

Bezpečnost používání platebních karet

Safety using credit cards

Bc. Jaroslav Chromík

**Diplomová práce
2011**



**Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky**

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jaroslav CHROMÍK**
Osobní číslo: **A10939**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Bezpečnost používání platebních karet**

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Analyzujte rizika v souvislosti s používáním platebních karet.
3. Zjistěte a vyhodnoťte statistické údaje zjištěných podvodů s platebními kartami.
4. Uveďte problémy s objasňováním uvedené trestné činnosti.
5. V rámci možností proveďte u útvarů Policie ČR výzkum za účelem zjištění problémů s usvědčováním pachatelů.
6. Proveďte a vyhodnoťte dotazníky náhodně oslovených respondentů za účelem zjištění míry zabezpečení jejich platebních karet a informovanosti o rizicích s jejich používáním.
7. Navrhněte vlastní opatření ke zvýšení bezpečnosti výběru z bankomatů.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. JURÍK, P. Platební karty: velká encyklopedie 1870–2006. 1. vyd. Praha: Grada Publishing, 2006. 296 s. ISBN: 80–247–1381–0.
2. JURÍK, P. Encyklopedie platebních karet. 1. vyd. Praha: Grada Publishing, 2003. 312 s. ISBN: 80–247–0685–7.
3. SCHLOSSBERGER, O., HOZÁK L. Elektronické platební prostředky. 1. vyd. Praha: Bankovní institut vysoká škola, 2005. 144 s. ISBN: 80–7265–073–4.
4. BROŽ, J., HRADECKÝ, M. Platební prostředky, jejich ochrana a padělání. Praha: Ministerstvo vnitra, odbor vzdělávání a správy policejního školství a Policie ČR, Útvar pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování, 2008. 160 s. ISBN: 80–7312–055–0.
5. Sdružení pro bankovní karty ČR: Souhrnné statistiky SBK [online]. 2011, poslední úpravy 2011–02–15 [cit. 2011–02–23]. Dostupné z WWW: http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html.

Vedoucí diplomové práce:

Ing. Miroslav Matýsek, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

28. února 2011

Termín odevzdání diplomové práce:

17. října 2011

Ve Zlíně dne 28. února 2011


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Hlavním cílem práce je zjistit, analyzovat a vyhodnotit míru bezpečnosti používání platebních karet v České republice. V teoretické části jsou popsány jednotlivé druhy karet, jejich ochranné prvky, záznamy dat, proces zpracování transakce a trestná činnost spojená se zneužitím karet včetně její trestněprávní kvalifikace. V praktické části jsou vyhodnoceny statistiky zjištěné trestné činnosti v souvislosti se zneužitím platebních karet. Z nich byla provedena kvantifikovaná analýza rizika zneužití platebních karet a vyhodnocena míra zjištěného rizika. Analyzovány byly také problémy s objasňováním uvedené trestné činnosti. V práci jsou realizovány 3 výzkumy formou dotazníků směřovaných bankám, držitelům karet a útvarům Policie České republiky Městského ředitelství v Ostravě. V závěru práce je navrženo preventivní a represivní opatření ke zvýšení bezpečnosti používání platebních karet.

Klíčová slova:

Platební karta, bankomat, platební terminál, platební transakce, skimming, phishing, libanonská smyčka, bezpečnost, analýza rizika.

ABSTRACT

The main purpose of this study is to identify, analyse and evaluate the security level of using payment cards in the Czech Republic. The theoretical part describes the different types of cards, their security features, data records, the process of transaction processing and crime associated with misuse of cards including their criminal determination. The practical part evaluates the statistics of crimes discovered in connection with the misuse of credit cards. Then, quantified analysis of the risk of misuse of credit cards was performed and the extent of the risk identified was assessed. The problems connected with clarifying the crime mentioned were also analysed. The work carries out three research questionnaires channelled to banks, cardholders and departments of the Police of the Czech Republic Municipal Headquarters in Ostrava. In conclusion of this study, there is a preventive and a repressive measure suggested, to increase the safety of using payment cards.

Keywords:

Credit card, ATM, payment terminal, payment transactions, skimming, phishing, Lebanese loop, safety, risk analysis.

Poděkování, motto

Děkuji Ing. Miroslavu Matýskovi, Ph.D., za vedení této diplomové práce, za jeho čas, trpělivost a rady, které mi poskytl. Poděkování patří také plk. Mgr. Tomáši Landsefildovi, řediteli Policie ČR Městského ředitelství policie v Ostravě, za umožnění výzkumu dotazníků u útvarů Policie ČR v rámci tohoto ředitelství, Sdružení pro bankovní karty za poskytnutí informací, respondentům dotazníků a v neposlední řadě také mé rodině a přátelům za podporu po celou dobu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	11
1 ZÁKLADNÍ ÚDAJE O PLATEBNÍCH KARTÁCH	12
1.1 PRÁVNÍ ÚPRAVA.....	12
1.2 DRUHY PLATEBNÍCH KARET	13
1.3 OCHRANNÉ PRVKY KARET A ZÁZNAMY DAT	16
1.3.1 Ochranné prvky	16
1.3.2 Záznamy dat	18
1.4 ZPRACOVÁNÍ TRANSAKCE	21
1.4.1 Ověření	21
1.4.2 Autorizace	21
1.4.3 Clearing	23
1.4.4 Zúčtování.....	23
2 TRESTNÁ ČINNOST	24
2.1 TRESTNÁ ČINNOST OPRÁVNĚNÉHO DRŽITELE PLATEBNÍ KARTY	24
2.1.1 Přecherpání dovoleného limitu	24
2.1.2 Fiktivní krádež	24
2.2 TRESTNÁ ČINNOST NEOPRÁVNĚNÉHO DRŽITELE PLATEBNÍ KARTY	24
2.3 ZÁVAŽNĚJŠÍ FORMY TRESTNÉ ČINNOSTI	26
2.3.1 Libanonská smyčka	26
2.3.2 Zadržné lišty na ATM pro výběr peněz	27
2.4 TRESTNÁ ČINNOST ORGANIZOVANÉHO ZLOČINU	27
2.4.1 Skimming	28
2.4.2 Phishing.....	31
2.4.3 Padělání platebních karet	32
3.5 TRESTNĚPRÁVNÍ KVALIFIKACE.....	33
II PRAKTICKÁ ČÁST	35
3 VYHODNOCENÍ STATISTIK TRESTNÉ ČINNOSTI	36
3.1 STATISTIKA TRESTNÉ ČINNOSTI V CELÉ ČR.....	36
3.2 STATISTIKA TRESTNÉ ČINNOSTI V KRAJÍCH	39
4 ANALÝZA RIZIKA ZNEUŽITÍ PLATEBNÍ KARTY	41
4.1 STANOVENÍ PRAVDĚPODOBNOTI.....	42
4.2 STANOVENÍ NÁSLEDKŮ	44
4.3 KVANTIFIKACE AKTIV	47
4.4 KVANTIFIKACE HROZEB	47
4.5 KVANTIFIKACE ZRANITELNOSTI	48
4.6 HODNOCENÍ RIZIKA	48
5 ANALÝZA PROBLÉMŮ S USVĚDČOVÁNÍM PACHATELŮ TRESTNÉ ČINNOSTI	52

5.1	PODVODY PÁCHANÉ OPRÁVNĚNÝM DRŽITELEM PLATEBNÍ KARTY.....	52
5.2	PODVODY SPÁCHANÉ NEOPRÁVNĚNÝM DRŽITELEM PLATEBNÍ KARTY.....	52
6	VYHODNOCENÍ DOTAZNÍKŮ	54
6.1	VYHODNOCENÍ DOTAZNÍKŮ ADRESOVANÝCH BANKÁM.....	54
6.2	VYHODNOCENÍ DOTAZNÍKŮ ADRESOVANÝCH DALŠÍM SUBJEKTŮM	54
6.3	VYHODNOCENÍ DOTAZNÍKŮ ADRESOVANÝCH UŽIVATELŮM KARET.....	56
6.4	VYHODNOCENÍ DOTAZNÍKŮ SMĚROVANÝCH ÚTVARŮM POLICIE ČR.....	59
7	NAVRHOVANÁ OPATŘENÍ KE ZVÝŠENÍ BEZPEČNOSTI POUŽÍVÁNÍ PLATEBNÍCH KARET	61
7.1	NÁVRH PREVENTIVNÍCH OPATŘENÍ	62
7.1.1	Zavedení biometrické identifikace	62
7.2	NÁVRH REPRESIVNÍCH OPATŘENÍ	67
	ZÁVĚR	68
	CONCLUSION	69
	SEZNAM POUŽITÉ LITERATURY	70
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	74
	SEZNAM OBRÁZKŮ	75
	SEZNAM TABULEK.....	76
	SEZNAM PŘÍLOH.....	77

ÚVOD

Používání platebních karet¹ je součástí nynějšího života obyvatel vyspělých i rozvojových zemí. Tento prostředek umožňuje lidstvu nakupovat zboží a využívat služeb bez nutnosti disponování hotovostními finančními prostředky. Mnoho lidí si bez platebních karet nedokáže představit svůj každodenní režim, což je v moderní lidské společnosti přirozené. S masivním rozvojem Internetu se lidem rozšířili možnosti nákupů a objednávek z tepla domova, přičemž využívají k placení přes Internet bezhotovostní platební prostředky. O globálním používání platebních karet svědčí také zjištění, že v roce 2008 bylo platebními kartami realizováno 54% objemu plateb na celém světě [30].

Někteří lidé neznají základní druhy platebních karet, rozdíl mezi nimi, jejich bezpečnostní prvky a neuvědomují si potenciální rizika, která používání platebních karet přináší. Podle sdělení České bankovní asociace je používání platebních karet v České republice (ČR) bezpečnější, než v Evropské unii (EU). Zatímco v EU dosáhl podíl podvodů na celkovém objemu karetních transakcí osm setin procenta, v ČR to byly jen dvě setiny procenta [42]. Cílem práce je zjistit a analyzovat konkrétní rizika v souvislosti s používáním platebních karet v naší zemi, zda jsou tato rizika reálná, jaká je míra rizika a zda jsou či nejsou rizika akceptovatelná. Na podobné téma již bylo napsáno více prací, avšak autorovým záměrem nebylo rizika zneužití platební karty popsat jen teoreticky, ale rizika zcela konkrétně analyzovat kvantifikovanou metodou ze statisticky vykázaných událostí, které již nastaly v období let 2001-2010. Ke snížení míry rizika byla navržena opatření ke zvýšení bezpečnosti používání platebních karet. Ačkoli bankovní subjekty či finanční společnosti vydávající platební karty z akceptovatelných důvodů neposkytnou požadovanou součinnost, tato práce může přispět k tomu, aby podle míry zjištěného rizika přijali opatření k ochraně držitelů (vlastníků) karet. Práce má význam také pro samotné držitele platebních karet, aby si uvědomili reálnost nebezpečí při jejich použití. Dodržováním doporučených zásad vydavatelů karet totiž mohou výrazně přispět ke zvýšení bezpečnosti používání platebních karet a tudíž ke snížení zjištěné míry analyzovaných rizik.

¹ V této práci je použit obecný termín „platební karta“ pro všechny druhy karet.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ ÚDAJE O PLATEBNÍCH KARTÁCH

Platební karty patří mezi základní formy elektronického bankovníctví, obdobně jako internetové bankovníctví², telefonní bankovníctví³ a GSM bankovníctví⁴. Velikost platebních karet je dána mezinárodní normou ISO 3554 na $85,6 \times 54 \times 0,76$ mm.

První plastová platební karta byla vydána americkou společností Diners Club v roce 1950 pro náhlé případy, kdy zákazník v restauracích nebude mít na zaplacení (proto název Diners). Placení kartami se však velmi rychle osvědčilo a postupně se rozmohlo po celém světě. V Evropě patří mezi nejrozšířenější platební karty typu MASTERCARD a VISA. V USA typu VISA, AMERICAN EXPRESS a DINERS CLUB a v dalších zemích karty typu VISA, AMERICAN EXPRESS nebo JCB [4].

První platební karta v naší zemi (v tehdejší Československé socialistické republice) byla vydána již v roce 1988 Živnostenskou bankou, jako dispoziční (debetní) karta k tuzexovým účtům.

1.1 Právní úprava

Podle § 1, odst. 3 zákona o bankách [18] je platební karta považována za platební prostředek vydaný bankou. Ustanovení o bankovních platebních kartách jsou obsažena ve všeobecných obchodních podmínkách bank, které vydává Česká národní banka [7]. Ačkoli tyto podmínky nemají charakter právního předpisu, banky se dohodly na respektování určitých zásad při vydávání a používání platebních karet. Platební styk upravuje zákon [12] a k jeho řízení a koordinaci je pověřena Česká národní banka. Podle článku 1, písm. a) Rámcového rozhodnutí Rady Evropské unie [19] lze definovat platební kartu jako platební nástroj, díky němuž může držitel nebo uživatel na základě jeho specifické povahy samostatně nebo ve spojení s jiným platebním nástrojem převést peníze nebo peněžní hodnotu. K vydávání platebních karet jsou podle § 1 zákona o bankách [18] oprávněné pouze banky a úvěrové společnosti. Předmětem způsobilým plnit funkci

² Internetové bankovníctví (Internetbanking) – forma přímého bankovníctví umožňující přístup k bankovnímu účtu prostřednictvím sítě Internet.

³ Telefonní bankovníctví (Telephonebanking) – bankovníctví umožňující přístup k účtu prostřednictvím telefonů pevných linek.

⁴ GSM bankovníctví (GSM banking) – bankovníctví poskytované prostřednictvím mobilních telefonů.

platební karty může být náhražka platební karty, vydaná nebo zhotovená neoprávněným subjektem, která neobsahuje veškeré náležitosti platební karty, ale umožňuje plnit některé její funkce [6].

Banka, která platební karty vydává, váže její používání na správnou volbu osobního identifikačního kódu (PIN kódu) nebo na prokázání totožnosti předložitеле, popřípadě na ověření jeho podpisu podle podpisového vzoru uvedeného na platební kartě [7]. U karet, jejichž používání je vázáno na prokázání totožnosti předložitеле, jsou příjemci platby oprávněni po předložiteli karty požadovat předložení platného průkazu totožnosti (např. občanského průkazu nebo cestovního pasu) a jsou povinni takto ověřit totožnost předložitеле. Stejně tak u karet, jejichž požití je vázáno na ověření podpisu, jsou povinni ověřit autentizaci podpisu předložitеле se vzorem na zadní straně karty.

1.2 Druhy platebních karet

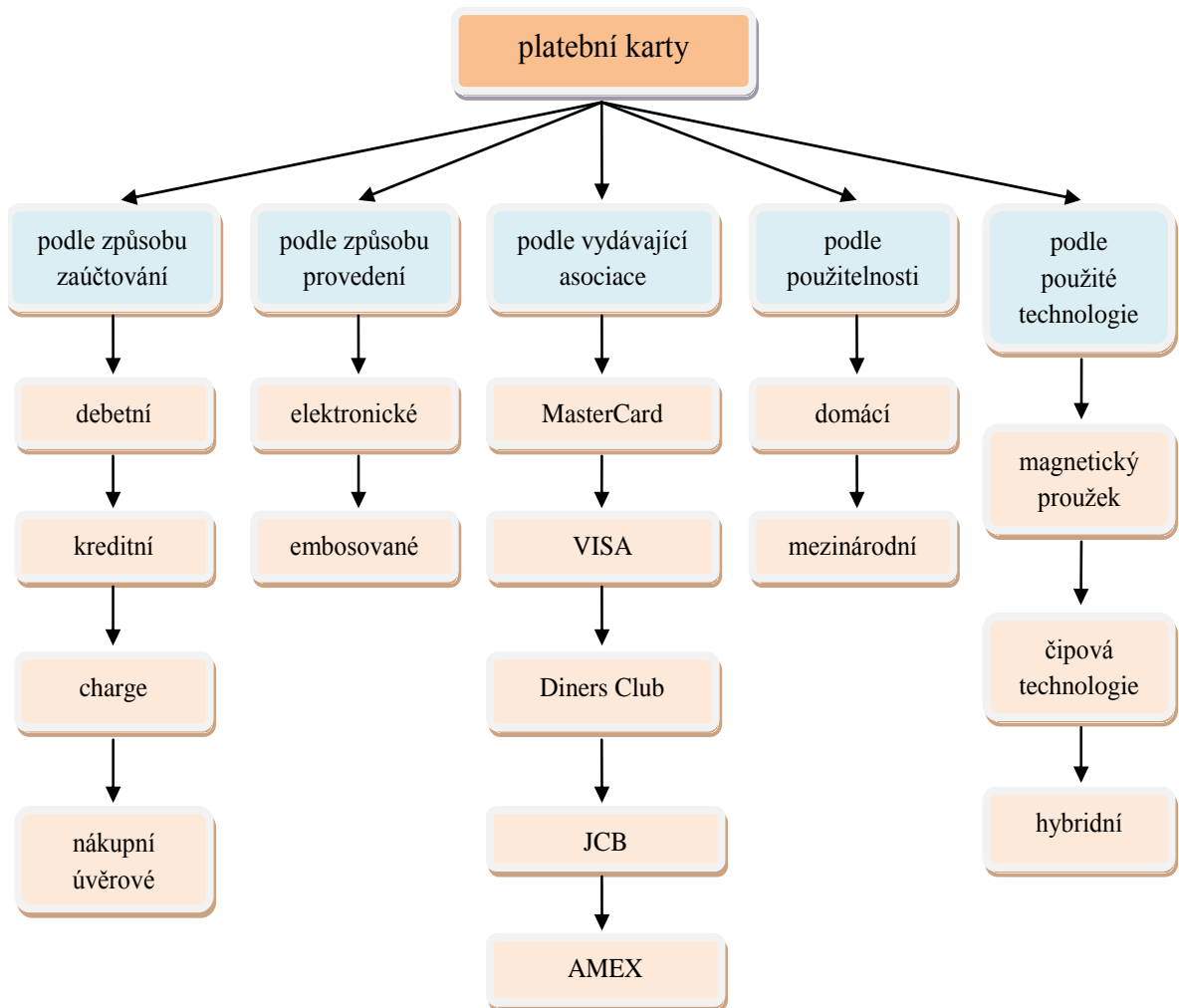
Platební karta musí obsahovat následující náležitosti:

- označení vydavatele,
- jméno držitele, popřípadě jeho identifikaci (např. rodné číslo, podpis),
- číslo,
- platnost,
- záznam dat (magnetický proužek, mikročip, optický nebo jiný speciální záznam).

Platební karty můžeme rozdělit podle několika kritérií. Kritéria a jednotlivé druhy znázorňuje obrázek (*Obr. 1*).

Debetní karty (debit cards)

Jsou karty, které přímo souvisí s finančními prostředky uloženými na běžném účtu. Po transakci provedené kartou (výběr z bankomatu, platba u obchodníka), dojde k odečtení příslušné částky z účtu. U elektronických karet se transakce zpravidla zaúčtuje maximálně do jednoho týdne, u embosovaných i později. Pokud je u běžného účtu zřízen kontokorent, může dojít k povolenému přečerpání účtu do jeho záporného zůstatku. Debetní karty tvoří největší podíl na kartách používaných v České republice.



Obr. 1. Rozdělení platebních karet⁵

Kreditní karty (credit cards)

Na rozdíl od předchozího typu je kreditní karta vázána k úvěrovému účtu. Každá transakce s kartou znamená použití úvěru do výše transakce. Banky stanoví určitou délku bezúročného období a po jejím překročení jsou k čerpanému úvěru přičteny i úroky dle sjednaných smluvních podmínek. Tyto karty jsou nejvíce využívány v USA, kde menší podíl představují karty debetní.

⁵ Vytvořeno autorem práce z údajů uvedených v [4].

Charge karty (charge cards)

Charge karty fungují podobně jako kreditní karty, avšak jsou vydávány ověřeným klientům s vysokou bonitou. Banka totiž na konci měsíce vystaví vyúčtování všech provedených transakcí. Splácení dluhu je jednorázové a bezúročné podle sjednaných podmínek s bankou.

Nákupní úvěrové karty

Jedná se o úvěrové karty vydávané subjekty z nebankovního sektoru. Od bankovních se liší zejména úročením, termíny a výší splátek úvěru, ale i omezenou použitelností. Do této skupiny patří např. OK karta, YES karta nebo Aura karta.

Elektronické karty

Jedná se o nejrozšířenější typ karty u nás. Mezi ně patří karty VISA Electron a Maestro. Jsou určené k platbě u obchodníků s elektronickým platebním terminálem (POS terminálem) a pro výběry z bankomatů (ATM), tedy pro transakce, které jsou online ověřovány v kartovém centru. Některé lze použít i pro platby na Internetu.

Embosované karty

Jsou snadno rozpoznatelné tím, že číslo karty, údaje o majiteli, platnost a popřípadě další údaje, jsou plasticky prolisovány či vyraženy. Proto jsou použitelné i u obchodníků, kteří nemají POS terminály, ale imprintery⁶. Postup transakce je takový, že obchodník vloží kartu do imprinteru, kde dojde k sejmutí všech vyražených údajů. Údaje se vytisknou a potvrdí podpisem držitele karty. Po nahlášení ztráty či odcizení karty je zařazena na stoplist, avšak tento proces je zdlouhavější, než blokace karty elektronické. Jejich výhodou je širší použitelnost, avšak nevýhodou představuje větší riziko zneužití neoprávněnou osobou.

MasterCard a VISA

Většina karet používaných v naší zemi je označena logem mezinárodní asociace MasterCard nebo VISA. Při použití karet v ČR nezáleží na uvedených značkách, neboť obě skupiny mají dostatečný a srovnatelný počet obchodních míst a také ATM. Při cestách

⁶Imprintery – zastaralé mechanické čtecí zařízení, často označované jako „žehličky“.

do zahraničí je vhodné předem získat informace o transakčních místech uvedených značek v dané zemi.

Do skupiny elektronických karet MasterCard se řadí karty Cirrus a Maestro, v embosované podobě jsou karty MC Standart a pro bonitní klienty MC Gold, popřípadě vrcholová řada World Signum. Karty VISA v elektronické podobě představuje typ VISA Electron, v embosované podobě VISA Classic. Vyšší třídy klientů jsou vydávány karty typu VISA Silver, VISA Gold a VISA Platinum.

Diners Club, JCB (Japan Credit Bureau) a AMEX (American Express)

Jedná se o méně užívané exklusivní platební nástroje užívané bonitními klienty.

Domácí a mezinárodní karty

Domácí karty jsou označovány nápisem „valid only in the Czech Republic“. Z důvodu omezenosti jejich použití pouze na území České republiky a poklesu zájmu klientů, jsou již na ústupu. Naprostá většina karet je v současné době vydávána jako mezinárodní.

Virtuální karty

Zvláštní kategorii tvoří karty virtuální, které slouží pouze pro internetové platby. Nejsou tedy použitelné pro výběr z ATM či k osobní platbě na POS terminálech u obchodníka.

1.3 Ochranné prvky karet a záznamy dat

Ochrannými prvky rozumíme obligatorní znaky, které daný typ karty jednoznačně charakterizují. Mezi ně řadíme číslo karty a logo asociace. Většina karet obsahuje také hologram, zvláštní viditelná nebo skrytá znamení. Pokud karta některá z těchto znaků postrádá, s největší pravděpodobností se jedná o padělanou kartu. Záznamy dat slouží k uložení identifikačních údajů o kartě a jeho majiteli, popřípadě k uložení hash bezpečnostních kódů, tzv. PIN kódů.

1.3.1 Ochranné prvky

Druh a vyobrazení ochranných prvků jednotlivých typů karet znázorňuje tabulka (Tab. 1). Jedná se o přehled základních ochranných prvků karet a není zdaleka

vyčerpávající. Některé nelze ani zveřejnit, neboť podléhají utajení. Není cílem práce je detailně popisovat, i z toho důvodu, že padělatelé je již detailně nenapodobují. Pro účely neoprávněného výběru z ATM používají polotovary z čistého plastu s magnetickým proužkem na zadní straně, popř. s jednoduchým nápisem na přední straně a potiskem stříbrné či zlaté barvy.

Tab. 1. Přehled ochranných prvků karet⁷

typ karty	VISA	MasterCard	American Express	Diners Club	JCB
počet číslic udávající číslo karty	13, popř. 16	16	15	14	16
číselné zobrazení	4-3-3-3 (4-4-4-4)	4-4-4-4	4-6-5	4-6-4	4-4-4-4
první číslice	4	5	34 nebo 37	30, 36 nebo 38	35
čísla identifikující vydavatelskou banku	prvních 6 čísel	prvních 6 čísel	prvních 6 čísel	prvních 6 čísel	prvních 6 čísel
hologram	stříbrný trojrozměrný obraz holubice, při pohybu proti světlu hýbe křídly	stříbrný trojrozměrný obraz zemské polokoule	není	u některých typů trojrozměrný obraz světové mapy s nápisem Diners Club International	stříbrný nebo zlatý trojrozměrný obraz Země a vycházejícího slunce
logo karty	emblém VISA v modro-bílo-zlatém provedení	2 propojené kruhy v barvě červené a žluté s nápisem MasterCard	Centurion s ostrými rysy	DC v levém horním rohu v tm.modré barvě doplněná textem Diners Club International	svislé pruhy červené, černé a modré barvy s nápisem JCB
zvláštní znamení (viditelná)	letící "V" na přední straně	do sebe zapadající písmena MC na přední straně	mikrotext opakujících se slov American Express	stylizovaný symbol DC	čínské ornamenty
skrytá znamení (viditelná pod UV světlem)	letící holub	písmena MC	nápis AMEX a fosforeskující obrazec Centurion	logo Diners Club International	nezjištěna

⁷ Vytvořeno autorem práce z údajů uvedených v [4].

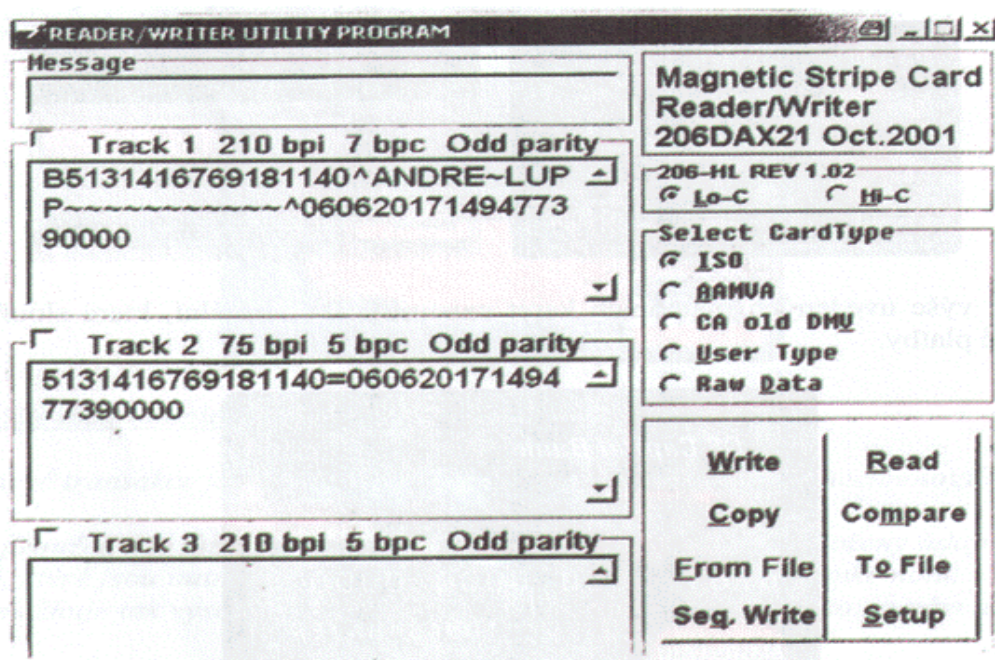
1.3.2 Záznamy dat

Záznamy dat jsou uloženy v magnetickém proužku nebo mikročipu. Údaje v něm obsažené jsou předmětem utajení před nepovolanými osobami. Banka je povinna zabezpečit je před zneužitím.

Magnetický proužek

Magnetický proužek je umístěn na rubové části karty. Jsou na něm ve formě magnetického záznamu uloženy identifikační údaje o kartě a jeho majiteli nezbytné pro provedení platební transakce. U typu této karty je jedinou možností ověření oprávněnosti držitele pouhý podpis, který lze snadno napodobit. Potom identifikace oprávněné osoby záleží jen na důslednosti obchodníka při zkoumání podpisu. Popisovaný způsob je již zastaralý a mnohdy i oprávněný uživatel má problémy se vždy podepsat stejným způsobem. Tento typ karty je snadno zneužitelný neoprávněným zkopírováním identifikačních kódů různými „skimmovacími“ zařízeními, o kterých bude hovořeno v dalších kapitolách. Vydavatelé platebních karet dnes již přecházejí na čipovou technologii, která je mnohem bezpečnější.

Magnetický proužek karty umožňuje zapisovat data do tří stop. Vydavatelé karet využívají 1. a 2. stopu, na nichž je uloženo kromě dalších zakódovaných dat také jméno držitele, číslo karty a datum její platnosti. Příklad zobrazení uložených záznamů na stopách magnetického záznamu znázorňuje obrázek (*Obr. 2*).



Obr. 2. Příklad uložení záznamů na stopách magnetického proužku platební karty⁸

Čip

V České republice se čipové karty zavedly v roce 2003 z důvodu prevence před trestnou činností spojenou se zneužitím platebních karet. Čipová technologie umožňuje uložit do paměti v čipu podrobnější informace o držiteli platební karty a také hash čtyřmístného identifikačního kódu nutného k provedení platební transakce, tzv. „PIN“. Jelikož tato technologie má vyšší zabezpečení oproti technologii s magnetickým proužkem, elektronické transakce se po zadání PIN neověřují v centru (tzv. „offline transakce“). Proto dochází k výraznému zkrácení doby transakce, což zákazníci ocení zejména při platbě u obchodníků. Zavedení této technologie se velmi rozmohlo. V ČR již téměř všechny ATM a POS terminály jsou schopny přijímat karty s čipovou technologií. Z hlediska preventivních opatření proti zneužití platební karty je zavedení čipových karet velmi přínosné a přispělo k poklesu trestné činnosti páchané zneužitím platebních karet.

⁸ Použito z [4].

Čipem je označován integrovaný obvod ve velmi malém provedení, který je určen pro zpracování informací nebo slouží jako paměť. Skládá se z následujících částí:

- Elektrické kontakty – definovány standardem normy ISO/IEC 7816-2, jejich rozmístění a přiřazení je znázorněno na obrázku (*Obr. 3*).
- CPU (mikroprocesor) – 8-mi nebo 16-ti bitový procesor, využívající zpravidla instrukční sadu Motorola 6805 nebo Intel 8051,
- Kryptografický koprocesor provádějící složité výpočty s kryptografickými operacemi.
- paměti typu RAM, ROM a EEPROM.



přiřazení kontaktů:

C1-VCC (power supply) – napájecí

C2-RST (reset signal) – reset

C3-CLK (clock signal) - hodiny

C5-GND (ground) – uzemnění

C6-VPP (program voltage input)

-rezervováno pro budoucí použití

C7-I/O (serial input a output)-vstup/výstup

C4, C8 - nepoužity

Obr. 3. Umístění a přiřazení kontaktů na čipové kartě⁹

Karty s čipovou technologií dělíme na karty kontaktní a bezkontaktní. U kontaktních je čip viditelně umístěn na lícové straně karty. U každé transakce se karta zasouvá do čtečky. U bezkontaktních je čip uschován v kartě a k načtení identifikačních údajů dojde bez fyzického kontaktu se čtečkou. Vyšší bezpečnost karet s touto technologií však znamená větší náklady na jejich výrobu, ale také náklady spojené s úpravou či výměnou ATM a POS terminálů, aby byly schopny snímat záznamy z čipových karet.

⁹ Použito a upraveno z [36].

Hybridní karty

Z důvodu rozšíření použitelnosti platebních karet, přičemž někteří obchodníci nedisponují terminály k provádění platební transakce v režimu offline, byly zavedeny karty hybridní. Ty obsahují obě zmíněné záznamy dat na magnetickém proužku i čipu.

1.4 Zpracování transakce

Proces bezhotovostní platby prostřednictvím platební karty za zboží (služby) anebo výběr hotovosti kartou lze rozdělit na proces ověření, autorizace, clearing a zúčtování.

1.4.1 Ověření

Procesem ověření je myšleno ověření platební karty u obchodníka, který je povinen zkontrolovat pravost karty, její platnost a zda ji předkládá oprávněná osoba, na jejíž jméno je karta vystavena (dle podpisu). V případě pochybností má obchodník oprávnění od osoby disponující kartou vyžádat doklad totožnosti (např. občanský průkaz nebo cestovní pas). Tato povinnost platí všeobecně u všech platebních transakcí nad 100 tisíc Kč. U čipových karet je totožnost ověřována POS terminálem (zadáním bezpečnostního kódu PIN).

1.4.2 Autorizace

Následuje po ověření. Jedná se o proces komunikace ATM nebo POS terminálů u obchodníků s vydavatelskou bankou držitele karty cestou karetní asociace. Autorizací je myšleno ověření, zda transakce je kryta finančními prostředky na účtu a zda se karta nenachází na stoplistu¹⁰. U karet bez čipu dochází nejdříve k ověření karty až poté k autorizaci.

Autorizace hlasová

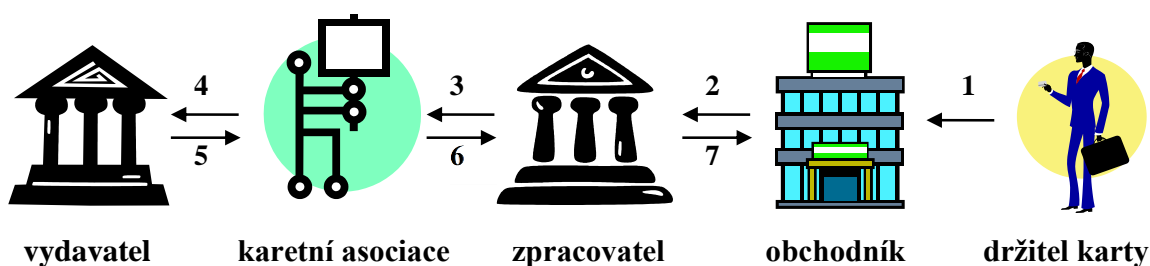
Při platbě u zastaralých mechanických imprinterů je obchodník povinen provést telefonickou (hlasovou) autorizaci na autorizační centrum při překročení autorizačního limitu. Autorizační limit je důvěrný a pro dané obchodní místo jej ve smlouvě stanovuje

¹⁰ Stoplist – Soubor dat v papírové nebo elektronické formě obsahující čísla blokových karet, které nesmějí být akceptovány k provedení transakce. Využití stoplistu při autorizaci zabraňuje zneužití zablokované karty [33].

zpracovatelská banka. Tento limit se vztahuje na součet všech transakcí v jednom dni na jednom místě, aby se platba nedala obejít rozmělněním na více transakcí. Hlasovou autorizaci je nutné provést také v případě pochybností o pravosti karty nebo podezření, že ji předkládá neoprávněná osoba. U hlasové autorizace operátor centra požaduje číslo karty, platnost, číslo obchodního místa, typ transakce (platba, výběr), částku, popřípadě další informace. V případě pozitivní autorizace je operátorem sdělen obchodníkovi autorizační kód, který se zapisuje na prodejní doklad nebo je transakce zamítnuta. Pokud následuje pokyn k zadržení karty, obchodník vyhodnotí situaci, zda ji zadrží sám nebo přivolá Policii ČR.

Autorizace automatická

Automatická autorizace probíhá vždy, pokud transakce probíhá přes ATM nebo POS terminál. Proces elektronické autorizace (od zaslání dotazu po obdržení odpovědi) ve většině případů činí 5-12 sekund. Proces autorizace znázorňuje obrázek (Obr. 4).



Obr. 4. Proces autorizace¹¹

1. Vložení karty do POS terminálu, který indikuje data uložená na magnetickém proužku nebo čipu.
2. POS terminál odešle údaje o kartě s částkou transakce zpracovateli (bance obchodníka).
3. Zpracovatel údaje přepoše do karetního systému asociace, kde jsou ověřovány některé údaje např. bezpečnostní prvky karet.

¹¹ Použito z [9].

4. Autorizační centrum karetní asociace zašle autorizační požadavek vydavateli (vydavatelské bance), která ověří oprávněnost požadované transakce z pohledu krytí dostatečnou výší prostředků na účtu, popřípadě ověří PIN.
5. Vydavatel zašle karetní asociaci autorizační odpověď (kladnou či zápornou).
6. Asociace přepošle autorizační odpověď zpracovateli.
7. Zpracovatelská banka dále přeposílá odpověď do POS terminálu, z jehož podnětu vzešel požadavek na autorizaci.

Outsourcing

Outsourcing znamená využití pro zpracování autorizace dalšího subjektu (specializovaných společností), kterým uděluje certifikaci kartová asociace. V ČR je dozorováno Českou národní bankou. Využívají jej některé banky z důvodu úspor za investování do nových systémů a technologií. V ČR se jedná např. o společnost Global Payments Europe (dříve MUZO, a.s.).

1.4.3 Clearing

Proces výměny údajů o finanční transakci mezi zpracovatelem a vydavatelem k umožnění zaúčtování transakce na účet držitele karty a rekonsiliace pozice člena asociace k vypořádání [33]. Poplatky za tento proces nehradí držitel karty, neboť se mezi sebou vypořádají účastníci transakce (vydavatel, zpracovatel, obchodník, karetní asociace).

1.4.4 Zúčtování

V této poslední fázi platební transakce dochází k převodu finančních prostředků mezi účastníky uvedenými v procesu autorizace. Clearingové organizace zasílají vydavatelům informace o transakci (jména klientů, čísla platebních karet, data, časy, částky, měny a místa transakce).

2 TRESTNÁ ČINNOST

Trestná činnost v oblasti zneužití platebních karet záleží na organizovanosti pachatelů, jejich technickému vybavení a schopnostem, obezřetnosti poškozených a technických či organizačních preventivních opatření bank. Podvody s platebními kartami se začaly objevovat prakticky od jejich uvedení na trh. V následujících podkapitolách budou uvedeny nejčastější formy této trestné činnosti, které se objevují i v ČR.

2.1 Trestná činnost oprávněného držitele platební karty

Trestné činnosti v souvislosti s použitím platební karty se kromě neoprávněné osoby mnohdy dopouští samotní držitelé karet, například přečerpáním dovoleného limitu a fiktivní krádeží.

2.1.1 Přečerpání dovoleného limitu

Tohoto protiprávního jednání se může dopustit oprávněný držitel karty tím, že přečerpá limit na svém účtu, k němuž má vydanou platební kartu a takto neoprávněně vzniklý debet nesplácí (insolvence). V 70. letech 20. století se některé banky v USA dostaly na okraj krachu, neboť klientům vydávaly karty bez ověření jejich solventnosti a bonity. V současné době jsou vydavatelé bankovních karet obezřetní a řádně si uvedené skutečnosti ověřují.

2.1.2 Fiktivní krádež

Vyskytují se i případy, že oprávněný držitel nahlásí ztrátu či odcizení své platební karty a poté v úmyslu získání neoprávněného majetkového prospěchu kartou provádí platební transakce ke škodě vydavatele platební karty. Toto však může provést pouze do doby blokace platební karty.

2.2 Trestná činnost neoprávněného držitele platební karty

K této trestné činnosti mnohdy zlodějům nebo nepoctivým nálezcům napomáhají samotní oprávnění držitelé platební karty svou hrubou nedbalostí. Někteří totiž mají platný PIN označený přímo na kartě nebo jejím obalu, ve svých poznámkách v peněženke nebo uložen ve svém mobilu bez šifrování. Pokud dojde ke ztrátě či odcizení věci s označeným

PIN kódem společně s kartou, snadno může dojít k neoprávněnému výběru finančních prostředků z účtu držitele karty.

Zneužití karty rodinnými příslušníky a osobami blízkými

Tyto případy jsou poměrně časté, neboť rodinní příslušníci a blízké osoby mohou poměrně snadno zjistit PIN oprávněného držitele. Poté bez svolení oprávněného držitele kartu použijí a vrátí zpět, takže vlastník karty tuto skutečnost zjistí z výpisu z účtu nebo neprovedením platební transakce z důvodu nedostatku finančních prostředků na účtu.

Zneužití karty kolemjdoucími osobami

Ohroženou skupinou bývají starší obyvatelé, kteří jsou mnohdy důvěřiví a často méně ostražití. Pachatelé jim s úsměvem na rtu nabídnou pomoc při výběru z ATM, avšak kolik skutečně vybrali, zjistí poškození většinou až z výpisu z účtu.

Nepoctivý nálezce

V případě ztráty karty záleží na tom, do jakých nepovolaných rukou se dostane. Pokud pachatel zjistí PIN, může pomocí nalezené platební karty neoprávněně čerpat prostředky z ATM nebo platit u obchodníka.

Krádež platebních karet

Jedním z nejčastějších způsobů zneužití platebních karet je jejich krádež spojená s jejich následným neoprávněným použitím. Zde je rozhodující doba, kdy toto poškození zjistí a provede následnou blokadu karty. V případě zjištění odcizení karty po několika dnech nebo až po obdržení výpisu z účtu, může vzniklá škoda dosáhnout velkých částek. Není ani nutná znalost PIN, neboť u některých obchodníků jsou stále využívány imprintery.

Zneužití nedoručené karty

Jedná se o typ podvodů ze strany zaměstnanců bank, pošt, kurýrních a bezpečnostních služeb, ale také sousedů, přátel nebo rodinných příslušníků. Pokud se nedoručená platební karta dostane do rukou neoprávněné osoby, může na čistý podpisový proužek napodobit podpis oprávněného držitele a poté kartu zneužít. Z tohoto důvodu většina bankovních institucí již platební karty vydává výhradně na svých pobočkách. Některé banky, např. mBank, AXA, GE Money Bank je sice doručují poštou,

avšak karta je aktivována buď službou Internetbanking nebo telefonicky přes operátora banky.

Odcizená identita

Byly zaznamenány i případy, ve kterých pachatelé získali kartu na základě podvodné žádosti o vydání platební karty, přičemž použili padělané či odcizené osobní doklady.

Padělání či pozměnění prodejních dokladů

Při platbě embosovanou kartou na imprinterech obchodník vyhotoví platební doklad, na němž jsou otisknuté údaje platební karty. U některých zjištěných případech obchodník ve svůj prospěch změnil částku pravého platebního dokladu, popřípadě padělal doklad celý. U pozměnění dokladu je pak na držiteli karty, aby prokázal rozdílnou výši skutečným dokladem. Proto je žádoucí doklady uchovávat minimálně do doby obdržení výpisu z účtu. Případy padělání či pozměnění platebních dokladů se vyskytují zejména v zahraničí.

2.3 Závažnější formy trestné činnosti

V následujících podkapitolách jsou uvedené závažnější formy trestné činnosti, neboť jednotliví pachatelé, popřípadě skupiny pachatelů již používají technické prostředky k získání platební karty nebo finančních prostředků z ATM.

2.3.1 Libanonská smyčka

Ve svém principu se jedná o jednoduché zařízení sloužící k záchytu platební karty v ATM. Představuje jednoduchý plastový kryt se smyčkou umístěný na vstupním otvoru pro kartu v ATM. Umožňuje sice vstup karty do ATM, již ne však výběr peněz a vyjmutí karty. Oprávněný držitel se poté domnívá, že z nějakého důvodu došlo k zadržení jeho karty bankou. Poté k němu přistupuje pachatel, jako náhodná „dobrá duše“ nebo převlečen za policistu a předstírá snahu pomoci s řešením této situace. Zmanipuluje klienta k opětovnému zadání PIN. Po opětovném neúspěchu klient opouští ATM a pachatel vyjme zachycenou kartu, kterou použije k neoprávněnému výběru z ATM či platbě u obchodníků.

Libanonskou smyčku zavedli v USA na počátku 90. let pachatelé z Libanonu, podle kterých pochází název této metody. Obranou je neopouštět ATM v případě, že nevydá platební kartu a okamžitě telefonicky přivolat provozovatele ATM, případně Policii ČR. Ukázky libanonských smyček jsou uvedeny v příloze *P I*.

2.3.2 Zadržné lišty na ATM pro výběr peněz

Pachatelé u vybraných typů ATM nasazují na štěrbinu pro výdej peněz lištu, která je k ATM ze zadní strany nalepena oboustrannou lepicí páskou. Uživatelé platební karty po zadání transakce nevyjedou žádné peníze, nalepí se totiž na pásku a pachatel je následně odcizí. Tyto případy se v roce 2007 vyskytovaly na Slovensku a následně se objevily také v ČR, poprvé v Hradci Králové, proto se začal používat termín „hradecká lišta“ [23]. Ukázka takové lišty je uvedena v příloze *P II*.

2.4 Trestná činnost organizovaného zločinu

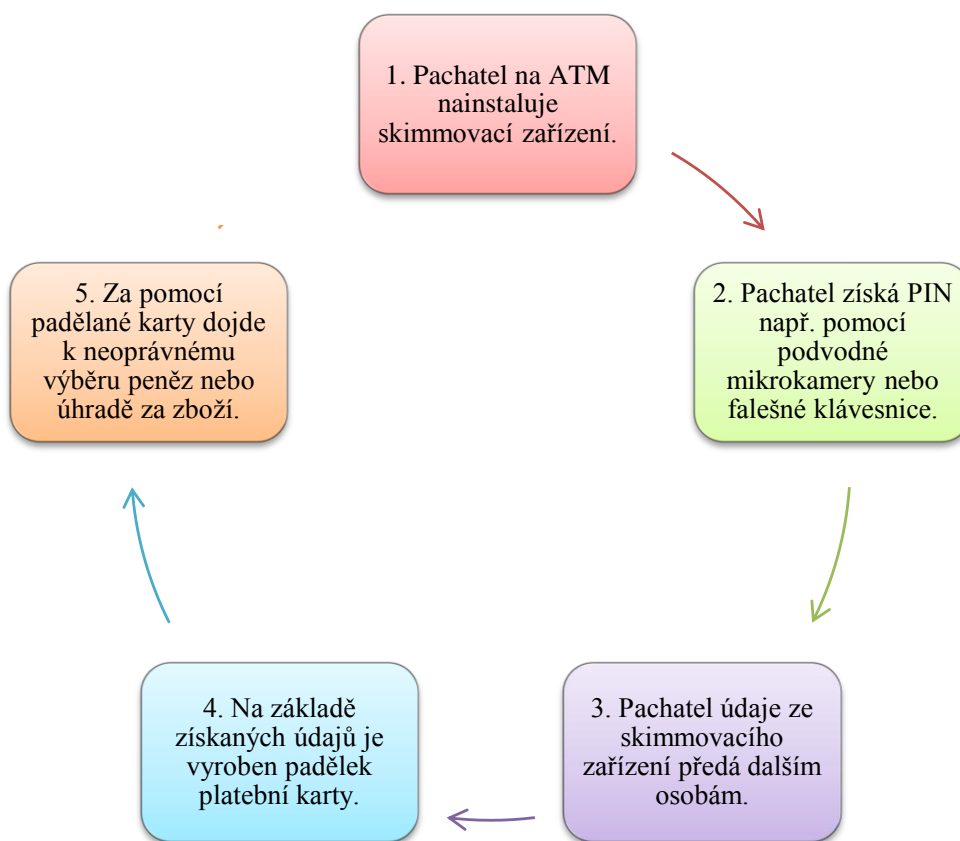
Jeden z nejnebezpečnějších společenských problémů dnešní doby představuje právě organizovaný zločin, který je mnohem nebezpečnější než trestná činnost páchaná jednotlivci. Činnost organizovaných skupin může způsobit nestabilitu světových ekonomických i politických systémů. Podle Útvaru pro odhalování organizovaného zločinu se zaměřují na podvody s platebními kartami bulharské gangy, ale také organizované skupiny pachatelů bývalého Sovětského svazu, zemí jihovýchodní Asie, Nigerie a západní Evropy [29]. K neoprávněnému výběru finančních prostředků poté dochází z ATM zejména ve státech východní Evropy.

Organizované skupiny se vyznačují složitostí struktur, které jsou rozdělené na početné podskupiny na území několika států. Vysoký stupeň organizovanosti a členitosti snižuje možnost dopadení pachatele. Například bulharský pachatel ve spolupráci s čínským informatikem mohou organizovat krádež dat z platebních karet v ČR. Neoprávněný výběr finančních prostředků nebo nákup zboží pomocí padělané karty potom provádí kdekoli ve světě třetí osoby, které jsou na konci řetězce organizované skupiny.

Trestná činnost uvedená v následujících podkapitolách bývá ve většině případů právě dílem organizovaného zločinu.

2.4.1 Skimming

Tímto termínem bývá označována trestná činnost spočívající v nelegálním zkopírováním údajů z magnetického proužku karty bez vědomí oprávněného držitele karty. Pochází z anglického slova „to skim“ (sbírat), přeneseně tedy z karty získat to nejlepší. Takto získané (odcizené) údaje z platební karty skupiny pachatelů používají k výrobě padělaných platebních karet, kterými zpravidla v jiných státech vybírají finanční prostředky z ATM popřípadě platí za různé zboží. Postup fenoménu skimming znázorňuje obrázek (Obr. 5).



Obr. 5. Postup skimming¹²

¹² Použito a upraveno z [39].

Skimming ATM

Pachatelé této trestné činnosti jsou velmi dobře technicky vybaveni a používají dnes již dokonalé skimmovací zařízení sloužící k neoprávněnému získání údajů z magnetického proužku karty, ale také k získání kódu PIN. Dokonale znají skutečný vzhled, barevné provedení, materiál a rozměry jednotlivých komponentů vytipovaného ATM. Vyrábí falešné nástavce se skimmovacím zařízením, popřípadě celé panely. Tyto nasadí na ATM, zejména za pomoci oboustranně lepicích pásek, suchých zipů nebo různých lepicích tmelů. Skimmovací zařízení na ATM ponechávají i několik dní. Získaná data jsou ukládána do paměti skimmovacích zařízení nebo jsou pomocí bezdrátového přenosu (např. bluetooth nebo SMS zprávami) přenášena do mobilních telefonů či notebooků. K tomuto přenosu jsou používány technické prvky z vysílaček nebo mobilních telefonů. Kapacita paměti skimmovacích zařízení umožní uložení dat minimálně z 200 ks platebních karet [4].

Provozovatelé ATM v rámci zvýšení bezpečnosti svých klientů začali u ATM používat antiskimmovací nástavce. Pachatelé se však přizpůsobili a dokáží instalovat skimmovací zařízení i na tyto nástavce viz obrázek (*Obr. 1 v příloze P III*).

ATM České spořitelny jsou chráněny antiskimmovacím zeleným nástavcem, tzv. „zelený zobák“, které bylo účinné do 1. poloviny roku 2008. V 2. polovině roku 2008 se objevila nová skimmovací zařízení překonávající i tuto ochranu viz obrázek (*Obr. 2 v příloze P III*). Koncem roku 2008 byly zjištěny technicky podstatně dokonalejší skimmovací zařízení viz obrázek (*Obr. 3 v příloze P III*). Konkrétně byly napadány ATM typu NCR 5884 a NCR 5887 [24].

Zařízení sloužící ke zjištění kódu PIN u ATM

PIN kód pachatelé získávají např. pozorováním klávesnice ATM dalekohledem nebo nahlížením oběti přes rameno. Sofistikovanější způsob jsou falešné klávesnice a miniaturní kamery umístěné na ATM, které snímají stisknutí tlačítek klávesnice. Získané údaje jsou potom ukládány do paměti, která je součástí falešných částí ATM.

Provozovatelé ATM v médiích často upozorňují klienty, aby při zadávání kódu PIN zakrývali klávesnici dlaní druhé ruky. Na toto pachatelé reagovali mikrokamerami skrytě umístěnými ve falešných krytech klávesnice viz obrázek (*Obr. 6 v příloze P III*).

V současné době ATM a POS terminály v ČR neobsahují technická zařízení, která by detekovala výskyt skimmovacích zařízení. Jejich výskyt lze zjistit pouze detailní vizuální prohlídkou. Ačkoli falešné části ATM se skimmovacím zařízení se na první pohled zdají být dokonalé, při detailním pozorování si můžeme povšimnout drobných technických nedostatků (např. podezřelé mezery ve spojích a rozích, barevné odlišnosti od ostatních částí ATM atd.) viz obrázek (*Obr. 4 v příloze P III*). Všechny části ATM musí být pevně připevněny, pokud se dají sejmut, je vysoké podezření, že ATM obsahuje skimmovací zařízení. U klávesnic pozorujeme, jestli na nich není přilepena jakákoli fólie, zda klávesy příliš nevystupují nebo naopak nejsou moc zapuštěné. Při jakémkoli takovém zjištění je nutné neprodleně vyrozumět Policii ČR nebo provozovatele ATM.

Skimming u vstupních dveří do samoobslužné zóny ATM

Některé ATM jsou umístěny v uzavřené místnosti, do které je umožněn vstup pouze po vložení platební karty do čtecího zařízení na dveřích. V Brně byl zjištěn výskyt skimmovacího zařízení u čtečky vstupních dveří. Pro zjištění zadávaného kódu PIN pak pachatelé používají různé záznamové zařízení např. vložené do požárního hlásiče nebo kdekoliv jinde s výhledem na klávesnici ATM. V tomto případě se však nenašlo. Na obrázku (*Obr. 7 v příloze P III*) je uvedena ukázka skimmovacího zařízení u čtečky vstupních dveří do zóny ATM.

Skimming platebních terminálů

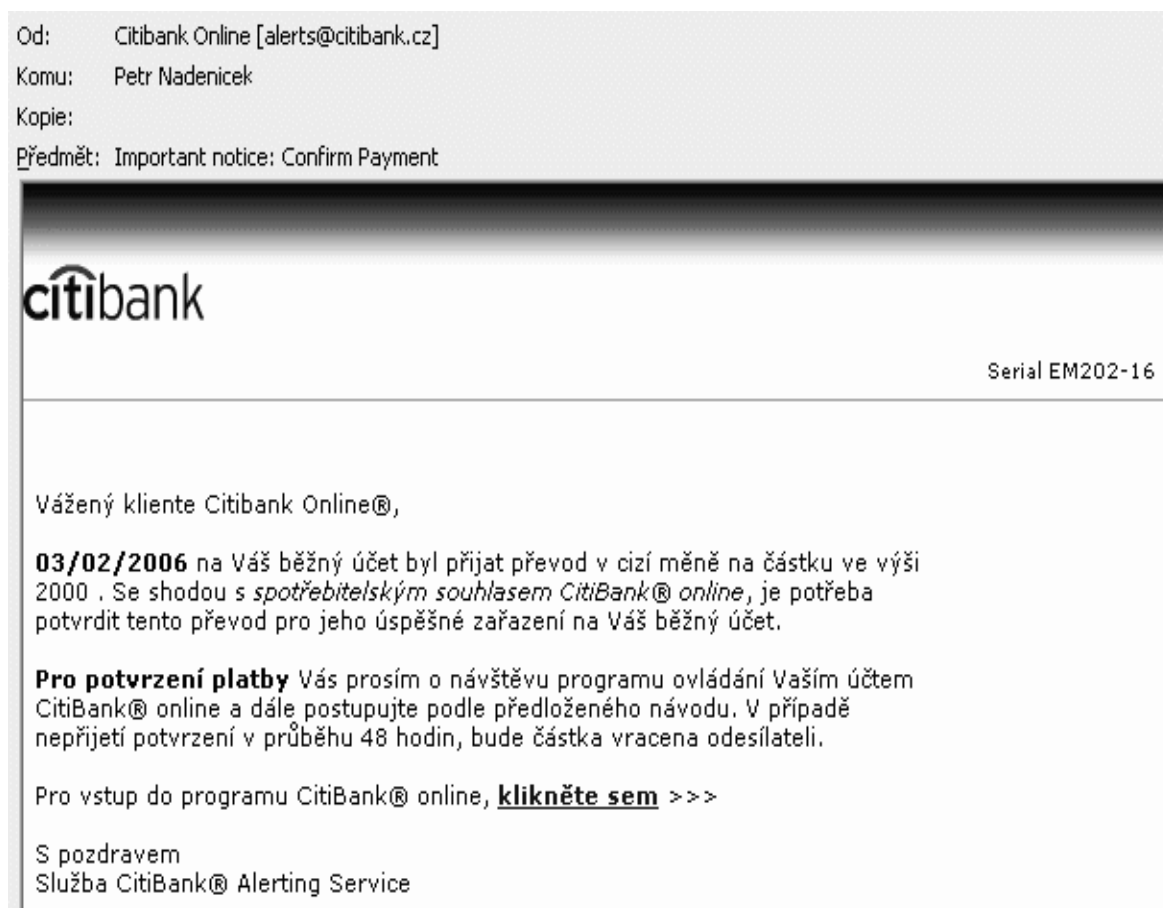
Byly zjištěny i případy instalace skimmovacích zařízení na POS terminálech u obchodníků, kteří byli součástí organizovaného zločinu. Výskyt těchto případů byl zjištěn v Rakousku, Švédsku, Švýcarsku, Německu, Francii, Španělsku, Holandsku, Itálii a Rumunsku [23]. Na obrázku (*Obr. 8 v příloze P III*) je uvedena ukázka takového zařízení.

Přenosné skimmovací zařízení

Byly také zjištěny případy, ve kterých oprávněný držitel karty při placení v restauraci či hotelu svěřil kartu obsluhujícímu personálu. Pachatel nenápadně protáhl kartu vlastní přenosnou čtečkou, čímž neoprávněně získal údaje z magnetického proužku karty. Takto odcizená data byla použita k výrobě padělků karet, kterými pachatelé platili v obchodech s imprintery. Podpis předložitelky karty totiž obchodníci většinou buď nekontrolují, nebo jen formálně. Přenosná skimmovací zařízení mohou mít i velmi malé

rozměry (velikost zapalovače). Možné typy provedení jsou uvedeny (*Obr. 9 v příloze P III*).

2.4.2 Phishing



Obr. 6. Phishing – podvodný e-mail¹³

Název pochází z anglického slova fishing (rybaření, či chytání údajů). Jde o nevyžádanou podvodnou e-mailovou zprávu údajně od banky nebo od asociace Visa. Klient je v ní vybízen ke sdělení údajů o svém účtu, kartě včetně její platnosti a kódu PIN. V e-mailu bývá i odkaz vzbuzující dojem k přihlášení do oficiální webové stránky banky. Podvržený odkaz však přesměruje na podvodnou stránku, z níž jsou sdělené údaje odesílány podvodníkům. Sdělení uvedených údajů je zdůvodňováno například údajným

¹³ Použito z [40].

podezřením ze zneužití karty. V ČR se tyto případy objevily na počátku roku 2004. Objektem zájmu byli klienti České spořitelny, a.s. ale také Citibank, a.s. která v roce 2007 zaznamenala čtyřicet tisíc případů Phishing. Klienti by v žádném případě na tyto výzvy neměli reagovat a informovat o tom Policii ČR. Na obrázku (*Obr. 6*) je uveden příklad zjištěného případu phishing na klienty Citibank, a.s.

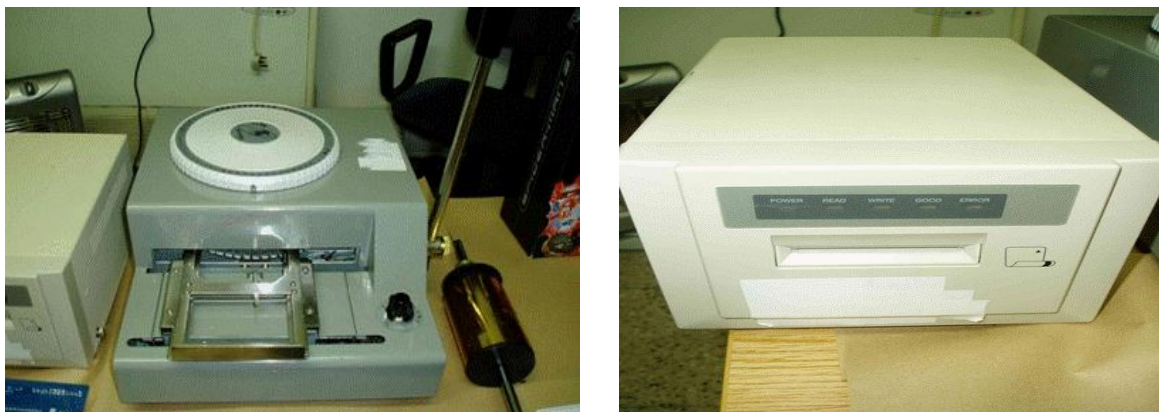
2.4.3 Padělání platebních karet

Prvními padělky platebních karet byly v podobě různě pozměněných a upravených originálních karet. Později se objevily kompletně padělané karty s pochybnou kvalitou. Padělatelé následně zjistili, že ATM přijme jakoukoli kartu s rozměry dle ISO 3554 a magnetickým proužkem. Proto pro výběr z ATM používají čistě bílé plastové karty, popřípadě v rámci ušetření také další karty (klientské, vstupní, věrnostní karty obchodních řetězců, čerpacích stanic, telefonní karty apod.) s nahranými zkopírovanými údaji na magnetickém proužku. Při platbě v obchodech používají padělky s napodobeninou originálního potisku karet, které však postrádají číslo karty, dobu platnosti, jméno uživatele a často také hologram. Spoléhají zkrátka na nedůslednost obchodníků. V roce 2006 byly na území EU nalezeny v ATM klubové karty stříbrné nebo zlaté barvy s nápisy např. SKY TEAM CLUB, CANCAN CLUB, NORWICH CLUB s adresou [4]. V první fázi bylo zjištěno, že na kartách byly nahrány údaje z velkého množství dat získaných hackery v USA. Kód PIN byl získán nezjištěným způsobem. Na padělání karet se podílely gangy ze zemí bývalého Sovětského svazu. Protože u některých karet nesouhlasil PIN kód, došlo k jejich zadržení v ATM. V mnohých případech odcizená data z platebních karet pachatelé používají u internetových plateb bez nutnosti fyzické přítomnosti platební karty.

K výrobě padělaných karet pachatelé zpravidla používají:

- program generování čísel karet (Internet-CreditMaster/Wizard),
- neoprávněně získané údaje z magnetického proužku karet (skimming),
- počítač, bílé plasty, encoder, embosser (cca 800,- USD), card printer,
- grafický program (např. Corel Draw, Paintshop Pro).

Celkové náklady na pořízení uvedeného hardware a software činí přibližně 4.000,- USD. Na obrázku (*Obr. 7*) je uvedena ukázka zařízení padělatelské dílny.



Obr. 7. Ukázka zařízení padělatelské dílny¹⁴

3.5 Trestněprávní kvalifikace

Případy zneužití platební karty je možno rozdělit do dvou hlavních skupin, tedy na případy neoprávněného držení a případy padělání či pozměnění platebních karet.

Neoprávněné držení platební karty

Tyto případy byly do konce roku 2009 kvalifikovány jako trestný čin stejného názvu podle § 249b trestního zákona [13]. Skutková podstata uvedeného trestného činu byla aplikována na toho, kdo si neoprávněně opatří nepřenositelnou platební kartu jiného, identifikovatelnou podle jména nebo čísla, nebo předmět způsobilý plnit její funkci. Za popisované jednání hrozil pachateli trest odnětím svobody až na dvě léta, nebo trest peněžitý či propadnutí věci nebo jiné majetkové hodnoty.

Od 1.1.2010 je popisované jednání kvalifikováno podle § 234 odst. 1 trestního zákoníku [14]. Skutková podstata byla rozšířena na jednání pachatele, který sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává nepřenositelnou platební kartu identifikovatelnou podle jména nebo čísla. Trest hrozící pachateli za uvedené jednání zůstal zachován.

K trestnosti popisovaného jednání postačí pouze neoprávněné držení platební karty bez právního důvodu a pachatel ji ani nemusí použít k další trestné činnosti čerpáním peněžních prostředků. Pokud za pomoci neoprávněně držené platební karty odčerpá z účtu

¹⁴ Použito z [24].

oprávněného vlastníka peněžní prostředky, dopustí se dále trestního činu krádeže nebo podvodu podle § 247 nebo § 250 trestního zákona [13], respektive § 205 či § 209 trestního zákoníku [14]. Výše trestu se poté odvíjí od vzniklé škody.

Padělání či pozměnění platební karty

Vzhledem k dřívější nejednoznačné aplikaci trestného činu padělání a pozměňování peněz podle § 140 odst. 2 a § 143 trestního zákona [13] na případy výroby a padělání platebních karet, požádalo policejní prezidium Policie ČR prostřednictvím odboru bezpečnostní politiky Ministerstva vnitra Nejvyšší státní zastupitelství (NSZ) o zaujetí právního stanoviska k trestnímu postihu uvedených případů. Výsledkem bylo vydání stanoviska NSZ [22], v němž je uvedeno, že „úmyslné jednání pachatele spočívajícího ve zhotovení napodobeniny (kopie) bezhotovostního platebního prostředku v takové kvalitě, že mu to umožní realizovat neoprávněně bankovní operaci (obchod), lze posoudit jako uvedený trestný čin. Kvalifikace tohoto trestného činu je možno aplikovat také na jednání pachatele, který provede bankovní operaci prostřednictvím bankomatu za pomoci napodobeniny platební karty (plastifikované karty opatřené překopírovaným magnetickým proužkem nebo údaji získanými z čipu) [22]. Za uvedený trestný čin hrozil pachatelům trest ve výši 5 až 10 let.

Nový trestní zákoník [14], účinný od 1.1.2010, ve skutkové podstatě dle § 234 odst. 3 již obsahuje přímo termín platební karty. Tímto trestním zákoníkem byl však snížen trest za padělání platební karty na 3 až 8 let.

II. PRAKTICKÁ ČÁST

3 VYHODNOCENÍ STATISTIK TRESTNÉ ČINNOSTI

Z údajů vložených jednotlivými policejními útvary do informačních systémů Policejní prezidium Policie ČR, Centrála informatiky a analytických procesů Služby kriminální policie a vyšetřování v Praze zpracovává statistické údaje o trestné činnosti. Ze souhrnných statistik trestné činnosti dostupných na policejním intranetu [34] byly zjištěny níže uvedené údaje k trestnému činu "Neoprávněné držení platební karty" podle § 249b trestního zákona [13] a trestného činu "Neoprávněné opatření, padělání a pozměnění platebního prostředku" podle § 234 trestního zákoníku [14].

3.1 Statistika trestné činnosti v celé ČR

Z uvedeného zdroje [34] byly zpracovány a vyhodnoceny statistiky trestné činnosti za období let 2000-2010 v rámci území celé ČR. V tabulce (*Tab. 2*) je uveden počet případů zjištěných¹⁵ a objasněných¹⁶, procento objasnění¹⁷, způsobená škoda a rozlišení případů podle speciálního hlediska pachatelů (recidivisté, nezletilí, mladiství)¹⁸. Z tabulkových údajů vyhotoven grafický vývoj trestné činnosti viz graf (*Obr. 8*).

Uvedené statistiky však nerozlišují konkrétní formy trestné činnosti uvedené v kapitole 2. Minimálně do 17.6.2004 v nich byly vedeny i případy oznámení krádeží či ztrát peněženek, kabelek, kufříků či zavazadel, v nichž se nacházela také platební karta. Na základě nálezu Ústavního soudu ČR [20] se již nekvalifikují a tudíž statisticky nevykazují případy, v nichž nebyl jednoznačně prokázán úmysl pachatele směřující ke zneužití platební karty. Od té doby byly již vykazovány pouze případy, v nichž se pachatel pokusil či skutečně vybral z účtu poškozeného finanční prostředky prostřednictvím ATM či POS terminálů. Proto lze považovat za lépe vypovídající o uvedené trestné činnosti statistiky od roku 2005. Je však evidentní, že počet zjištěných případů je od roku 2005 více než 10x vyšší než v letech 2000 a 2001. Od této doby osciluje kolem hranice 8000 případů za rok.

¹⁵ Zjištěné případy – takové, které byly Policii oznámeny občany, popřípadě bankovními ústavy.

¹⁶ Objasněné případy – případy, u kterých byla vytipována a usvědčena konkrétní osoba pachatele.

¹⁷ Procento objasnění – podíl případů objasněných ke zjištěným * 100 [%].

¹⁸ Recidivisté – pachatelé, kteří se trestné činnosti dopustili opakovaně. Nezletilí – pachatelé, kteří nejsou trestně odpovědní (do 15-ti let), mladiství – pachatelé ve věku od 15-ti do 18-ti let).

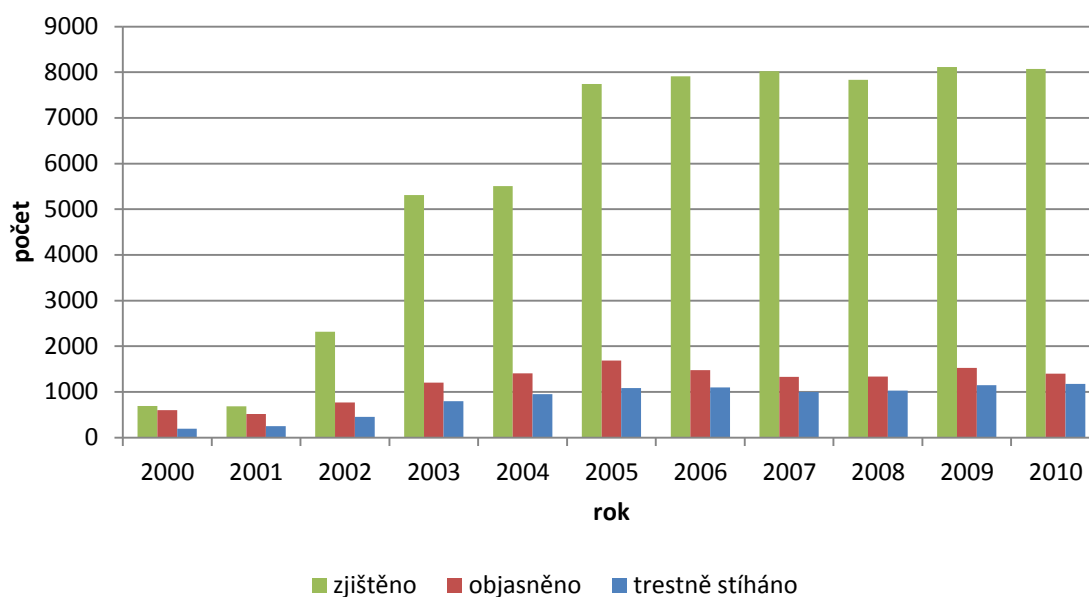
Tab. 2. Statistika trestné činnosti spojené s neoprávněným držením platební karty v ČR¹⁹

rok	zjištěno	objasněno	procento objasnění	trestně stíháno	způsobená škoda [tisíce Kč]	speciální hledisko pachatelů		
						recidivisté	nezletilí	mladiství
2000	693	604	87,16%	191	4 450	140	150	71
2001	688	520	75,58%	251	6 774	172	25	69
2002	2 321	769	33,13%	453	19 874	380	27	90
2003	5 310	1 206	22,71%	799	26 745	605	60	105
2004	5 510	1 408	25,55%	951	33 837	682	60	109
2005	7 739	1 684	21,76%	1 083	43 606	789	71	96
2006	7 908	1 479	18,70%	1 101	41 621	714	87	117
2007	8 023	1 332	16,60%	1 000	44 082	647	38	103
2008	7 833	1 337	17,07%	1 026	51 278	680	44	93
2009	8 113	1 529	18,85%	1 148	52 855	805	53	106
2010	8 074	1 398	17,31%	1 175	339 919	891	32	125
průměr	5 656	1 206	32,22%	834	60 458	591	59	99

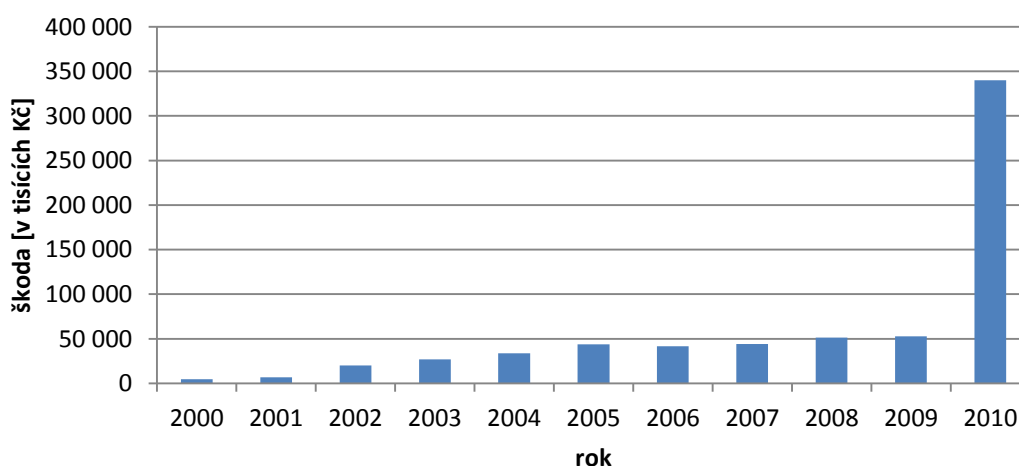
Ze statistik bylo zjištěno procento objasněných případů, které bylo velmi dobré v prvních dvou letech sledovaného období, od roku 2006 kleslo pod hranici 20%. Počet trestně stíhaných osob je menší než počet objasněných případů, což je způsobeno tím, že v některých případech bylo trestní stíhání podle § 11 odst. 1 trestního řádu [15] nepřipustné (např. amnestie, promlčení, nezletilí) nebo podle § 172, odst. 2 trestního řádu [15] neúčelné (např. trest, k němuž by trestní stíhání vedlo, byl zcela bez významu vedle trestu, za jiný trestný čin, který byl obviněnému již uložen nebo který by ho podle očekávání postihl).

Přehled škod způsobených trestnou činností spojenou se zneužitím platebních karet v ČR a jejich vývoj zobrazuje graf (Obr. 9). Je zřejmé, že po postupném narůstání škod způsobených uvedenou trestnou činností do roku 2005, se vývoj poměrně stabilizoval. V roce 2010 byl zaznamenán prudký nárůst, více než 6x vyšší, v porovnání s předcházejícími léty. Počet případů byl přitom ještě o 39 menší než v roce 2009.

¹⁹ Vytvořeno autorem práce ze statistických údajů uvedených v [34].



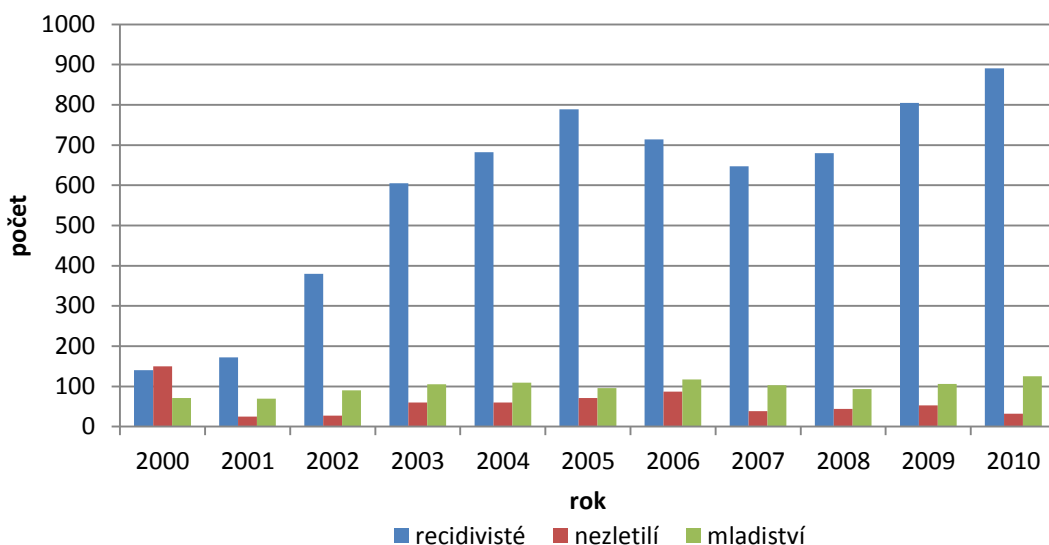
Obr. 8. Vývoj trestné činnosti spojené se zneužitím platebních karet v ČR²⁰



Obr. 9. Přehled škod způsobených trestnou činností spojenou se zneužitím platebních karet v ČR²⁰

Graf (Obr. 10) znázorňuje vývoj speciálního hlediska pachatelů zájmové trestné činnosti. Na ní mají od roku 2001 největší podíl recidivisté, mnohonásobně nižší nezletilí a mladiství pachatelé.

²⁰ Vytvořeno autorem práce ze statistických údajů uvedených v [34].



Obr. 10. Speciální hledisko pachatelů sledované trestné činnosti²¹

3.2 Statistika trestné činnosti v krajích

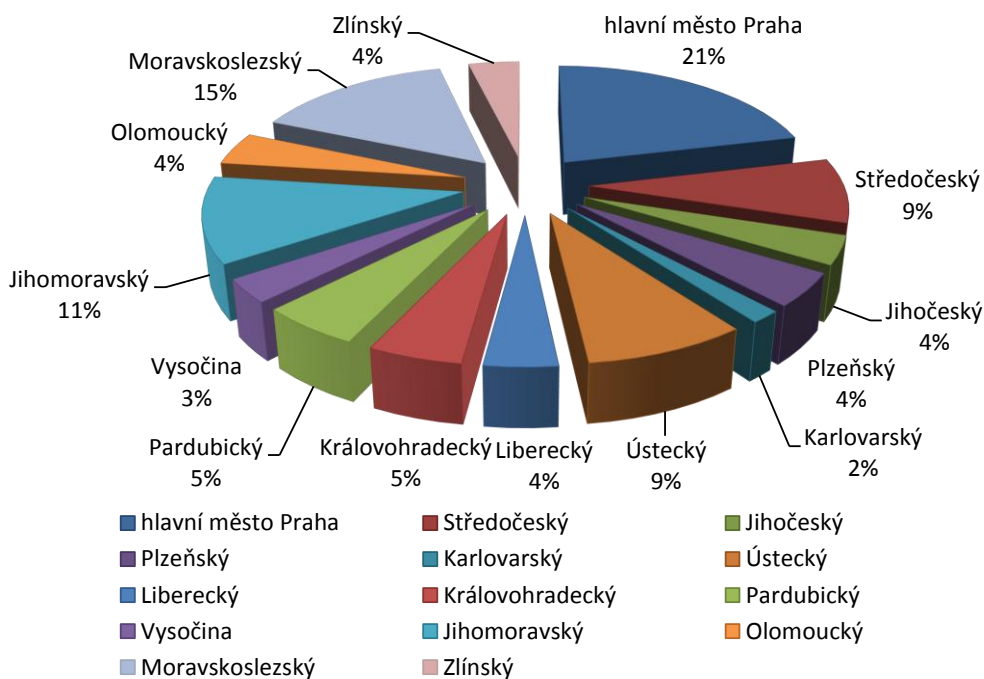
Statistické údaje předmětné trestné činnosti byly rozlišeny podle místa spáchání v rámci území jednotlivých samosprávních územních celků (krajů). Číselné hodnoty jsou vyobrazeny v tabulce (Tab. 3) a vývoj v grafu (Obr. 11).

Tabulka (Tab. 3) v porovnání s tabulkou (Tab. 2) postrádá údaje za rok 2000, neboť za tento rok jsou vedeny statistiky pouze pro území tehdy 8 krajských správ Policie ČR, jejichž územní působnost nebyla v souladu s rozdělením územních samosprávních celků v ČR. Tyto údaje by nebylo možno objektivně použít pro další analýzu. Přední místo s podílem 21% zaujímá Hlavní město Praha, druhé Moravskoslezský kraj (15%) a třetí Jihomoravský kraj (11%).

²¹ Vytvořeno autorem práce ze statistických údajů uvedených v [34].

Tab. 3. Statistika trestné činnosti spojené s neoprávněným držením platební karty v rámci jednotlivých krajů²²

rok	kraj														ČR celkem
	hlavní město Praha	středočeský	jihocheský	plzeňský	karlovarský	ústecký	liberecký	královohradecký	pardubický	vysočina	jihomoravský	olomoucký	moravskoslezský	zlínský	
2001	260	65	34	33	19	33	13	47	14	26	63	21	41	19	688
2002	422	144	81	117	74	124	71	130	202	149	335	81	266	125	2 321
2003	710	332	271	422	164	323	197	310	338	177	698	309	815	244	5 310
2004	770	499	376	182	87	442	217	327	394	167	680	307	862	200	5 510
2005	1 909	556	402	378	122	658	330	339	428	208	699	334	1 059	317	7 739
2006	1 730	651	406	356	102	740	335	397	386	210	771	318	1 210	296	7 908
2007	1 642	780	211	334	123	754	363	388	397	252	811	389	1 246	333	8 023
2008	1 638	683	154	348	116	745	290	399	426	205	911	358	1 291	269	7 833
2009	2 045	818	116	290	103	707	313	384	412	213	915	356	1 200	241	8 113
2010	1 963	744	259	270	102	750	251	340	324	324	1 115	223	1 114	295	8 074
celkem	13 089	5 272	2 310	2 730	1 012	5 276	2 380	3 061	3 321	1 931	6 998	2 696	9 104	2 339	61 519



Obr. 11. Přehled trestné činnosti spojené s neoprávněným držením platební karty zjištěná v rámci území jednotlivých krajů v ČR za období let 2001-2010²²

²² Vytvořeno autorem práce ze statistických údajů uvedených v [34].

4 ANALÝZA RIZIKA ZNEUŽITÍ PLATEBNÍ KARTY

Za riziko je obecně považována možnost, že s určitou pravděpodobností nastane událost, která je z bezpečnostního hlediska nežádoucí. Analýza rizika představuje proces, v němž se identifikují hrozby, určí se jejich velikost a zkoumá se jejich vliv na bezpečnost posuzovaného subjektu. Metody stanovení rizika jsou kvalitativní a kvantitativní. Kvalitativní metody používají slova k popisu rozsahu možných následků a pravděpodobnosti, že k nim dojde. Oproti tomu u kvantitativních metod jsou používány číselné hodnoty, které jsou získány z různých zdrojů, například ze statistických údajů událostí, které již nastaly v minulosti.

Při analýze rizika bude vycházeno z následujících otázek:

- Jaký nežádoucí stav může nastat?
- Jaká je pravděpodobnost, že se takto stane?
- Jak závažné mohou být následky nežádoucího jevu?

Vzhledem k problematice řešené v této diplomové práci byly stanoveny následující odpovědi:

- **Nežádoucí stav** – krádež či jiné neoprávněné držení platební karty a neoprávněné získání jejich identifikačních kódů (skimming) pachatelem jednajícím v úmyslu kartu či údaje o kartě použít k nezákonnému obohacení sebe popřípadě dalších osob.
- **Pravděpodobnost** – míra určitosti, že se stane nežádoucí stav ve vztahu k jedné platební kartě a ve vztahu k vlastníkovu karty.
- **Následky** – vyjádřeny v podobě finančních škod a jejich ekonomických dopadů na poškozené majitele platebních karet.

Mezinárodní normy a statistiky umožňují použít nejen již zavedené, ale i vlastní metody analýzy rizika. Jediným požadavkem je, aby při zvýšení hodnoty aktiva, hrozby nebo zranitelnosti se zvýšila i závažnost rizika [8]. Proto pro analýzu rizika byla zvolena vlastní kvantitativní metoda v analogii s analýzou dle [8] vycházející ze zjištěných případů neoprávněného držení platebních karet za období let 2001-2010 [34].

4.1 Stanovení pravděpodobnosti

Pravděpodobnost se obvykle vyjadřuje jako počet událostí za časovou jednotku. Ze zjištěných statistických údajů v tabulce (Tab. 2) byla vypočítána pravděpodobnost vzniku 1 posuzované nežádoucí události v ČR za jednotku času [hod, min]. Stanovena byla také pravděpodobnost, s jakou nastane 1 nežádoucí událost každou hodinu [%] viz tabulka (Tab. 4). Dále byla vypočtena pravděpodobnost zneužití platební karty na jednu kartu a pravděpodobnost poškození touto událostí občanů ČR starších 15-ti let.

Tab. 4. Pravděpodobnost vzniku události²³

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	průměr
pravděpodobnost vzniku 1 události za čas [hod:min]	13:13	4:17	2:05	1:59	1:13	1:11	1:09	1:12	1:08	1:08	2:51
pravděpodobnost vzniku 1 události za hodinu [%]	7,85	26,50	60,62	62,90	88,34	90,27	91,59	89,42	92,61	92,17	70,23

V tabulce (Tab. 5) je uvedena pravděpodobnost napadení platebních karet, tedy pravděpodobnost zneužití jedné platební karty v [%] a počet karet na jednu nežádoucí událost. Pro tuto analýzu byly použity údaje o celkovém počtu všech vydaných platebních karet, které ve svých statistikách zveřejňuje SBK [31].

Tab. 5. Pravděpodobnost napadení platebních karet²⁴

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	průměr
celkový počet všech vydaných karet [tis]	4659	5296	6 373	6 867	7 390	7 865	8 623	8 931	9 054	9 268	7433
pravděpodobnost zneužití jedné karty za rok [%]	0,015	0,044	0,083	0,08	0,105	0,101	0,093	0,088	0,09	0,087	0,079
počet karet na 1 případ za rok	6 772	2 282	1 200	1 246	955	995	1 075	1 140	1 116	1 148	1793

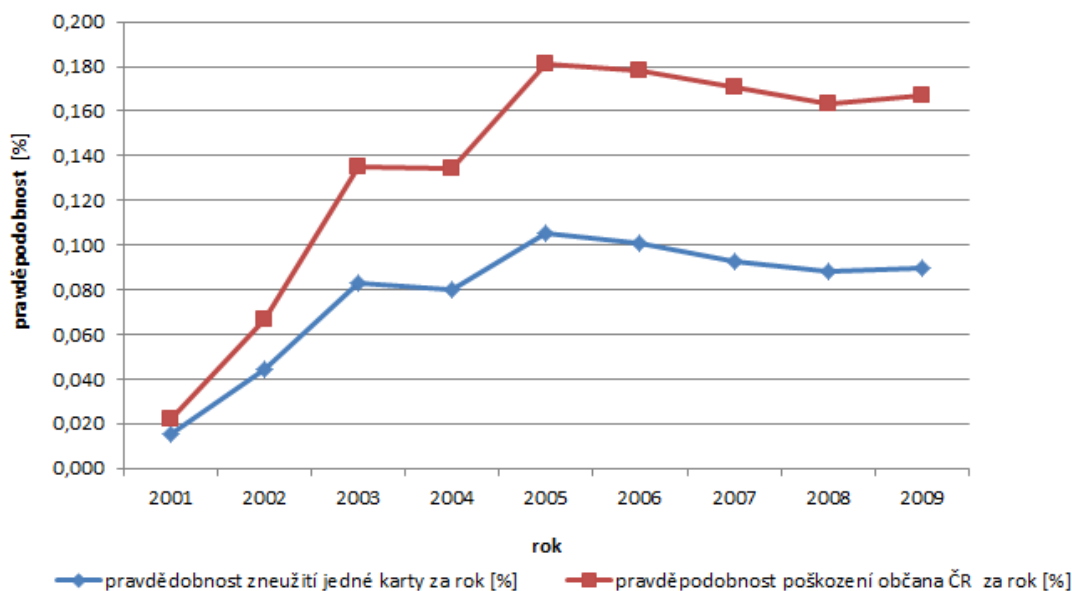
²³ Vytvořeno autorem práce ze statistických údajů uvedených v [34].

²⁴ Vytvořeno autorem práce ze statistických údajů uvedených v [34] a [31].

Tabulka (Tab. 6) znázorňuje pravděpodobnost poškození vlastníka karty. Vzhledem k tomu, že SBK neuvádí počet vlastníků karet, bude pravděpodobnost poškození trestným činem vztažena na 1 občana ČR staršího 15-ti let. Nepředpokládá se, že by osoby pod touto hranicí vlastnily platební karty. Údaje o počtu obyvatel této věkové skupiny byly získány ze statistik zveřejňovaných Českým statistickým úřadem (ČSÚ) [35]. Vývoj obou pravděpodobnosti vzniku události na kartu a občana ČR je znázorněn v grafu (Obr. 12). Do roku 2005 byl zaznamenán výrazný nárůst obou pravděpodobností.

Tab. 6. Pravděpodobnost poškození vlastníka karty²⁵

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	průměr
počet občanů ČR nad 15-let (vlastníků karet) [tis.]	10 224	10 201	10 202	10 207	10 234	10 267	10 323	10 430	10 491	10 287
počet případů za rok	688	2321	5310	5510	7739	7908	8023	7833	8113	5 938
pravděpodobnost poškození občana ČR za rok [%]	0,007	0,023	0,052	0,054	0,076	0,077	0,078	0,075	0,077	0,058
počet občanů na 1 případ za rok	14 860	4 395	1 921	1 852	1 322	1 298	1 287	1 332	1 293	3 285



Obr. 12. Vývoj pravděpodobnosti vzniku události na kartu a občana ČR²⁵

²⁵ Vytvořeno autorem práce ze statistických údajů uvedených v [31], [34] a [35].

Z poskytnutých údajů SBK a údajů zveřejňovaných na Internetu [31] byla stanovena pravděpodobnost napadení karet skimming, tedy pravděpodobnost napadení 1 karty za rok a počet karet připadajících na 1 případ za rok viz tabulka (Tab. 7). Je zřejmé, že pravděpodobnost ve vztahu k jedné kartě je velmi malá až zanedbatelná, za sledované období v průměru 0,000726 %.

Tab. 7. Pravděpodobnost napadení karet skimming²⁶

rok	2006	2007	2008	2009	2010	průměr
celkový počet všech vydaných karet [tis]	7 865	8 623	8 931	9 054	9 268	8 748
počet případů skimming	20	94	53	70	85	64
pravděpodobnost napadení 1 karty skimming za rok [%]	0,000254	0,001090	0,000593	0,000773	0,000917	0,000726
počet karet na 1 případ za rok	393 250	91 734	168 509	129 343	109 035	178 374

4.2 Stanovení následků

Pro účely hodnocení rizika zneužití platební karty byly jako následky stanoveny škody, které vnikly či hrozí poškozeným osobám neoprávněným odčerpáním finančních prostředků z jejich účtů za pomoci neoprávněně držené karty (svěřené, ztracené či odcizené), popřípadě padělané s oskimmovanými identifikačními údaji. Pro stanovení následků byly použity údaje z již zjištěných případů ze sledovaného období. Škody vzniklé na jeden případ jsou uvedeny v tabulce (Tab. 8).

SBK uvedlo, že nedisponuje údaji o výši neoprávněně vybraných finančních prostředků z účtů vztahujících se k napadeným platebním kartám. Z tohoto důvodu a také vzhledem k nezískání těchto údajů od bank (viz kapitola 6.1), nemohla být provedena analýza následků skimming.

²⁶ Vytvořeno z údajů poskytnutých SBK a údajů zveřejněných na [33].

Tab. 8. Škody způsobené na jeden případ²⁷

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	průměr
škoda na jeden případ [Kč]	9 846	8 563	5 037	6 141	5 635	5 263	5 494	6 546	6 515	42 100	10 114

Stanovení sociálního dopadu na poškozené

Aby bylo možno posoudit sociální dopad zneužití platební karty na poškozenou osobu, byly opět použity údaje zveřejněné ČSÚ [35], tentokrát týkající se životní úrovně obyvatel ČR viz tabulka (Tab. 9).

Tab. 9. Životní úroveň obyvatelů ČR²⁸

rok	peněžní hrubé příjmy na 1 člena domácnosti [Kč/rok]	peněžní hrubé výdaje na 1 člena domácnosti [Kč/rok]	finanční rezerva na 1 člena domácnosti [Kč/rok]	finanční rezerva na 1 člena domácnosti [Kč/měsíc]
2001	105 776	99 897	5 879	490
2002	109 011	102 732	6 279	523
2003	114 760	108 023	6 737	561
2004	119 923	111 805	8 118	677
2005	127 294	117 784	9 510	793
2006	134 569	125 605	8 964	747
2007	144 743	139 134	5 609	467
2008	156 598	143 055	13 543	1 129
2009	160 675	146 895	13 780	1 148

Vzhledem k tomu, že k datu vypracování této diplomové práce ČSÚ na svých stránkách [35] nezveřejnil statistické údaje za rok 2010, nemohla být v této práci provedena analýza za tento rok.

Pro výpočet sociálního dopadu na poškozené byl autorem diplomové práce použit následující vzorec:

$$t_{dopadu} = \frac{\dot{s}_{1p}}{fin_{1den}} \quad [\text{dny}]^{29}$$

²⁷ Vytvořeno autorem práce ze statistických údajů uvedených v [34].

²⁸ Vytvořeno autorem práce ze statistických údajů uvedených v [35].

²⁹ Vztah vytvořený autorem práce.

t_{dopadu} - délka sociálního dopadu na poškozené - viz tabulka (Tab. 10),

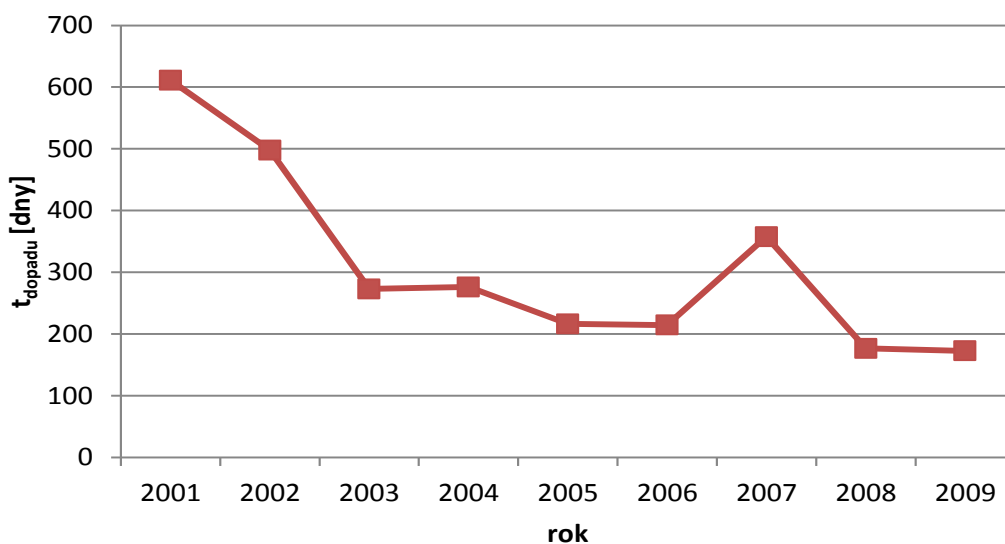
$\dot{\mathit{s}}_{1p}$ - škoda na 1 případ – viz tabulka (Tab. 8),

$\mathit{fin}_{1\text{den}}$ - finanční rezerva osoby na 1 den - přepočtem z údajů v tabulce (Tab. 9).

V případě, že poškozený nemá vytvořenou finanční rezervu, t_{dopadu} by se ještě prodloužila hrazením úroků z případného úvěru určeného k pokrytí vzniklé škody. Z tabulky (Tab. 9) je zřejmé, že sociální dopad na poškozené je poměrně vysoký. Doba sociálního dopadu je v průměru více než 10 měsíců a pro mnohé může znamenat existenční problémy. Vývoj následků nežádoucích událostí v podobě délky sociálního dopadu na poškozené znázorňuje graf (Obr. 13). Délka sociálního dopadu výrazně klesala do roku 2003, následně klesala mírně, kromě roku 2007, kdy byl zaznamenán její nárůst.

Tab. 10. Délka sociálního dopadu poškozených³⁰

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	průměr
t_{dopadu} [dny]	611	498	273	276	216	214	358	176	173	311



Obr. 13. Vývoj následků v podobě sociálního dopadu na poškozené³⁰

³⁰ Vytvořeno autorem práce ze vzorce a údajů uvedených v [34] a [35].

4.3 Kvantifikace aktiv

Aby bylo možné provést analýzu rizika nikoli jen v teoretické rovině, ale také číselnými hodnotami, které mají lepší vypovídající schopnost o riziku, je žádoucí provést kvantifikaci. Aktiva představují chráněné zájmy. Jejich kvantifikace vyjadřuje číselné vyjádření závažnosti hrozícího nebezpečí (zneužití platební karty) ve finanční podobě na poškozené jednotlivce. Hranice jednotlivých škod byly stanoveny autorem této práce, přičemž bylo vycházeno z životní úrovně obyvatel ČR uvedené v tabulce (Tab. 9). Kvantifikace aktiv je uvedena v tabulce (Tab. 11).

Tab. 11. Kvantifikace aktiv³¹

stupeň	výše dopadu	popis dopadu	výše škody na 1 případ		procentní body	
			od	do	od	do
1	nízká	malé škody	x	5 000,00 Kč	0	25
2	střední	vážné škody	5 000,00 Kč	100 000,00 Kč	25	50
3	vysoká	velmi vážné škody	100 000,00 Kč	500 000,00 Kč	50	75
4	kritická	škody likvidační	500 000,00 Kč	x	75	100

4.4 Kvantifikace hrozeb

Hrozby budou kvantifikovány na základě zjištěné pravděpodobnosti jejich výskytu dle tabulky (Tab. 12).

Tab. 12. Kvantifikace hrozeb³¹

stupeň	úroveň hrozby	pravděpodobnost	hodnota	
			od	do
1	nízká	nepravděpodobná	0	0,25
2	střední	pravděpodobná	0,25	0,5
3	vysoká	vysoce pravděpodobná	0,5	0,75
4	jistá	jistá	0,75	1

³¹ Použito a upraveno z [8].

- stupeň č. 1 – výskyt hrozby je velice ojedinělý,
 stupeň č. 2 – hrozba se vyskytuje často,
 stupeň č. 3 – výskyt poměrně častý,
 stupeň č. 4 – hrozba se vyskytuje i několikrát ročně.

4.5 Kvantifikace zranitelnosti

Míra zranitelnosti určuje, jak je aktivum odolné vůči působení dané hrozby. Při stanovení míry zranitelnosti se bere v úvahu prostředí a stávající protiopatření, která mohou snižovat úroveň zranitelnosti [8]. Při kvantifikaci zranitelnosti bude vycházeno z tabulky (Tab. 13).

Tab. 13. Kvantifikace zranitelnosti³²

stupeň	zranitelnost	opatření	procentní body	
			od	do
1	nízká	opatření jsou zavedena, dokumentována, kontrolována a zlepšována	0	0,25
2	střední	opatření jsou zavedena, dokumentována a kontrolována	0,25	0,5
3	vyšší	opatření jsou zavedena a dokumentována	0,5	0,75
4	kritická	žádná opatření nejsou zavedena, dokumentována, kontrolována a zlepšována	0,75	1

4.6 Hodnocení rizika

Výše rizika vypočítáme podle následujícího vzorce:

$$R = A \times H \times Z^{32}$$

- R** - riziko, nabývá hodnot <0,100>,
A - aktivum, nabývá hodnot <0,100>,
H - hrozba, nabývá hodnot <0,1>,
Z - zranitelnost, nabývá hodnot <0,1>.

³² Použito a upraveno z [8].

Výpočet (stanovení) číselných hodnot:

- A** - při určení výše procentních bodů aktiv vycházíme z tabulky (Tab. 9), u průměrné škody na jeden případ vypočítáme:

$$A = \frac{10114 \times (3 - 0,3)}{100000 - 5000} \times 100 = \mathbf{28,75}$$

- H** - jelikož případy se vyskytují několikrát ročně, je podle tabulky (Tab. 12) stanovena maximální hodnota **H = 1**.
- Z** - vzhledem k tomu, že banky a provozovatelé ATM na zjištěné případy reagují různými opatřeními, která zlepšují, je dle 1. řádku tabulky (Tab. 13) stanovena střední hodnota z intervalu, tedy **Z = 0,12**.

Výše uvedeným postupem bylo stanoveno číselné vyjádření rizika, které bylo hodnoceno podle tabulky (Tab. 14). Přehled takto stanoveného rizika je uveden v tabulce (Tab. 15) a jeho grafické znázornění v grafu (Obr. 14).

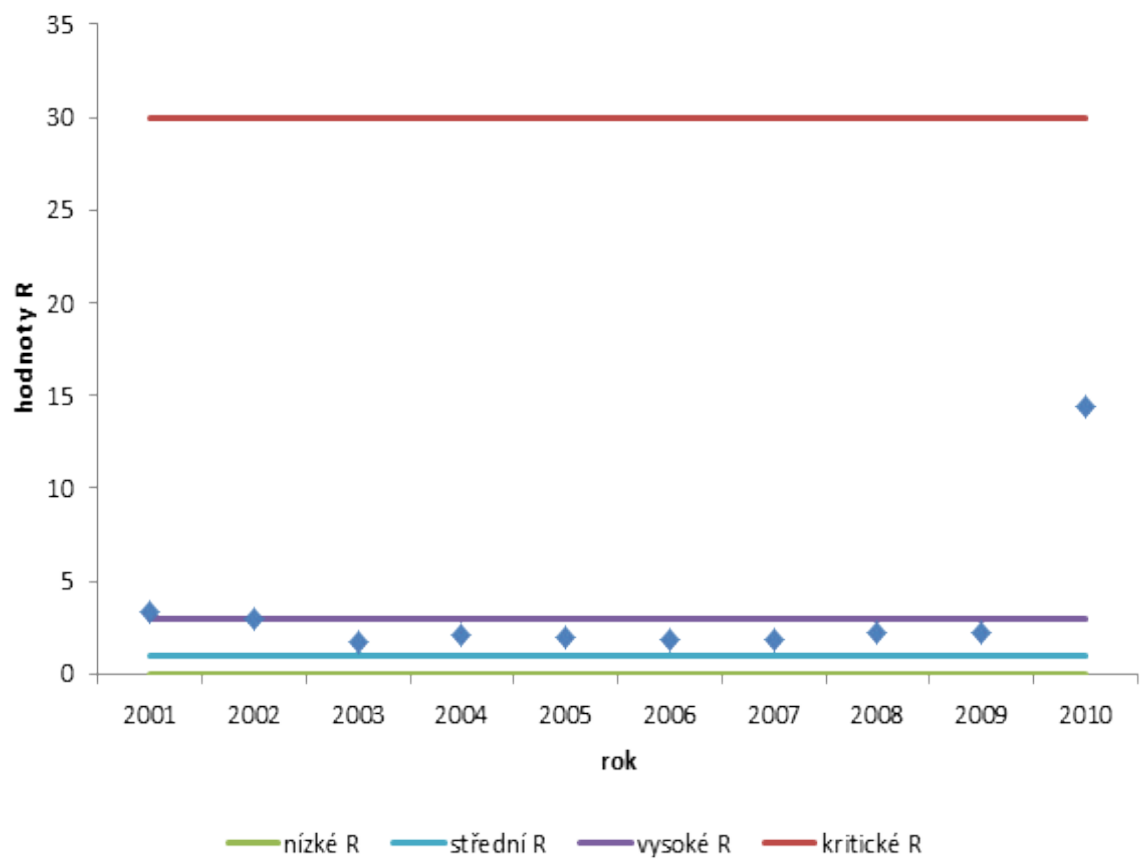
Tab. 14. Hodnocení rizika³³

stupeň	výše rizika	zkratka	popis rizika	hodnota	
				od	do
1	nízká	N	riziko je akceptovatelné, postačí monitoring	0	1
2	střední	S	riziko musí být zvládáno podle plánu	1	3
3	vysoká	V	riziko musí být zvládáno podle plánu	3	30
4	kritická	K	riziko musí být ihned zvládáno	30	100

³³ Použito z [8].

Tab. 15. Přehled hodnoceného rizika³⁴

rok	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	průměr
škoda na 1 případ [Kč]	9 846	8 563	5 037	6 141	5 635	5 263	5 494	6 546	6 515	42 100	10 114
A	27,98	24,34	14,32	17,45	16,02	14,96	15,61	18,60	18,52	119,65	28,75
R	3,36	2,92	1,72	2,09	1,92	1,79	1,87	2,23	2,22	14,36	3,45
stupeň rizika	3	2	2	2	2	2	2	2	2	3	3
výše rizika	V	S	S	S	S	S	S	S	S	V	V

Obr. 14. Grafické znázornění stanoveného rizika³⁵

³⁴ Hodnoty škod na 1 případ použity z tabulky č. 8, hodnota A vypočítána podle tabulky č. 11, hodnota R, stupeň rizika a jeho výše stanovená podle tabulky č. 14.

³⁵ Vytvořeno z údajů uvedených v tabulce č. 15.

Zvolenou metodou analýzou rizika bylo zjištěno, že riziko zneužití platební karty se v období let 2002-2009 pohybovalo v pásmu středního rizika. Hranice směrem do oblasti vysokého rizika byla překonána v letech 2001 a 2010. V roce 2010 dosáhlo riziko největší míry. Je velice obtížně identifikovat, co způsobilo tento výrazný nárůst. Počet případů se přitom oproti předchozím letům nezvýšil, z čehož lze jen usoudit, že pachatelé na stejný počet případů odčerpali z účtů poškozených větší částky. Je pravděpodobné, že zvýšení předmětného rizika může být i následkem rozvíjející se ekonomické krize. Bylo by žádoucí sledovat další vývoj uvedené trestné činnosti v dalších letech, proces analýzy rizika opakovat a na základě analytického zjištění zvážit přijetí dalších opatření ke snížení míry rizika. Na druhou stranu ve sledovaném období nebylo ani zdaleka dosaženo kritických hodnot rizika a postačí tedy riziko zvládat podle plánu. Každopádně míra rizika se dá podstatně snížit např. pojištěním platební karty proti jejímu zneužití. Následky se poté přenesou na bankovní, finanční či pojišťovací subjekty, pro které vzhledem k nemalým ziskům budou zanedbatelné. Z výzkumu provedeného v kapitole 6.3 je zřejmé, že možnost pojištění proti zneužití karty využívá jen 11 % respondentů.

5 ANALÝZA PROBLÉMŮ S USVĚDČOVÁNÍM PACHATELŮ TRESTNÉ ČINNOSTI

5.1 Podvody páchané oprávněným držitelem platební karty

Přečerpání povoleného limitu

U některých takových případů se nejedná o trestný čin, ale o občansko-právní spor, k jehož projednání je místně příslušný soud v občanskoprávním řízení. Trestný čin podvod podle § 209 trestního zákoníku [14] je totiž trestný čin úmyslný, jehož obligatorním znakem je zavinění. Je nutné prokázat, že pachatel již v době uzavření smlouvy s bankou či subjektem z nebankovního sektoru jednal s úmyslem úvěr nesplácet. Pokud u takové smlouvy uvede nepravdivé údaje rozhodné pro poskytnutí úvěru, vzniká v takovém případě podezření ze spáchání trestného činu úvěrového podvodu podle § 211 trestního zákoníku [14].

Fiktivní krádež

Skutečnost, že platební kartu po nahlášení její ztráty či odcizení nadále používá její oprávněný držitel je prokazatelná například vyžádaným záznamem snímacího zařízení u ATM. Vzhledem k problému, který bude podrobněji popsán v kapitole 6.4, může být záznam z kamery neprůkazný, popřípadě být jen důkazem nepřímým. Dalším důkazem může být zjištění výskytu věcí, které byly pořízeny platbou údajně odcizené karty a samozřejmě nejlépe zajištění karty samotné přímo u pachatele, v jeho bytě či zaměstnání. Zajištěním je v tomto případě myšleno využití všech zákonně dostupných oprávnění orgánů činných v trestním řízení (např. vydání a odnětí věci, osobní prohlídka, domovní prohlídka, prohlídka jiných prostor a pozemků atd.).

5.2 Podvody spáchané neoprávněným držitelem platební karty

Odcizená identita

Pokud je platební karta vydána neexistujícím fiktivním subjektům, dopadení pachatele je velmi obtížné. K objasnění těchto případů napomáhá fakt, že pachatelé většinou v trestné činnosti pokračují. Při zneužití osobních dokladů je pro majitele odcizených (ztracených) dokladů obtížné a problematické dokazování odcizené identity.

K prevenci proti této trestné činnosti přispívá zákon [16], dle kterého u každého zájemce o vydání platební karty, který dosud nevyužívá jiný produkt banky, musí být osobně ověřena jeho totožnost, a to buď při podání žádosti o platební kartu, nebo při jejím převzetí.

Další formy trestné činnosti neoprávněným držitelem platební karty

Při usvědčování pachatelů dalších forem trestné činnosti, která je popisována v kapitolách 2.2, 2.3 a 2.4, mohou nastat problémy identifikované a popsané v kapitole 6.4. Orgány činné v trestním řízení jsou však povinny vyhledávat všechny důkazy svědčící ve prospěch i neprospěch pachatele. V případě, že záznam z kamer instalovaných v ATM je z důkazního hlediska nepoužitelný, snahou policistů pověřených k vyšetřování trestných činů a také státních zástupců je najít další důkazní prostředky. Tyto však nemohou být v práci popsány z důvodu zachování jejich mlčenlivosti stanovené zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti [17] a také z taktických důvodů.

6 VYHODNOCENÍ DOTAZNÍKŮ

6.1 Vyhodnocení dotazníků adresovaných bankám

Původní záměr autora diplomové práce bylo také provedení analýzy rizika skimming. K této analýze je však nutné získat statistické údaje o počtu zjištěných případů skimming a také celkové částky neoprávněně vybrané z účtů majitelů oskimmovaných karet. Za tímto účelem byly v období od 22.2.2011 do 26.2.2011 bankovním subjektům uvedených v příloze *P IV* rozeslány žádosti o zodpovězení níže uvedených otázek:

- **Kolik případů v období od r. 2001 do roku 2010 vaše společnost zaznamenala v souvislosti s nelegálním zkopírováním magnetických kódů platebních karet (skimming), s rozlišením za jednotlivé roky?**
- **Jaká částka byla z důvodů uvedených v předchozím bodě neoprávněně odčerpána vašim klientům v jednotlivých letech?**
- **Jaké jste přijali opatření ke snížení rizika „skimming“?**

Takto bylo obesláno 16 vydavatelů platebních karet z bankovního sektoru. 7 bank uvedlo, že požadované informace nemohou sdělit, neboť je považují za interní, 6 bank neodpovědělo vůbec, Českomoravská záruční a rozvojová banka, a.s. se vyjádřila, že nevydává platební karty. PPF banka, a.s. vydává karty od září roku 2010 a dosud nezaznamenala žádný případ skimming. Československá obchodní banka, a.s. poskytla pouze obecné statistické údaje, které však podmínila tím, že nebudou součástí diplomové práce v písemné podobě a mohou být použity výhradně při ústní obhajobě. Vzhledem k neúplnosti těchto údajů, nemožnosti jejich analýzy a zveřejnění, bylo od tohoto postupu upuštěno.

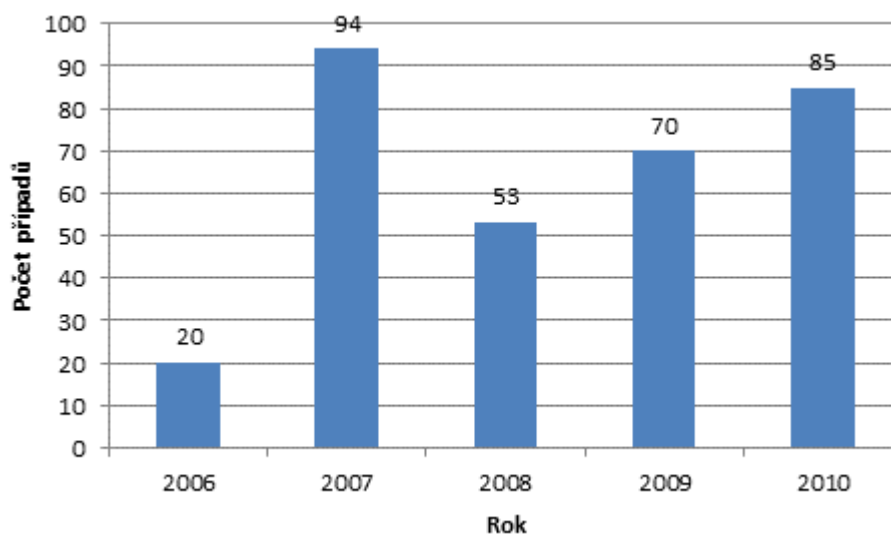
6.2 Vyhodnocení dotazníků adresovaných dalším subjektům

Dotazníky zmiňované v předchozí kapitole byly v období od 14.2.2011 do 27.2.2011 rozeslány také vydavatelům karet z nebankovního sektoru. Seznam oslovených subjektů je uveden rovněž v příloze *P IV*.

Sdružení pro bankovní karty (SBK) byla zaslána žádost o sdělení k následujícím otázkám:

- Kolik případů v období od r. 2000 do současné doby bylo zaznamenáno, pokud možno s rozlišením za jednotlivé roky a banky?
- Jaká částka byla takto neoprávněně odčerpána klientům bank?
- V případě, že disponujete také uvedenými údaji ve vztahu k pobočkám zahraničních bank, prosím, sdělte také tyto údaje k nim.

SBK poskytla pouze údaje o zjištěném počtu skimming všech platebních karet na území ČR za období let 2006-2010. Zjištěné údaje byly použity pro stanovení pravděpodobnosti v kapitole 4.1. Graf (Obr. 15) znázorňuje vývoj počtu případů skimming. Je zřejmé, že nejvíce uvedených případů bylo v roce 2007 a poté v roce 2010. SBK nesdělila údaje o výši neoprávněně vybraných finančních prostředků z účtů následkem skimming, neboť těmito dle svého sdělení nedisponuje. Proto nemohlo být provedeno stanovení následků skimming a hodnocení tohoto nebezpečí.



Obr. 15. Vývoj počtu případů skimming v ČR³⁶

Z 5-ti oslovených vydavatelů platebních karet z nebankovního sektoru 4 neodpověděli. Společnost Home Credit uvedla odkaz na tiskové zprávy zveřejněné na internetových stránkách [37] a [38]. V těchto se uvádí, že lidé si své kreditní karty

³⁶ Vytvořeno z údajů poskytnutých SBK.

nechrání, nosí PIN napsaný na kartě v peněžence, kartu nechávají bez dozoru nebo s ní platí na rizikových serverech. Společnost Home Credit v roce 2009 odhalila 28 případů zneužití a v roce 2010 39 případů. V roce 2009 činila celková hodnota neoprávněně vybraných finančních prostředků cca. 165 tis Kč a v r. 2010 téměř 300 tisíc korun. Nejčastěji kreditní karty neoprávněně použil někdo z rodiny.

Zjištěné případy skimming u spol. Home Credit, a.s.:

r. 2009 – 1 případ. Ke zkopírování magnetického proužku karty došlo v Praze poblíž Václavského náměstí, kde bylo na ATM umístěno skimmovací zařízení. Podvodníci pak s padělanou kartou vybrali z ATM v Bulharsku téměř 10 tisíc korun.

r. 2010 – 2 případy. Podvodníci byli úspěšní pouze u jednoho z těchto případů. Klient svou kartu ponechal jako zástavu v hotelu, kde někdo neoprávněně zkopíroval její magnetický kód. Padělkem karty poté bylo zapláceno ve Spojených státech amerických.

Preventivní opatření proti skimming u spol. Home Credit, a.s.:

Spol. Home Credit sleduje podezřelé transakce speciálním programem Fraud monitoring. Ten zabránil zneužití platební karty u druhého případu v r. 2010. Karta byla okopírovaná v pražském ATM, o pár hodin později se pachatel pokusil vybrat peníze v Austrálii, avšak bezvýsledně. Díky uvedenému systému, který vyhodnotil uvedené transakce na velkou vzdálenost za krátký čas jako podezřelé, došlo k zablokování karty, ačkoli se majitelku karty v té době nepodařilo telefonicky kontaktovat. O pár měsíců později policie dostihla muže, u kterého našla velké množství čísel kreditních karet, mezi nimiž byla také karta klientky Home Credit, a.s.

Program Fraud monitoring preventivně sleduje veškeré platby, které mohou být rizikové. Jde například o internetové sázení, casina nebo některé zahraniční transakce. V roce 2010 Home Credit, a.s. získala přes 26 tisíc upozornění na podezřelou transakci.

6.3 Vyhodnocení dotazníků adresovaných uživatelům karet

Za účelem zjištění informovanosti veřejnosti o rizicích spojených s používáním platebních karet byl v období měsíce března r. 2011 proveden výzkum formou náhodně oslovených respondentů v rámci území města Ostravy. Bylo osloveno 80 osob, kterým

byly pokládány otázky dle dotazníku uvedeného v příloze *P IV*. Bylo vybráno 20 zástupců z každé věkové skupiny:

skupina A): 15-45 let,

skupina B): 26-40 let,

skupina C): 41-60 let,

skupina D): nad 60 let.

Dotazníky byly na položené otázky zjištěny následující odpovědi:

- **Vlastníte jakoukoli platební kartu?** 89 % kladných odpovědí.
- **Je použití Vaší karty podmíněné zadáváním bezpečnostního PIN kódu?** 96 % kladných odpovědí.
- **Kde máte uložen PIN Kód?** 43% dotazovaných má PIN kód uložen pouze ve své paměti, 6 % jej má poznačen na platební kartě či jejím obalu, 24 % v mobilním telefonu bez šifrování (v seznamu kontaktů uloženo pod názvem PIN), 6 % v mobilním telefonu s šifrováním (např. prohozená čísla v seznamu uložená pod jiným názvem) a zbývajících 21 % má PIN kód uložen na jiném místě (např. v poznámkových blocích či na různých v papírcích v peněžence).
- **Došlo někdy ke ztrátě či odcizení Vaší karty?** Zkušenost se ztrátou či odcizením má 7,5 % respondentů (6 dotazovaných).
- **Byla Vaše ztracená či odcizená karta zneužita?** Zjištěno u 2,5 % respondentů (2 dotazovaní).
- **Jaká částka vám byla neoprávněně odčerpána z účtu?** V prvním případě došlo k pokusu o výběr finančních prostředků z ATM (k výběru nedošlo z důvodu neznalosti PIN kódu. U druhého došlo k neoprávněné platbě na benzínové čerpací stanici v hodnotě 1.500,- Kč. K dalšímu zneužití karty již nedošlo z důvodu provedení blokace jejím uživatelem.
- **Pokud došlo k neoprávněnému použití platební karty, uveďte, proč se tak stalo?** V obou případech z důvodu pozdní blokace karty.
- **Víte, co je to skimming?** 17,5% kladných odpovědí.
- **Došlo někdy k neoprávněnému výběru z Vašeho účtu bez ztráty či odcizení**

platební karty, tedy následkem skimming? Tuto zkušenost neměl nikdo z dotazovaných.

- **Víte, jak „skimmovací“ zařízení vypadá a jak jej rozpoznat?** 10 % dotazovaných uvedlo, že ano. O instalaci skimmovacích zařízení a možných způsobů provedení se dozvěděli převážně z internetu nebo z televize.
- **Zjistili jste někdy výskyt „skimmovacího“ zařízení na bankomatu?** 0 % kladných odpovědí.
- **Znáte desatero bezpečného používání bankomatu a bezpečné platby kartou u obchodníků, které vydává Sdružení bankovních karet?** 3 respondenti (3,75 %) uvedli, že toto desatero znají z internetových stránek SBK. 10 respondentů (12,5 %) uvedlo, že neznají přímo uvedené desatero, ale z klientských dokumentů své banky nebo z jiných médií mají obecné informace o bezpečném používání platebních karet.
- **Jakou formu platby preferujete u obchodníků?** 52,5 % respondentů odpovědělo, že upřednostňuje platbu platební kartou.
- **Kde většinou nakupujete?** 67,5 % uvedlo, že v kamenných obchodech, zbývajících 22,5 % na internetu, převážně elektroniku, drogistické a kosmetické přípravky.
- **Jakou formu platby preferujete na internetu?** Z 18-ti respondentů, kteří kladně odpověděli na předchozí otázku, 2 uvedli platbu platební kartou, 11 platbu bankovním převodem na základě příkazu k převodu přes Internetbanking a zbývajících 5 uvedlo platbu v hotovosti při převzetí zboží zaslaného na dobírku.
- **Máte ke kartě sjednáno pojištění proti jejímu zneužití?** Z 89 dotazovaných vlastníků karet má kartu pojištěno proti zneužití pouhých 11 % a 27 % o tom uvažuje.
- **Je podle Vás používání platebních karet v ČR bezpečné?** 72,5 % kladných odpovědí.

6.4 Vyhodnocení dotazníků směřovaných útvarům Policie ČR

V rámci plnění služebních povinností u Policie ČR se autor diplomové práce setkal s problémy s usvědčováním pachatelů trestné činnosti v souvislosti se zneužitím platebních karet. Ty potom mají za následek poměrně nízké procento objasnění trestné činnosti uvedené v tabulce (Tab. 2). Byly zjištěny níže uvedené nedostatky bankovních institucí provozujících ATM.

1. Nesoulad času záznamu pořízeného ze snímací kamery ATM a času provedené transakce.
2. Malé rozlišení kamerového snímacího zařízení ATM a nevhodný úhel snímání obličeje osob u ATM.

Za účelem ověření existence uvedených nedostatků byl proveden výzkum v rámci základních útvarů Policie ČR, Krajské ředitelství policie moravskoslezského kraje, Městské ředitelství policie Ostrava (KŘP MSK, MŘP Ostrava). Po schválení ředitelem MŘP Ostrava byly vedoucím pracovníkům 18-ti útvarů uvedených v příloze P VI doručeny dotazníky uvedené v téže příloze. Rozeslání dotazníků nebylo rozšířeno na útvary v rámci služební působnosti jiných měst či krajů, neboť v současné napjaté atmosféře u Policie ČR způsobené neutěšenou ekonomickou situací by nebyla zaručena ochota spolupráce jiných útvarů podílet se na tomto výzkumu. V rámci Moravskoslezského kraje, tedy i v Ostravě byl zjištěn vysoký počet zájmové trestné činnosti. Proto bylo vyhodnoceno, že výzkum v rámci Ostravy je dostačující.

Dotazovaných 18 útvarů odpovědělo následovně:

- **Zjistili pracovníci vašeho útvaru PČR v rámci šetření či prověřování uvedené trestné činnosti nedostatek ad 1)?** 12 kladných odpovědí (67 %).
- **Jak velký časový rozdíl byl zjištěn mezi časem z výběru bankomatu a časem záznamu ze snímací kamery?**

Z 12-ti útvarů, které se setkaly s tímto problémem, uvedly:

- 2 útvary (17 %) časový rozdíl < 30 s,
- 1 útvar (8 %) časový rozdíl 30 až 60 s,
- 9 útvarů (75 %) časový rozdíl > 60 s.

- **Zjistili pracovníci vašeho útvaru PČR v rámci šetření či prověřování uvedené trestné činnosti nedostatek ad 2)?** 17 kladných odpovědí (94 %).
- **V kolika případech za období od 1.1.2009 jste zaznamenali uvedené nedostatky?**

1 útvary (5,5 %) uvedl, že se nesetkal s žádným z uvedených problémů,
7 útvary (39 %) v uvedeném období zaznamenalo < 10 případů,
10 útvary (55,5 %) v uvedeném období uvedlo > 10 případů.
- **Měly uvedené nedostatky následek neprokázání trestné činnosti vytipované osobě pachatele?** 12 kladných odpovědí (67 %).
- **Byl pracovníky vaší součástí Policie ČR dán podnět bankovním institucím k odstranění zjištěných nedostatků?** 4 kladné odpovědi (22 %).

7 NAVRHOVANÁ OPATŘENÍ KE ZVÝŠENÍ BEZPEČNOSTI POUŽÍVÁNÍ PLATEBNÍCH KARET

Z dostupných informací bylo zjištěno, že vydavatelé platebních karet a provozovatelé ATM bezpečnost svých klientů nepodceňují a průběžně reagují na zjištěné případy trestné činnosti v souvislosti se zneužíváním platebních karet. Kromě různých organizačních opatření, používají řadu bezpečnostních technických prostředků a zdokonalují používaný software. V neposlední řadě informují veřejnost o možnostech preventivní ochrany proti zneužití platebních karet. Například SBK na stránkách [32] vydává desatero pro držitele platebních karet a pro obchodníky, popisuje jednotlivé druhy podvodů, včetně způsobů jejich odhalení a prevence.

Společnost Wincor Nixdorf AG již v roce 2003 předvedla své první anti-skimmingové zařízení. V lednu 2010 v Paderborn v Německu představila vylepšený modul Anti-Skimming II, který detekuje skimmingové zařízení, spouští tichý poplach a současně zahajuje další akce, např. monitorování okolí videokamerou. Současně také vysílá silné interferující magnetické pole zabráňující přečtení údajů z karty. Výhodou je, že po zabránění skimmingového útoku může činnost ATM pokračovat. Jedním z preventivních opatření je také použití analytického software Optical Security Guard. Detekuje změny provedené na operačním panelu bankomatu. Je využíván u systémů CINEO a bankomatů série Procash 8000 [26].

Dalším opatřením je zavedení protokolu 3-D Secure (Three Domain Secure), který je dílem společnosti VISA. Vytvoření tohoto protokolu bylo z důvodu zvýšení bezpečnosti online platebních transakcí. U platebních karet asociace VISA je implementace protokolu 3-D Secure nabízena jako služba s názvem Verified by Visa. Verzi tohoto protokolu později aplikovala i asociace MasterCard a implementovala jej pod názvem MasterCard SecureCode. Tímto protokolem byla přenesena odpovědnost za podvodné transakce ze společností vydávající platební karty na společnosti, které tuto technologii neimplementovaly.

I přes veškerá opatření, které vydavatelé platebních karet a provozovatelé ATM činí, jsou navrhována opatření uvedená v následujících podkapitolách.

7.1 Návrh preventivních opatření

Jako preventivní opatření proti zneužití platební karty neoprávněnou osobou je navrženo zavedení biometrické identifikace u ATM a POS terminálů.

7.1.1 Zavedení biometrické identifikace

Biometrie – obor, který využívá matematické statistiky pro zkoumání proměnlivosti živých organismů. Automaticky jsou vyhodnocovány neměnné fyziologické a behaviorální lidské charakteristiky [25].

Měřitelnými vlastnostmi jsou:

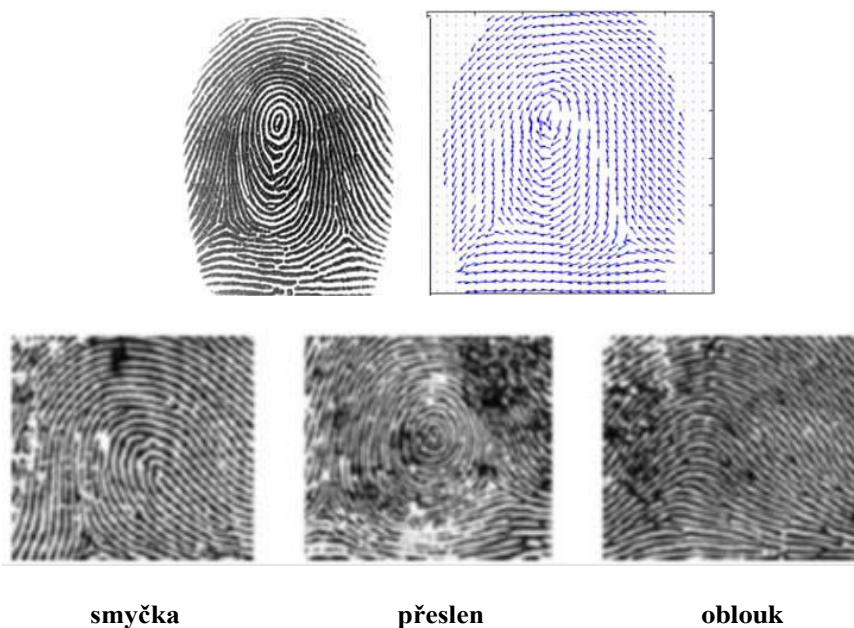
- fyziologické – otisk prstu, geometrie ruky, rozpoznání obličeje, oční duhovka a oční sítnice,
- behaviorální – ověřování hlasu, dynamika podpisu a dynamika stisku kláves.

Biometrika zahrnuje 2 základní systémy, kterými jsou verifikace a identifikace. Verifikační systém zajišťuje identitu člověka porovnáním biometrických dat s šablonou, která je uložena v databázi. Identifikační systém rozpoznává osobu s šablonami všech uživatelů uložených v databázi za účelem zjištění, které osobě patří biometrická data [25].

Biometrické metody jsou již ve světě běžně používány, například při vstupu do chráněných objektů. Metody založené na otisku prstu pronikly i do oblastí spotřební elektroniky, jsou součástí např. notebooků k přístupu k datům oprávněným uživatelům.

Pro zvýšení úrovně autentizace oprávněného uživatele platební karty je autorem diplomové práce navrhováno zavést u ATM a POS terminálů biometrické senzory na otisky prstů, které mohou určit, zda použitý prst je reálný a živý. Digitální identifikační kód by pak mohl být uložen v čipu u platební karty. Mikropočítač ATM či POS terminálu by údaje získané z biometrického čidla porovnal s identifikačním kódem na čipu. V případě ověření autentizace oprávněného držitele by bylo umožněno provést platební transakci. Oproti jiným typům biometrických technologií, které vyžadují speciální přípravky, odstranění brýlí, správné fyzické umístění nebo speciální podmínky prostředí, pro identifikaci otisků prstů potřebujeme pouze jednoduchý dotyk prstu. Z tohoto důvodu je navrhována tato metoda, která je pro identifikaci oprávněného držitele platební karty považována za dostačující.

Prsty, ale i dlaně obsahují papilární linie (vyvýšeniny a prohlubně), které se vytváří během prvních sedmi měsíců života. Jedná se o jednoznačnou identitu jedince, neboť různé otisky mají i jednovaječná dvojčata. Na obrázku (*Obr. 16*) je uveden vzorek otisku prstu s detailem papilárních linií a jejich druhů.



Obr. 16. Vzorek otisku prstu s detailem papilárních linií³⁷

Autentizace otisku prstů

K rozpoznání otisků prstů jsou využívány snímače, které se vyznačují svou poměrně vysokou přesností a malými finančními pořizovacími náklady. Technologií je několik, za základní lze považovat snímače optické, kapacitní, ultrazvukové a teplotní.

Optické snímače:

- přiložený prst je osvětlován laserovým světlem,
- analyzuje se rozptyl nebo odraz světla v místech dotyku papilárních linií se snímací plochou (rozptyl světelného paprsku v rýhách, odraz od papilárních linií),

³⁷ Použito z [25].

- nevýhoda větší rozměry a nutnost čistoty přikládaného prstu.

Kapacitní (silikonové) snímače:

- měření nepatrných změn elektrického náboje na povrchu prstu (kapacitní odpor),
- desky kondenzátoru jsou tvořeny přiloženým prstem a podložkou snímače,
- obraz se vytváří ze zachycených hodnot kapacitních odporů (papilární linie mají větší kapacitní odpor),
- oproti optickým snímačům je výhodou, že mají menší rozměr a přikládaný prst může být mírně znečištěný.

Ultrazvukové snímače:

- jedná se o patentovanou technologii ve vlastnictví americké společnosti Ultrascan,
- detekují se změny ultrazvukových vln, které jsou vysílány k přiloženému prstu,
- nevýhodou jsou větší rozměry, které jsou však kompenzovány vysokou přesností i při znečištěném prstu, např. mastnotou, nikotinem, pleťovou vodou nebo inkoustem novinového papíru.

Teplotní snímače:

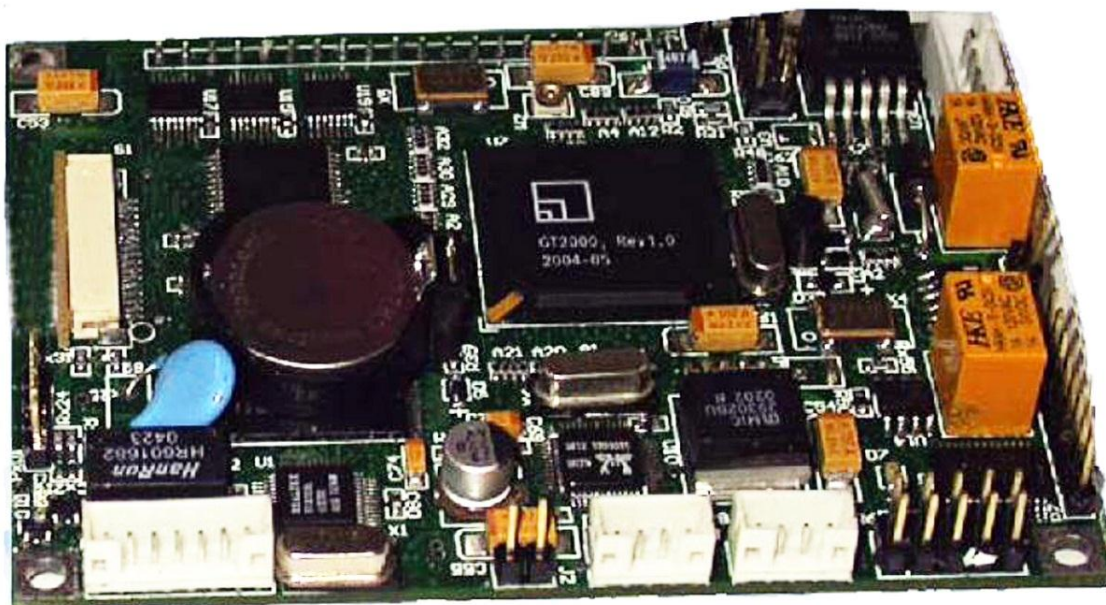
- snímač je tvořen mikročipem, který pokrývá teplotně citlivá vrstva sestavená ze 14000 zobrazovacích prvků,
- čip zaznamenané nepatrné teplotní rozdíly konvertuje na 50-100 obrazových řezů zobrazující papilární linie prstu,
- speciální software asi za desetinu sekundy složí řezy do celkového snímku.

Z výše uvedených hledisek, zejména z důvodu spolehlivosti, přesnosti a schopnosti efektivního čtení různorodých otisků prstů je navrhováno použití ultrazvukového snímače do ATM a POS terminálů. Pro uvedený účel byl nalezen jako optimální produkt ZEM200 EDK (ultrazvukový snímač otisku prstu) od firem ZK Software a US Digitalpersona, distribuovaný firmou COMFIS s.r.o., Buchlovice [41].

Ultrazvukový snímač otisku prstu ZEM200 EDK

EDK je multifunkční platforma ve formě základní desky pro vývoj vestavěných samostatných Linuxových produktů využívající otisky prstů. Vyhovuje požadavkům na většinu vestavěných produktů s otiskem prstů. Obsahuje různé komunikační rozhraní,

např. TCP/IP, USB, RS232, RS485 a Wiegand. Do základní desky je implementován výkonný procesor RISC s vynikajícím, spolehlivým a vysokorychlostním algoritmem pro identifikaci otisků prstů a standardním Linux jádrem [41].



Obr. 17. ZEM200 EDK³⁸

Specifikace:

- senzor: U.are.U 4000, U.are.U firefly,
- výkon: menší než 2 W,
- napájecí napětí: DC5V,
- CPU: Vestavěný vysokorychlostní RISC CPU,
- SDRAM: 16MB,
- NOR FLASH: 16MB,
- RS232: 8 linkové RS232 + 3 linkové RS232,
- Ethernet: RJ45, LED indikace příjem/vysílání,
- USB: dva standardní USB 1.1 HOST,

³⁸ Použito z [41].

- Wiegand: Vstup/výstup standard 26 Bit/zákaznický formát,
- RS485: 4 linkové RS485,
- provozní teplota: 0 °C - 45 °C,
- provozní vlhkost: 20 % - 80 %,
- skladovací teplota: 0 °C - 50 °C,
- skladovací vlhkost: 10 % - 80 %,
- LCM: Standardní 128 x 64 LCD,
- zvuk: AC97 dekodér + zesilovač,
- rozměry: 90 (d) x 76 (š) mm.

Výhody:

- podpora funkcí odložení a spánku,
- čas spuštění: méně než 10 s,
- základní deska EDK je konstruována na nepřetržitý 24-hodinový provoz,
- zabezpečení proti zaseknutí při běhu programů,
- softwarové načasování vypínání a zapínání,
- podpora bezkontaktních zařízení na karty RFID,
- omezuje vývojové problémy a zrychluje harmonogram vývoje,
- výběr ze senzorů ZK nebo U.are.U,
- monitoring napájecího napětí a programovatelná funkce watchdog,
- plná demo verze zdrojového kódu ke zvýšení rychlosti vývoje.

Firma COMFIS uvádí jako jednu z možných aplikací právě bezpečnostní ověření u bankovních přepážek pro ATM a POS terminálů, avšak z veřejně dostupných informací nebyla zjištěna jejich realizace do praxe.

Vzhledem k tomu, že technologie ATM a POS terminálů podléhá zákonu o ochraně utajovaných informací [17] a také vzhledem k tomu, že návrh implementace biometrických snímačů do uvedených systémů by byl značně rozsáhlý, tato problematika není v práci řešena.

7.2 Návrh represivních opatření

Vzhledem ke zjištěným problémům popsaných v kapitole 6.4., byla autorem diplomové práce navržena následující opatření, která by přispěla k represii trestné činnosti v souvislosti se zneužitím platebních karet. Těmito opatřeními by jistě došlo ke zvýšení objasňenosti uvedené trestné činnosti, což by se po čase dostalo do povědomí pachatelů. Represe je totiž v přímé souvislosti s prevencí a navrhovaná opatření by napomohla také ke snížení případů zneužití platebních karet.

- Použití snímacích kamer u všech ATM.
- Synchronizace času kamerových kamer s časem platební transakce.
- Použití kamerových snímacích zařízení s lepším rozlišením.
- Snímání obličeje osob u ATM z více úhlů v kombinaci s kamerami umístěnými i v okolí ATM, aby bylo možno snímat také další spolupachatele, kteří nestojí bezprostředně u ATM.

Jelikož vnitřní struktura ATM včetně jednotlivých snímacích zařízení a bezpečnostních prvků podléhá utajení dle zákona [17] a nelze je zveřejnit, byla uvedená opatření navržena pouze v obecné rovině. Nicméně by mohla být podkladem pro vědecké zkoumání či k přijetí opatření provozovatelů ATM v ČR, popřípadě v dalších zemích.

ZÁVĚR

Hlavními úkoly práce bylo analyzovat rizika v souvislosti s používáním platebních karet, zjistit a vyhodnotit statistiky zjištěných podvodů s platebními kartami, uvést problémy s objasňování uvedené trestné činnosti, provést výzkum u náhodně oslovených respondentů za účelem zjištění míry zabezpečení jejich platebních karet a informovanosti o rizicích s jejich používáním a navrhnout vlastní opatření ke zvýšení bezpečnosti výběru z ATM.

Statistické údaje podvodů s platebními kartami oslovené banky neposkytly, nicméně z informačních systémů Policejního prezidia Policie ČR byly získány vykázané statistické údaje o trestné činnosti spojené se zneužitím platebních karet v ČR za období let 2001-2010 s rozlišením trestné činnosti i v jednotlivých krajích. Vyhodnocením získaných údajů bylo zjištěno, že od roku 2005 do 2010 vznikla téměř jedna událost každou hodinu, s průměrnou škodou ve výši 10 114,- Kč. Největší počet případů byl zaznamenán na území hlavního města Prahy. Podle životní úrovně obyvatel ČR byly vypočítány následky v podobě průměrné délky sociálního dopadu na poškozené ve výši 311 dní. Stanovené míry pravděpodobnosti a následků byly podkladem pro kvantifikovanou analýzu rizika zneužití platebních karet. Zvolenou metodou bylo zjištěno, že uvedené riziko se ve sledovaném období let 2001-2010 pohybovalo v pásmu středního rizika, avšak v letech 2001 a 2010 dosáhlo míry vysoké.

Dále byly analyzovány problémy s usvědčováním pachatelů trestné činnosti, které se potvrdily výzkumem na základních útvarech Policie ČR Městského ředitelství v Ostravě. Byl totiž zjištěn nesoulad času záznamu pořízeného ze snímací kamery ATM a nedokonalý kamerový systém ATM. Proto bylo navrženo opatření ke zlepšení zjištěné situace a také opatření ke zvýšení bezpečnosti používání platebních karet zavedením biometrických prvků u ATM a POS terminálů. Míra bezpečnosti jakéhokoli systému je však vyvážena nemalými finančními investicemi a realizace tohoto návrhu je spíše vizí budoucnosti.

Navzdory všem rizikům, která jsou v práci popsána a analyzována, je zřejmé, že rizika ani zdaleka nedosáhla kritických hodnot. Rizika jsou adekvátně řešena a pokud držitelé karet budou dodržovat zásady doporučované vydavateli karet, lze s jistotou prohlásit, že systém používání platebních karet v ČR je bezpečný.

CONCLUSION

The main task of this study was to analyse the risks associated with using payment cards, to identify and evaluate the statistics of fraud with credit cards, then to mention problems concerning clearing the crime, do research with respondents at random to determine the security on their credit cards and the risks of their own use knowledge and to suggest measures to increase security of choosing from the ATM.

Banks addressed did not provide statistics about credit card frauds, but from the information systems of the Police Presidium of the Police of the Czech Republic, I have obtained reported statistics about crimes related to misuse of credit cards in the Czech Republic for the period 2001-2010 with a definition of crime in each region. By evaluating the data, there was found that from 2005 to 2010 almost one event per hour happened, with an average loss of 10,114, - CZK. The largest number of cases was recorded in the capital city of Prague. According to the standard of living of the population in the Czech Republic, the consequences were calculated as the average length of the social impact of 311 days for the injured. The specified degree of probability and consequences has been the basis for a risk quantified analysis of misuse of credit cards. The chosen method found that the risk in the reference period 2001-2010 varied in the range of secondary risks, but between 2001 and 2010 reached a high level.

Further problems analysed were how to convict offenders, and these problems were confirmed using the research in departments of the Police of the Czech Republic, Municipal Headquarters in Ostrava. However, the time inconsistencies recorded by the ATM cameras were found, likewise imperfect ATM camera system. Therefore, the measure to improve the situation identified was suggested, and also measure to increase the safety of using credit cards, by the introduction of biometrics at ATMs and POS terminals. The security rate of any system is balanced by considerable financial investment and the implementation of this proposal is rather a vision of the future.

Despite all the risks described and analysed in this study, it is clear that the risks did not reach critical values at all. The risks are adequately solving and if the cardholders comply with the principles recommended by the card issuers, it is possible to say with certainty that the system of using the credit cards in the Czech Republic is adequately safe.

SEZNAM POUŽITÉ LITERATURY

Monografie:

- [1] JUŘÍK, P. *Platební karty: velká encyklopedie 1870–2006*. 1. vyd. Praha: GradaPublishing, 2006. 296 s. ISBN: 80-247-1381-0.
- [2] JUŘÍK, P. *Encyklopedie platebních karet*. 1. vyd. Praha: GradaPublishing, 2003. 312 s. ISBN: 80-247-0685-7.
- [3] SCHLOSSBERGER, O., HOZÁK L. *Elektronické platební prostředky*, 1. vyd. Praha: Bankovní institut vysoká škola, 2005. 144 s. ISBN: 80-7265-073-4.
- [4] BROŽ, J., HRADECKÝ, M. *Platební prostředky, jejich ochrana a padělání*. Praha: Ministerstvo vnitra, odbor vzdělávání a správy policejního školství a Policie ČR, Útvar pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování, 2008. 160 s. ISBN: 80-7312-055-0.
- [5] VALÁŠEK, J., KOVAŘÍK, F. a kolektiv. *Krizové řízení při nevojenských krizových situacích, modul C*. Praha: Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru ČR, 2008. 102 s. ISBN: 978-80-86640-93-8.
- [6] ŠÁMAL, P. a kolektiv. *Trestní zákon. Komentář. II. díl (§ 91 až § 301)*. 6. doplnění a přepracování. Praha: C. H. Beck, 2004. 1468 s. ISBN: 80-7179-896-7.
- [7] ŠÁMAL, P. a kolektiv. *Trestní zákoník. Komentář. II. díl (§ 140 až § 421)*. 1. vydání. Praha: C. H. Beck, 2010. 2528 s. ISBN: 978-80-7400-0102.
- [8] ČERMÁK, M. *Řízení informačních rizik v praxi*. Brno: Tribun, 2009. 138 s. ISBN-80-7179-896-7.

Diplomové práce:

- [9] HRYZBYLOVÁ, M. *Analýza zúčtování operací prováděných platební kartou*. Praha: 2008. 69 s. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta financí a účetnictví.
- [10] ZAORALOVÁ, L. *System elektronických plateb*. Brno: 2009. 75 s. Diplomová práce. Masarykova univerzita, Fakulta informatiky.
- [11] KONEČNÁ, H. *Trestněprávní aspekty zneužívání vybraných typů elektronického bankovníctví*. Brno: 2009. 70 s. Diplomová práce. Masarykova univerzita, Právnická fakulta.

Právní předpisy:

- [12] Zákon č. 284/2009 Sb. o platebním styku, v platném znění.
- [13] Zákon č. 140/1961 Sb., trestní zákon (účinnost do 31.12.2009), ve znění pozdějších předpisů.
- [14] Zákon č. 40/2009 Sb., trestní zákoník (účinnost od 1.1.2010), ve znění pozdějších předpisů.
- [15] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
- [16] Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, v platném znění.
- [17] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- [18] Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů.
- [19] Rámcové rozhodnutí Rady Evropské unie č. 2001/413/SVV, o potírání podvodů a padělání bezhotovostních platebních prostředků.

Další zdroje:

- [20] Rozhodnutí Ústavního soudu ze dne 17.6.2004, spisová značka IV ÚS37/03 k právu na soudní a jinou právní ochranu.
- [21] Stanovisko Nejvyššího státního zastupitelství č. 3/2005 Sb. ke sjednocení výkladu zákonů a jiných právních předpisů k otázce právního posouzení odcizení platební karty.
- [22] Stanovisko Nejvyššího státního zastupitelství č. 2/2007 Sb. ke sjednocení výkladu zákonů a jiných právních předpisů k možnosti postihu jednání osoby spočívajícího v padělání či pozměňování platební karty jako trestného činu padělání a pozměňování peněz podle § 140 odst. 2, § 143 trestního zákona.
- [23] *Padělání platebních karet*. Presentace. Praha: 2011. Policie ČR, Služba kriminální policie a vyšetřování, Útvar pro odhalování organizovaného zločinu.
- [24] *Skimmovací zařízení v ČR 2008-2010*. Presentace. Praha: 2011. Policie ČR, Služba kriminální policie a vyšetřování, Útvar pro odhalování organizovaného zločinu.
- [25] LUKÁŠ, L. *Systémy kontroly vstupu jako zdroj informací o pohybu zaměstnanců II*. Výuková presentace. Zlín: 2008. Univerzita Tomáše Bati ve Zlíně, Ústav měření a elektrotechniky.

Časopisecká díla:

- [26] Wincor Nixdorf - Snaha o zvýšení bezpečnosti u bankomatů. *Cardmag: magazín nejen o kartách*. 17. března 2010, No 1/2010 - zimní vydání, s. 34. Dostupné z WWW: [<http://www.cardmag.cz>].
- [27] SADOVSKÝ, D., SUCHÁNEK, J. Platební karty a možnosti jejich zneužití. *Kriminalistika: časopis pro kriminalistickou teorii a praxi*. 2004, roč. XXXVII, č. 1, s. 20-29. ISSN 1210-9150.
- [28] KOČÍ, P. Virtuální peníze v ohrožení. *Týden: zpravodajský týdeník*. 2008, roč. XV, č. 33, s. 44-48. ISSN 1210-9940.
- [29] HRADECKÝ, M.; BROŽ, J. Skimming platebních karet v roce 2007. *Kriminalistický sborník*. 2008, roč. LII, č. 3, s. 44.
- [30] Za výrazným růstem plateb ve světě stojí platební karty. *Bankovníctví*. 2008, roč. XVI, č. 9, s. 7. ISSN 1212-4273.

Elektronické zdroje:

- [31] *SBK bankovní karty: souhrnné statistiky ke stažení* [online]. 2011, aktualizace 2011-07-29 [cit. 2011-08-02]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html>.
- [32] *SBK bankovní karty: bezpečnost* [online]. 2011, aktualizace 2011-07-29 [cit. 2011-08-02]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html>.
- [33] *SBK bankovní karty: slovník* [online]. 2011, aktualizace 2011-07-29 [cit. 2011-08-02]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/slovník_platebni_karty.html>.
- [34] *Souhrnné statistiky* [online]. Policejní prezidium, Centrum informatiky a analytických procesů Služby kriminální policie a vyšetřování. 2011 [cit. 2011-03-05]. Dostupné na policejním intranetu z WWW: <http://essk.pcr.cz/essk/_sest_root.esp>.
- [35] *Česká republika v číslech* [online]. Český statistický úřad. 2010, 2010-12-10 [cit. 2011-02-27]. Dostupné z WWW: <<http://www.czso.cz/csu/2010edicniplan.nsf/publ/1409-10-2010>>.

- [36] Smart card. In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 7 July 2004, last modified on 12 March 2011 [cit. 2011-03-14]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Smart_card>.
- [37] *Lidé reklamují výběry z bankomatu, které provedl příbuzný* [online]. Home Credit. Brno: 17.01.2011 [cit. 2011-03-24]. Dostupné z WWW: <http://www.homecredit.cz/cs/tiskove_centrum/tiskove_zpravy/146.shtml>.
- [38] *Zneužití karty hrozí nejvíce po její krádeži a na internetu* [online]. Home Credit. Brno: 3.2.2010, [cit. 2011-03-24]. Dostupné z WWW: <http://www.homecredit.cz/cs/tiskove_centrum/tiskove_zpravy/120.shtml>.
- [39] *Jak vyvrát na skimming* [online]. Česká spořitelna. Praha: 2010 [cit. 2011-03-27]. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/sc_5683.xml>.
- [40] NESEJT, P. *První phishing v Česku, terčem byla CitiBank* [online]. Finance.cz, 16. 3. 2006 [cit. 2011-03-29]. Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/>>.
- [41] *COMFIS: Produkty-Terminály a Privaris* [online]. Buchlovce: 2008 [cit. 2011-07-31]. ZEM200 EDK. Dostupné z WWW: <<http://www.comfis.cz/produkty/vyvojove-produkty/zem200-sdk>>.
- [42] SVOBODA, J. *Placení kartami je v ČR bezpečnější než v EU* [online]. Právo, 28. 5. 2008 [cit. 2011-07-31]. Dostupné z WWW: <<http://www.novinky.cz/clanek/140974-placeni-kartami-je-v-cr-bezpecnejsi-nez-v-eu.html>>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

a.s.	Akciová společnost.
ATM	Automated teller machine (bankomat).
ČR	Česká republika.
ČSÚ	Český statistický úřad.
EEPROM	Electrically Erasable Programmable Read Only Memory.
EU	Evropská unie.
KŘP MSK	Krajské ředitelství policie Moravskoslezského kraje.
MŘP	Městské ředitelství policie Ostrava.
NSZ	Nejvyšší státní zastupitelství.
POS	Point Of Service (místo transakce, prodejní místo).
RAM	Random Acces Memory.
ROM	Read Only Memory.
SBK	Sdružení bankovních karet.
USA	Spojené státy americké.
USD	Americký dolar.

SEZNAM OBRÁZKŮ

Obr. 1. Rozdělení platebních karet	14
Obr. 2. Příklad uložení záznamů na stopách magnetického proužku platební karty	19
Obr. 3. Umístění a přiřazení kontaktů na čipové kartě	20
Obr. 4. Proces autorizace	22
Obr. 5. Postup skimming	28
Obr. 6. Phishing – podvodný e-mail	31
Obr. 7. Ukázka zařízení padělatelské dílny	33
Obr. 8. Vývoj trestné činnosti spojené se zneužitím platebních karet v ČR.....	38
Obr. 9. Přehled škod způsobených trestnou činností spojenou se zneužitím platebních karet v ČR.....	38
Obr. 10. Speciální hledisko pachatelů sledované trestné činnosti	39
Obr. 11. Přehled trestné činnosti spojené s neoprávněným držením platební karty zjištěná v rámci území jednotlivých krajů v ČR za období let 2001-2010	40
Obr. 12. Vývoj pravděpodobnosti vzniku události na kartu a občana ČR.....	43
Obr. 13. Vývoj následků v podobě sociálního dopadu na poškozené	46
Obr. 14. Grafické znázornění stanoveného rizika.....	50
Obr. 15. Vývoj počtu případů skimming v ČR.....	55
Obr. 16. Vzorek otisku prstu s detailem papilárních linií.....	63
Obr. 17. ZEM200 EDK.....	65

SEZNAM TABULEK

Tab. 1. Přehled ochranných prvků karet	17
Tab. 2. Statistika trestné činnosti spojené s neoprávněným držením platební karty v ČR.....	37
Tab. 3. Statistika trestné činnosti spojené s neoprávněným držením platební karty v rámci jednotlivých krajů.....	40
Tab. 4. Pravděpodobnost vzniku události	42
Tab. 5. Pravděpodobnost napadení platebních karet	42
Tab. 6. Pravděpodobnost poškození vlastníka karty.....	43
Tab. 7. Pravděpodobnost napadení karet skimming	44
Tab. 8. Škody způsobené na jeden případ	45
Tab. 9. Životní úroveň obyvatelů ČR	45
Tab. 10. Délka sociálního dopadu poškozených.....	46
Tab. 11. Kvantifikace aktiv.....	47
Tab. 12. Kvantifikace hrozeb.....	47
Tab. 13. Kvantifikace zranitelnosti	48
Tab. 14. Hodnocení rizika.....	49
Tab. 15. Přehled hodnoceného rizika.....	50

SEZNAM PŘÍLOH

P I: LIBANONSKÁ SMYČKA

P II: HRADECKÁ LIŠTA

P III: SKIMMOVACÍ ZAŘÍZENÍ

P IV: DOTAZNÍKY BANKÁM A DALŠÍM SUBJEKTŮM

P V: DOTAZNÍKY NA RESPONDENTY

P VI: DOTAZNÍKY NA POLICEJNÍ ÚTVARY V OSTRAVĚ