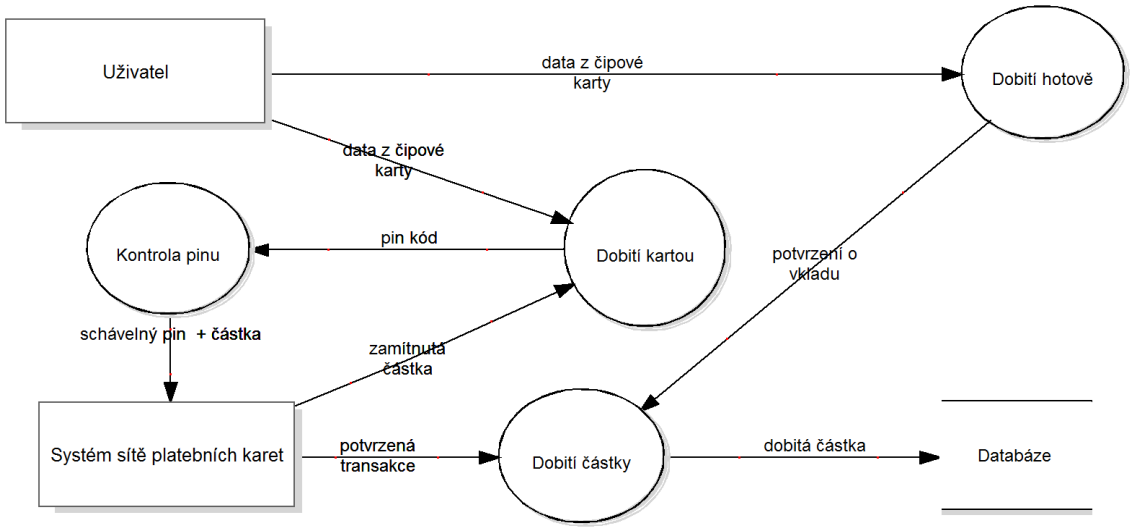
Název	Označení	Popis
uživatel	terminátor	uživatel systému
administrátor	terminátor	administrátor systému
pokladní systém	terminátor	pokladna v systému
vstupní data	datový tok	ID uživatele + kontrolní číslo
zadání částky	proces	odeslání částky ke kontrole
ID uživatele + částka	datový tok	hodnoty uživatele
ověření částky	proces	požadavek na kontrolu účtu
data se zůstatkem	datový tok	data z databáze
databáze	datastore	databáze v systému
schválená částka	datový tok	schválená částka pro výběr
založení transakce	proces	nová transakce
založená transakce	datový tok	data o založení transakce
data o transakci	datový tok	data s transakcí
data o nové transakci	datový tok	data z pokladny
založení transakce	proces	částka
způsob výběru	proces	hotovost nebo na účet
potvrzená transakce	datový tok	částka+ datum + způsob výběru
tisk účtenky	proces	vytisknutí účtenky
snižovaná částka + ID	datový tok	data do databáze
data s příkazem k úhradě	datový tok	data pro banku
banka	terminátor	banka platebního systému

Tabulka 44 vrácení finančních prostředků (vlastní zpracování)

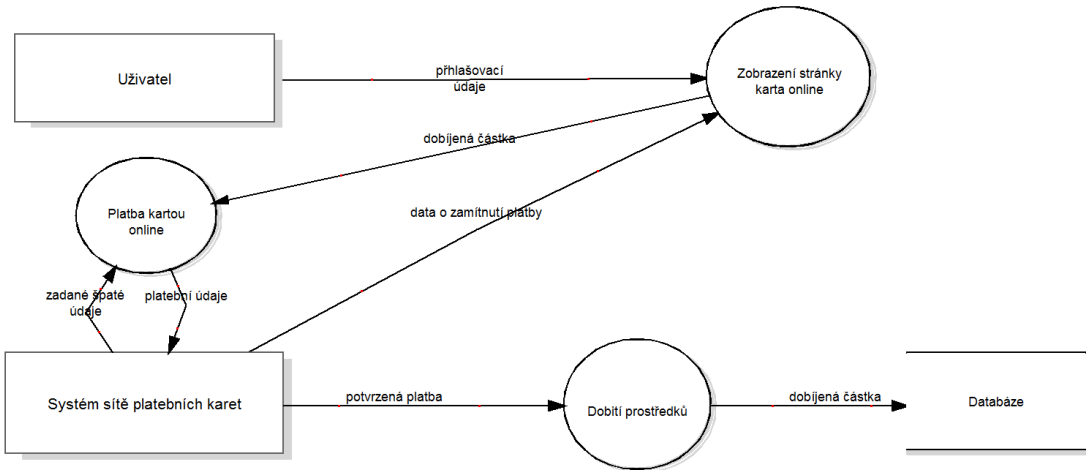
Název	Označení	Popis
uživatel	terminátor	uživatel systému
částka + ID	datový tok	ID uživatele + dobitá částka
provedení dobití	proces	kartou, hotově, převodem, sms
tvorba emailu	proces	vytvoření potvrzovacího emailu
odeslání emailu	proces	odeslání na uživatelův email
data o platbě	datový tok	ID, datum, částka a místo
vytvořený email	datový tok	vygenerovaný email s platbou
data o chybném odeslání	datový tok	ID uživatele + email uživatele
administrátor	terminátor	administrátor systému
potvrzení o odeslání	datový tok	ID, datum, částka, místo a potvrzení
databáze	datastore	databáze v systému

Tabulka 45 zaslání potvrzení emailem (vlastní zpracování)

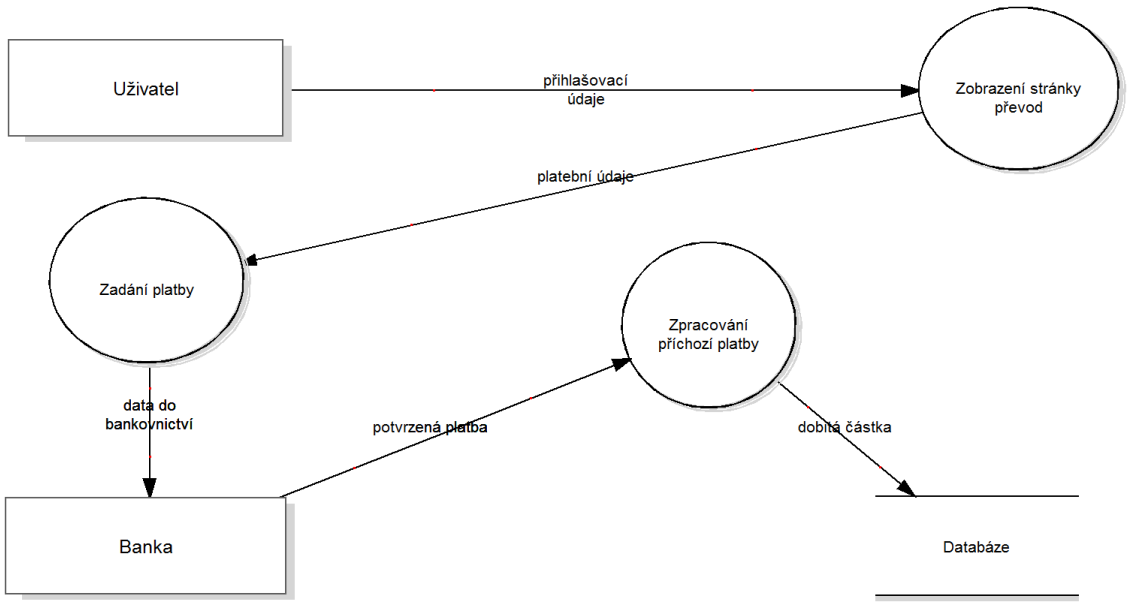
14.6 Příloha 6 DFD diagramy



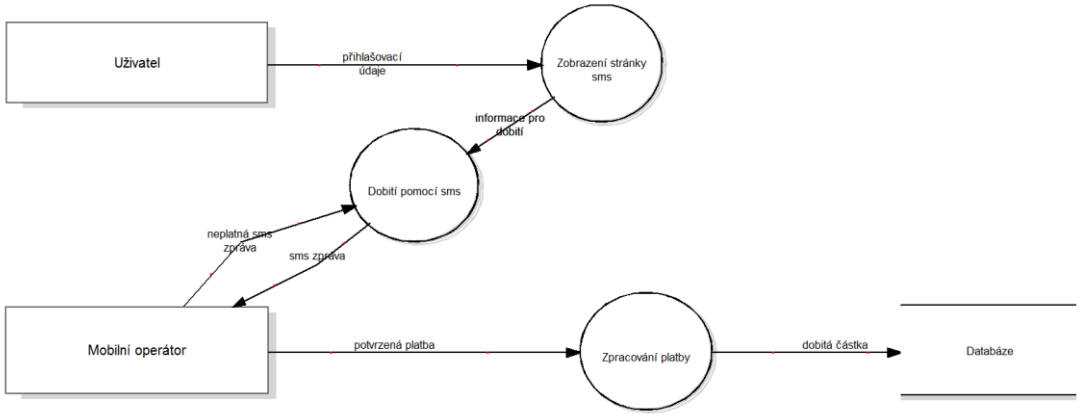
Obrázek 24 DFD diagram dobití prostřednictvím automatu (vlastní zpracování)



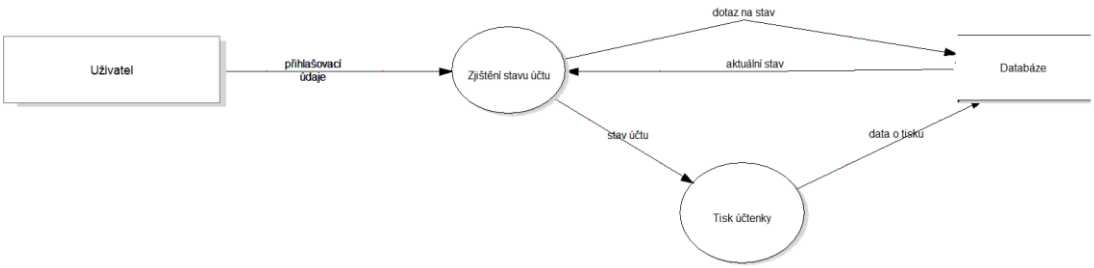
Obrázek 25 DFD diagram dobití prostřednictvím kartou online (vlastní zpracování)



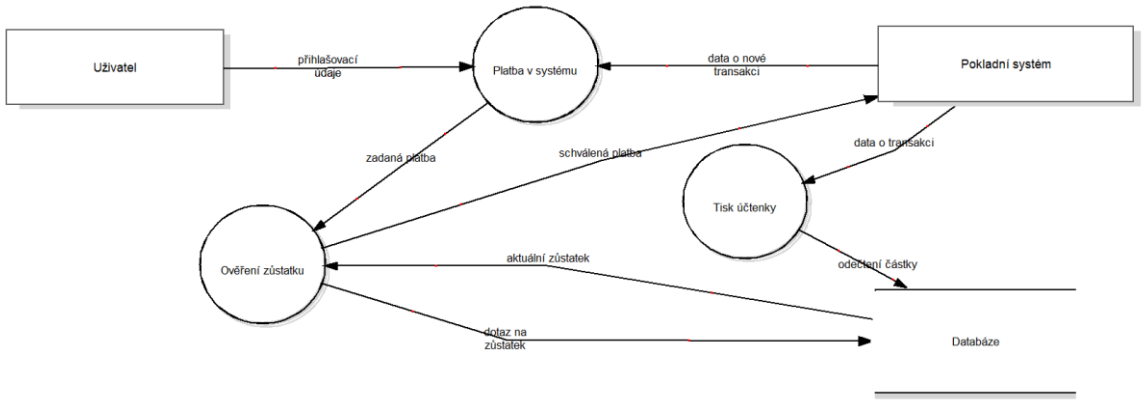
Obrázek 26 DFD diagram dobití prostřednictvím převodem na účet (vlastní zpracování)



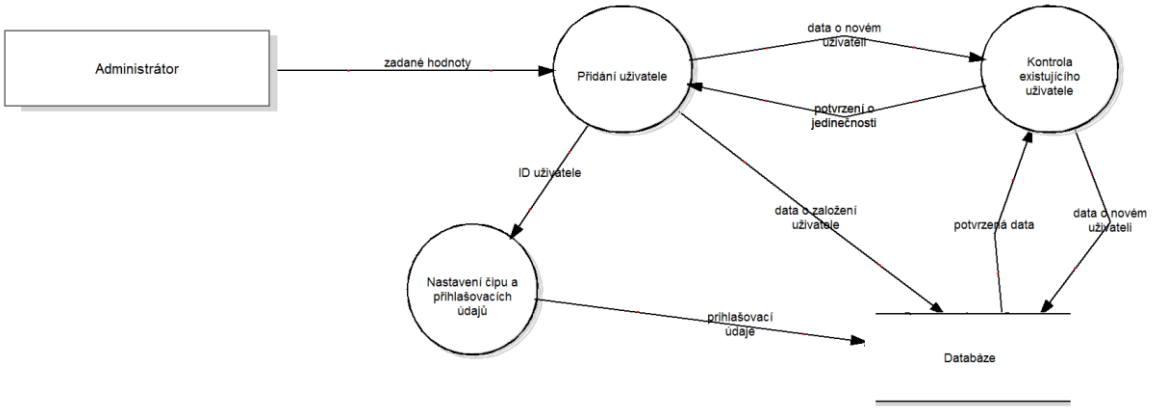
Obrázek 27 DFD diagram dobití prostřednictvím sms zprávy (vlastní zpracování)



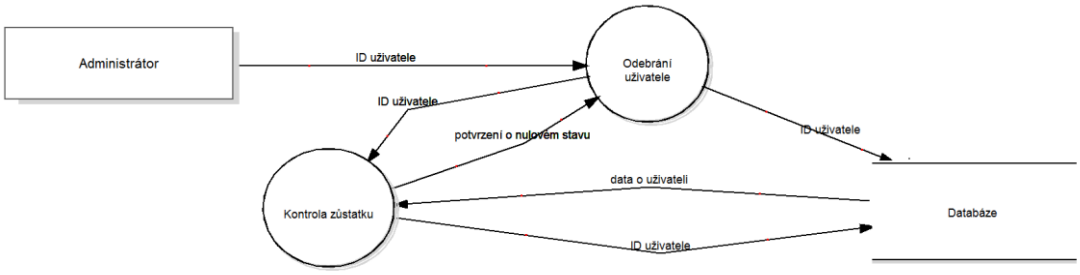
Obrázek 28 DFD diagram zjištění aktuálního stavu účtu (vlastní zpracování)



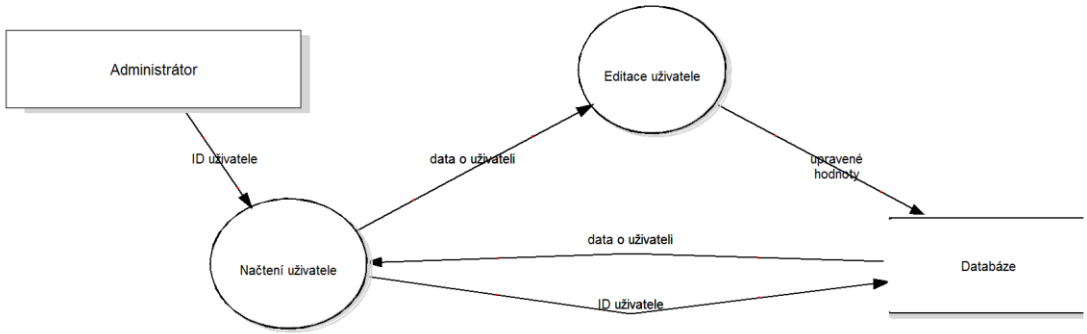
Obrázek 29 DFD diagram platba v systému (vlastní zpracování)



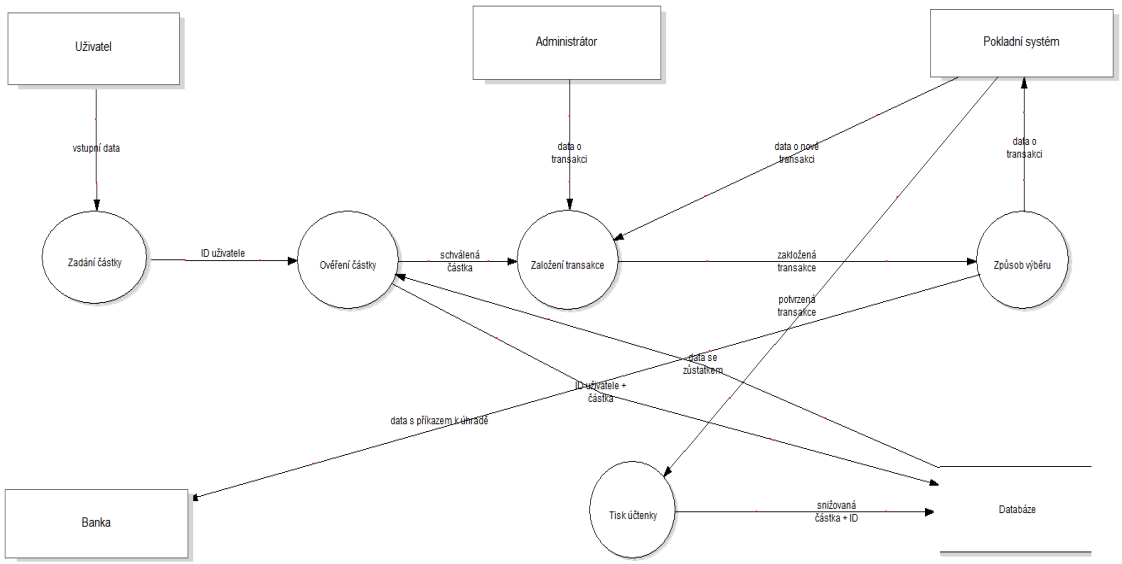
Obrázek 30 DFD diagram přidání uživatele do systému (vlastní zpracování)



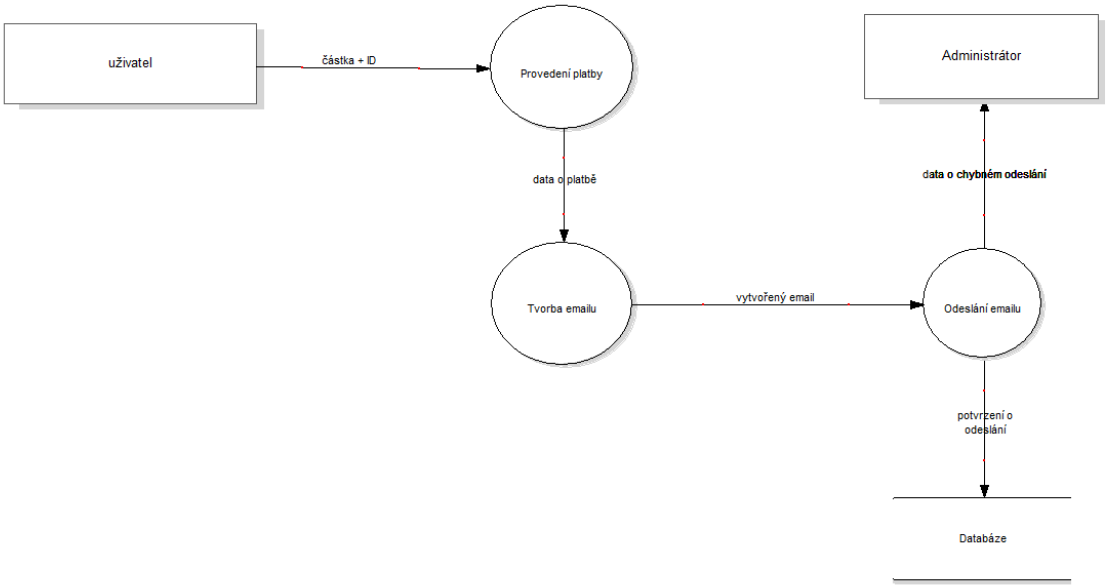
Obrázek 31 DFD diagram odebrání uživatele ze systému (vlastní zpracování)



Obrázek 32 DFD diagram úprava uživatele v systému (vlastní zpracování)



Obrázek 33 DFD diagram vrácení finančních prostředků (vlastní zpracování)



Obrázek 34 DFD diagram zaslání potvrzení emailem (vlastní zpracování)