UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

Ochrana bankovního sektoru jako segmentu kritické infrastruktury

Bc. Aleš Pulkrábek

Diplomová práce

2009

Originál zadávacího listu

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 20. srpna 2009

Aleš Pulkrábek

Poděkování

Tímto bych rád poděkoval všem, kteří mi byli nápomocni při psaní této práce, zvláště pak vedoucímu mé diplomové práce doc. RNDr. Petru Linhartovi, Csc. za cenné rady a připomínky. Dále děkuji Mjr. Ing. Jarmilu Valáškovi, který mi poskytl nezbytné materiály pro vyhotovení mé práce.

ANOTACE

Obsahem teoretické části diplomové práce je problematika kritické infrastruktury a popis jejich jednotlivých segmentů. V praktické části se práce zabývá popisem platebních karet, jejich rizik a zaváděním čipové technologie. Pomocí statistických metod je vyjádřen vztah mezi náklady na zavedení čipové technologie a snížením zneužití platebních karet+. Součástí práce jsou i návrhy na zkvalitnění ochrany .

KLÍČOVÁ SLOVA

kritická infrastruktura, bankovní sektor, platební karta, čipová technologie

TITLE

Protection of banking sector as a section of critical infrastructure

ANNOTATION

The theoretical part of the thesis contains questions of critical infrastructure and description of their particular sections. The practical part is concerned with the credit cards description, the risk of there usage, and chip technology implementing. Statistical methods are used to formulate the dependance between expenses of chip technology implementing and reduction in credit cards abuse. Suggestions of banking sector upgrading are components of the diploma paper.

KEYWORDS

critical infrastructure, banking sector, credit/debit card, chip technology

Obsah

Seznamy

Seznam zkratek

ATM ..... bankomat

AX ..... American Express

BIN ..... bankovní identifikační číslo

BP ..... Basis Points

CAM ..... metoda autentikace karty

CVC ..... kontrolní kód používaný asociací MasterCard

CVM ..... metoda ověření držitele karty

CVV ..... kontrolní kód používaný asociací Visa

DCI ..... Diners‘ Club International

EMV ..... technické specifikace k používání čipové technologie v platebním styku

IS ..... informační systém

JCB ..... Japan Credit Burelu

KI ..... kritická infrastruktura

MC ..... MasterCard

MV ..... ministerstvo vnitra

PIN ..... osobní identifikační číslo

SBK ..... Sdružení pro bankovní karty ČR

SEPA ..... Single Euro Payment Area

SÚJB ..... Státní úřad pro jadernou bezpečnost

Seznam obrázků

Seznam tabulek

Seznam grafů

Úvod

Žijeme v době, která přináší lidem vědecko – technický pokrok. Nové prostředky a technologie ulehčují lidem jejich každodenní život. Na druhé straně s sebou pokrok přináší i řadu nových problémů. Vznikají nová rizika, která mohou vyústit až v krizové situace a mít negativní dopad na obyvatelstvo i životní prostředí.

Systémy, jejichž nefunkčnost by měla vážné dopady na bezpečnost, ekonomiku a zachování funkcí státu při krizových situacích, se nazývají kritická infrastruktura. Kritická infrastruktura slouží k vedení a ochraně státu, ochraně životů obyvatel, majetku, zdraví i majetku.

Nehody, katastrofy, havárie, přírodní pohromy a jiná rizika mívají ničivý dopad. Lidé se těmto vzniklým problémům snaží předcházet. Možným východiskem jsou preventivní opatření a schopnost zajistit rychlou obnovu poškozených systémů a subsystémů. Díky vzniku a vymezení kritické infrastruktury bude mít každý stát vytvořený vlastní systém ochrany se stanovenými pravidly, kterými se bude řídit v případě vzniklého nebezpečí.

Do kritické infrastruktury spadají prvky pro správné fungování státu nepostradatelné. Z tohoto důvodu bylo navrhnuto téma mé diplomové práce, která by měla alespoň trochu přispět k rozpoznání možných rizik vybrané oblasti kritické infrastruktury.

První kapitola se bude zabývat popisem základních pojmů z oblasti kritické infrastruktury. Popis těchto pojmů je důležitý pro správné pochopení souvislostí v navazujících kapitolách a pro lepší orientaci v dané problematice.

V druhé kapitole budou představeny jednotlivé segmenty kritické infrastruktury. Tyto segmenty jsou nezbytné pro bezpečné fungování státu.

Třetí kapitola bude obsahovat podrobnější popis bankovního sektoru jako jednoho ze segmentů kritické infrastruktury. První tři kapitoly mé práce budou teoretického charakteru a jejich úkolem seznámit čtenáře s danou problematikou.

Čtvrtá kapitola bude zaměřena na výběr určité oblasti bankovního sektoru. Tato oblast bude blíže představena a stručně analyzována. Údaje získané z analýzy budou předmětem zkoumání. Prostřednictvím statistických metod by měly být dosaženy závěry, které budou následně interpretovány.

V poslední kapitole budou nastíněna opatření a doporučení, které by mohly vést ke zvýšení ochrany zkoumané oblasti bankovního sektoru.

Diplomová práce má tři cíle. Prvním z nich je obecný popis problematiky kritické infrastruktury, druhým je popis vybrané oblasti bankovního sektoru a její analýza. Třetím cílem je vytvoření návrhu na opatření, který přispěje k ochraně dané oblasti.

1 Problematika kritické infrastruktury na začátku 21. století

1.1 Kritická infrastruktura

S rostoucím pronikáním nových informačních a komunikačních technologií do všech oblastí života vznikají nové hrozby nejen pro jednotlivce, ale i pro stát, hospodářství a společnost. Jsou zaměřeny proti infrastruktuře zemí s vyspělou technologií, na které v rostoucím rozsahu závisí všechny funkční oblasti informačního věku. Hrozby mohou vycházet od jednotlivých pachatelů trestných činů, teroristických a kriminálních organizací, ale také z nepřátelských států. Do té míry se stále více překrývá civilní a vojenské ohrožení i vnitřní a vnější bezpečnost. Informační struktura zemí s vyspělou technologií je zranitelná tou měrou, do jaké je prostřednictvím komunikačních technologií veřejně a anonymně přístupná, lokálně, národně a celosvětově síťovaná. Běžné rozlišování například mezi válkou a neválkou, mezi veřejnými a soukromými zájmy, válečnými a kriminálními aktivitami nebo politickými a zeměpisnými hranicemi se v kybernetickém boji stále více prolínají. Čím je některá oblast života společnosti závislejší na informačních technologiích, tím závažněji na daný sektor infrastruktury působí nefunkčnost informačních technologií. Tím se dostává problematika kritické infrastruktury z „abstraktní“ oblasti kybernetiky do oblasti zabezpečení života společnosti v sektorech jako je např. telekomunikace, doprava, zásobování energií, potravinami a pitnou vodou, ale také zabezpečení zdravotnictví, bankovnictví, fungování státní správy atd.

Pod kritickou infrastrukturou jsou převážně míněny systémy, jejichž zničení nebo omezení funkčnosti by mělo vážné dopady na ekonomickou a společenskou stabilitu, obranyschopnost a bezpečnost státu, na fungování státu jako územně společenské komunity.

1.1.1 Výchozí přístupy v pojímání kritické infrastruktury

USA a Austrálie patří mezi první státy, které začaly vnímat potenciál a šířku problému kritické infrastruktury. Byly to právě tyto země, které zahájily diskusi o zranitelnosti životní infrastruktury (později označované jako kritické infrastruktury). Prvním uceleným materiálem, řešícím otázky ochrany kritické infrastruktury, byla tzv. Bílá kniha (White Paper). Jednalo se o Směrnici 63, kterou vydal v květnu 1998 prezident USA Clinton, jako prezidentské rozhodnutí (Presidential Decision Directive 63). Bílá kniha pojímá kritickou infrastrukturu jako základní systémy, které mají hmotnou a kybernetickou základnu a mají vliv na funkčnost ekonomiky a státu. Tyto základní systémy zahrnují oblasti: telekomunikace, energie, bankovní a finanční sektor, dopravu, zásobování vodou a záchranné služby. Hlavním záměrem prezidentské směrnice bylo přijetí nezbytných opatření k rychlé eliminaci zranitelnosti a to z hlediska hmotných a kybernetických útoků na kritickou infrastrukturu. Větší důraz byl v té době přikládán možným útokům na kybernetické systémy.

Důležitým požadavkem Bílé knihy je rozšiřování politiky ochrany kritické infrastruktury ke všem zainteresovaným subjektům jak v soukromém, tak veřejném sektoru. Politika ochrany kritické infrastruktury stanovila cíle, poskytla koncepci a zdroje a zařadila kritickou infrastrukturu mezi národní životní zájmy. Nehledě na události 11. září 2001 lze učinit závěr, že politika ochrany kritické infrastruktury vytvořila novou startovní čáru pro opatření v oblasti vnitřní bezpečnosti.

1.1.2 Počátky vnímání kritické infrastruktury v Evropě

Otázkami kritické infrastruktury se rovněž zabývala státní administrativa v evropských zemích. Snad nejdříve tomu bylo ve Velké Británii, kde na konci roku 1999 bylo ustanoveno Koordinační centrum pro bezpečnost národní infrastruktury (National Infrastructure Security Coordination Centre). Úkolem koordinačního centra bylo rozvíjet a koordinovat činnost k ochraně kritické národní infrastruktury. Byly identifikovány systémy, jejichž kontinuita je důležitá pro fungování státu, resp. jejichž ztráta nebo narušení by vedla nebo by mohla vést k ohrožení životů, vážným

negativním hospodářským a sociálním dopadům na společnost nebo její velkou část. Mezi tyto systémy byly zahrnuty státní správa, nouzové služby (např. policie, hasičská záchranná služba, zdravotní záchranná služba, povodňová a pobřežní obrana), dodávky energií a paliv (plyn, elektřina, ropa, jaderné palivo, uhlí apod.), dodávky vody a oblast kanalizací, telekomunikace, dodávky potravin, zdravotnictví (záchranná služba, zdravotnické potřeby, veřejné zdraví, sesterská péče a pohřební služby), doprava (letecká, železniční, silniční a autobusová, metro a tramvajová doprava, lodní doprava, přístavní doprava a přívozy, pobřežní hlídky), finance a ekonomika, komunikace (poštovní služby, noviny, televizní a rozhlasové vysílání), spravedlnost (ochrana před kriminálními živly, tj. soudnictví, vězeňská služba, imigrační kontrola atd.), vzdělání, věda a výzkum, sociální opatření a služby (sociální podpory a služby, bydlení, hygienická zařízení a likvidace odpadu) a předpověď počasí.

Ochrana kritické národní infrastruktury je ve Velké Británii rozpracovávána a rozvíjená jak pro veřejný, tak soukromý sektor.

Otázkami kritické infrastruktury se po roce 1998 zabývaly další Evropské státy. Lze v této souvislosti poznamenat aktivity ve SRN, kde např. byl v prosinci 1999 projednán materiál „Informačně technické ohrožení klíčových infrastruktur v Německu“. Nelze opomenout významné aktivity a opatření při řešení ochrany kritické infrastruktury na národní úrovni v Holandsku.

Společným jmenovatelem problematiky ochrany kritické infrastruktury tohoto období byl především důraz na ochranu informačních a komunikačních technologií.

1.2 Kritická infrastruktura po 11. září 2001

Po teroristickém útoku na světové obchodní centrum v New Yorku, k němuž došlo 11. září 2001, otázky ochrany kritické infrastruktury eskalují a nabývají nový obsah a rozměr. První a nejpropracovanější reakce vznikly v USA. Již 16. října 2001 vydává prezident USA Georgie W. Bush „Vládní nařízení na ochranu kritické infrastruktury“ (Executive Order on Critical Infrastructure Protection). Toto nařízení bylo vydáno za účelem zabezpečit ochranu informačních systémů pro kritickou infrastrukturu, včetně nouzové komunikační připravenosti a ochrany hmotných zařízení, které informační

systémy podporují. Jako prioritní bylo stanoveno zabezpečení tří vzájemně závislých funkcí: ekonomiky, činnost státu (vlády) a vedení národní obrany.

Řešení kritické infrastruktury v USA doznalo svého vyvrcholení v únoru 2003, a to vydáním národní strategie. Tomuto kroku předcházelo zpracování a vydání v červenci 2002 „Národní strategie vnitřní bezpečnosti“ (The National Strategy for Homeland Security). Mimo jiné tato strategie uvádí definici kritické infrastruktury a rozumí pod ní „systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA, a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci“. 14. února 2003 pak byla vydána „Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“ (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets) a „Národní strategie zabezpečení kybernetického prostoru“ (The National Strategy to Secure Cyberspace).

Přijetím strategie ochrany kritické infrastruktury a strategie zabezpečení kybernetického prostoru došlo k určitému rozdělení, resp. specifikaci kritické infrastruktury, a to z hlediska kybernetického a hmotného. V oblasti kybernetiky jde o zabezpečení, resp. ochranu kybernetického prostoru, který je, z pohledu USA, vlastněn, řízen, kontrolován nebo se kterým je v interakci. V oblasti hmotných prostředků jde o fyzickou ochranu kritické infrastruktury a klíčových zařízení.

„Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“ je v současnosti nejkomplexnějším materiálem zabývajícím se problematikou kritické infrastruktury. Formuluje politiku státu v této oblasti a při tom zdůrazňuje, že USA musí chránit takovou kritickou infrastrukturu a klíčová zařízení, která by:

- oslabila schopnost federální vlády vykonávat základní národní bezpečnostní úkoly a zabezpečovat veřejné zdraví a bezpečnost
- narušila schopnosti centrálních a místních orgánů při udržování pořádku a zabezpečování základních veřejných služeb
- poškodila funkčnost privátního sektoru při zabezpečování řádného chodu ekonomiky a základních služeb

- podkopávala veřejnou morálku a důvěru v národní ekonomiku a politické instituce

1.3 Kritická infrastruktura v ČR

V České republice laická veřejnost pojem „bezpečnost“ často chápe velmi úzce, obvykle jen ve smyslu spojeném s účely, pro které byla zřízena policie či armáda a dodnes je tak na veřejnosti interpretován. Skutečnost je poněkud odlišná. Již v r. 1994 byla vypracována teoretická studie o bezpečnostní politice, která byla postupně uváděna do politické praxe. Bezpečnostní politika byla pojímána v širokém slova smyslu a byla prezentována jako systémové a cílevědomé působení jednotlivých složek státu. V EU, USA a dalších vyspělých zemích je pojem „bezpečnost“ chápán ve smyslu komplexním, který koresponduje s pojetím používaným v oblasti technologií a vyplývá z dlouhodobé pozornosti státních orgánů této důležité podmínce života společnosti.

Z důvodu nekoncepčního řízení „bezpečnosti“ se výzkum bezpečnosti v České republice provádí jen v úzkých, navzájem nekoordinovaných oblastech zaměřených na aspekty jednotlivých resortů - policie, armády či bývalé civilní ochrany. Dále se izolovaně výzkum bezpečnosti provádí v oblasti jaderných technologií, chemických a biologických rizik, v oblasti bezpečnosti práce a nově po implementaci direktivy Seveso[1] i v oblasti chemických technologií.

Z výše uvedeného vyplývá, že v řadě dalších oblastí se výzkum bezpečnosti neprovádí a v těch oblastech, ve kterých se provádí, není vzájemně provázaný, a tudíž chybí synergický[2] efekt.V souvislosti se vstupem ČR do Severoatlantické aliance a převažujícímu hodnocení hrozeb i jejich predikce se devět z desíti občanů neobávalo ozbrojených konfliktů, nebyli je schopní identifikovat a vnější bezpečnost, vnitřní bezpečnost a ochranu obyvatelstva nepovažovali za prioritu. Bezprostředně po 11. září 2001 obavy výrazně vzrostly. Po povodních v roce 2002 ustoupila problematika vnější bezpečnosti do pozadí a výrazně stouply obavy z účinků přírodních katastrof.

1. [1] směrnici č. 82/501/EEC, jejímž cílem bylo zavedení jednotné legislativy, týkající se prevence a připravenosti na závažné průmyslové havárie a zpracování a uplatňování vhodných opatření.
2. [2] vzájemně působící

Zaměření dlouhodobého směru výzkumu vyplývá z § 12, zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, v jehož kontextu Ministerstvo vnitra ČR (MV) je ústředním orgánem státní správy pro krizové řízení, civilní nouzové plánování, ochranu obyvatelstva, integrovaný záchranný systém a požární ochranu a jemu tedy náleží koordinační funkce. Předmětné specifické oblasti se vzájemně prolínají a existují ve vzájemných propojeních a souvislostech.

Jedná se o úkoly na úseku:

- krizového plánování a jeho příprav
- na úseku civilního nouzového plánování
- na úseku ochrany obyvatelstva
- na úseku integrovaného záchranného systému
- na úseku požární ochrany vyplývající ze zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů a zákona č. 133/1985 Sb., o požární ochraně plní MV- generální ředitelství Hasičského záchranného sboru ČR

V ČR není bezpečnostní politika chápana komplexně. Principiálně se bezpečnostní politika rozčleňuje na tři základní oblasti:

- ochrana životního prostředí
- ochrana obyvatelstva
- ochrana majetku

1.3.1 Bezpečnostní politika ČR

Bezpečnostní politika je souhrn určitých opatření a kroků, který je veden za účelem prevence a eliminace hrozeb a z nich vyplývajících rizik s cílem zajistit vnitřní a vnější bezpečnost, obranu a ochranu občanů a státu. Bezpečnostní politika je prováděna pomocí zahraniční, obranné a hospodářské politiky a taky politiky v oblasti vnitřní bezpečnosti a veřejné informovanosti, které jsou rovnocenné, soudržné a navzájem provázané. Při zajišťování bezpečnosti je vždy důležité aktivní a hlavně preventivní

působení v celém spektru bezpečnostní politiky. Především jde zde o prohlubování mezinárodní spolupráce mezi státy a účast ČR ve spojeneckých svazcích, zapojování našich občanů do dílčích aktivit při zajišťování bezpečnosti, ale nutně také o vytváření podmínek pro uvědomělé konání občanů ČR. Teroristické útoky a protiteroristické úsilí nám potvrzuje, že vnitřní a vnější bezpečnost je v dnešním otevřeném světě nutné zajišťovat na základě komplexního přístupu.

Výkonnost ČR v úseku hospodářství a míra mezinárodní spolupráce velmi významně spoluurčují možnosti ČR při zajišťování její bezpečnosti. Zajištění bezpečnosti občanů, demokratického státu, principů právního státu a principů tržního hospodářství v ČR jsou prvotními předpoklady pro efektivní rozvoj hospodářství. Dalšími potřebnými faktory pro rozvoj hospodářství ČR jsou taky prvky ekonomické bezpečnosti a globální ekonomické stability. Úkolem vlády ČR je v daném rozsahu zajišťovat hlavně bezpečnost občanů, suverenitu země, demokratické zřízení a principy právního státu. Bezpečnost ČR musí brát jako prioritu bezpečnost jednotlivce, ochranu jeho života, zdraví a majetku a státních institucí včetně jejich funkčnosti. Za celkovou bezpečnost státu je odpovědná vláda, ale i tak je po občanech a orgánech veřejné správy požadována aktivní spolupráce při odstraňování možných ohnisek hrozeb. Vláda se snažila a nadále bude vycházet vstříc svým občanům při aktivním zajišťování bezpečnosti státu. Proto musí být informovanost občanů o dané bezpečnostní situaci ve státě prováděna co nejpodrobněji a co nejlépe, aby každý daný problém pochopil.

Bezpečnostní politika ČR vychází z principu nedělitelnosti bezpečnosti. Neustálým zájmem ČR je udržení postoje u OSN a taky snaha o posílení euroatlantického bezpečnostního prostoru. ČR se nemůže lhostejně chovat k ostatním zemím a jiným národům, je proto vždy připravena společně s ostatními zeměmi čelit problémům z hlediska bezpečnosti a zmírňováním jejich následků.

ČR nikdy neupřednostňovala řešení problému pomocí ozbrojených konfliktů. Vždy to z „druhé strany“ nemusí být pravidlem, ale i přesto je snaha ČR řešit problém diplomatickými prostředky. Pokud však i zde selžou mírové prostředky, musí se ČR obrátit k použití síly na ochranu svých životně důležitých prvků a v případě nutnosti i vybraných strategických zájmů.

ČR se vstupem do Severoatlantické aliance zavázala k posílení individuální schopnosti z hlediska obrany. To byl prvotní důvod ke vzniku profesionální armády.

Moderně vyzbrojená, flexibilní a hlavně vysoce mobilní armáda je schopna pomáhat v mezinárodních operacích, a to i mimo ČR. Tohle je cílený výsledek seskupení národů, kolektivní obrany a bezpečnosti v rámci mezinárodních organizací a jiných uskupení. Pilířem kolektivní obrany je pro ČR NATO. ČR se těší bezpečnostním zárukám a to díky členství v NATO, kde je vše ukotveno v Severoatlantické smlouvě. ČR se taky aktivně snaží zapojit do Společné zahraniční a bezpečnostní politiky EU a v jejím rámci do Evropské bezpečnostní a obranné politiky.

ČR v dnešní době vychází z předpokladů, že v dohledné době by nemělo dojít k jakémukoli přímému vojenskému útoku, jak na její území tak i na území jejich spojenců. V euroatlantickém prostoru došlo k prohlubování integračních a demokratizačních procesů, ale mimo euroatlantický prostor začalo vznikat nebezpečí s možností teroristického útoku, které může mít nedozírné následky.

V podmínkách bezpečnostní politiky ČR je rozvíjeno především krizové řízení, které je pojato jako souhrn řídících činností věcně příslušných orgánů, které jsou zaměřeny na analýzu a vyhodnocení rizik, plánování, organizování, realizaci a kontrolu činností, prováděných v souvislosti s přípravou na řešení a s řešením krizové situace. Za krizovou situaci je považována mimořádná událost, při níž je vyhlášen některý z krizových stavů (stav nebezpečí, nouzový stav, stav ohrožení státu a válečný stav). Krizové řízení je rovněž vnímáno jako komplex opatření a úkolů, které pro zajištění ochrany a bezpečnosti obyvatelstva při vzniku mimořádných, resp. krizových situací plní orgány veřejné správy ve spolupráci s dalšími organizacemi. Jedná se zejména o činnosti směřující k udržení funkčnosti veřejné správy, udržení fyzického a duševního zdraví obyvatelstva, zajištění dostupnosti životně důležitého zboží a služeb, uchování soukromého a veřejného majetku, organizaci záchranných, likvidačních a obnovovacích prací na postiženém území, humanitární pomoci postiženému území. Nedílnou součástí je identifikace a ochrana kritické infrastruktury, např. zásobování vodou, elektřinou a teplem. Z hlediska zabezpečování bezpečnosti státu nabývá ochrana kritické infrastruktury stále většího významu a priority zejména proto, že vytváří podmínky pro zvládání mimořádných událostí a krizových situací. Prvky kritické infrastruktury rozhodujícím způsobem ovlivňují schopnost reakce na krizové situace.

Civilní nouzové plánování souvisí se vznikem a vývojem NATO. Aktivity byly zpočátku zaměřeny především na podporu vojenské činnosti, později také na pomoc při obnově společnosti po válečném konfliktu, ochranu civilního obyvatelstva a další

činnosti související s řešením krizových situací mírového charakteru. Tvoří tak ucelenou oblast plánování ochrany společností členských států NATO před účinky krizových situací. Ochrana obyvatelstva je charakterizována jako soubor činností a postupů věcně příslušných orgánů, dalších subjektů i jednotlivých občanů směřujících k minimalizaci dopadů mimořádných událostí na životy a zdraví obyvatelstva, majetek a životní prostředí.

Předpokládané výsledky výzkumu jsou v kontextu s aktuální politikou vlády v oblasti bezpečnosti státu. Výsledky výzkumu budou v praxi znamenat především zvýšení úrovně a efektivnosti krizového řízení, civilního nouzového plánování, ochrany obyvatelstva, integrovaného záchranného systému a požární ochrany při krizových situacích.

Využití výsledků výzkumu je základním prvkem zkvalitnění procesu realizace preventivních opatření orgánů státní správy, samosprávy a dalších subjektů zodpovědných za přípravu na řešení a řešení krizových situací. Předpokládané výsledky výzkumu tak zahrnují vědeckou podporu zdokonalování systému a specializovaných opatření ke zvýšení kvality účinnosti krizového řízení, civilního nouzového plánování, ochrany obyvatelstva, integrovaného záchranného systému a požární ochrany ČR.

Výše finančních prostředků vynakládaná ze státního rozpočtu na bezpečnostní výzkum v ČR je v diametrálním rozporu s cíli a závazky ČR. Prostředky poskytuje MV, Státní úřad pro jadernou bezpečnost (SÚJB) a ostatní resorty.

ČR chybí centrální, zastřešující instituce, která by bezpečnostní výzkum řídila a rozvíjela komplexně. Neřešení uvedených skutečností by představovalo zásadní stagnaci bezpečnostního výzkumu ve specifických oblastech orientovaných do oblasti krizové řízení, civilního nouzového plánování, ochrany obyvatelstva, integrovaného záchranného systému a požární ochrany, včetně konzervace současných nedostatků a v konečném důsledku i neschopnost ČR adekvátním způsobem reagovat na současné a zejména pak nově vznikající hrozby.

1.3.2 Prvky kritické infrastruktury

Na základě zkušeností ve světě byly pro podmínky České republiky vytipovány prvky kritické infrastruktury. Udržitelnost prvků KI má přímou vazbu na udržitelnost životní úrovně obyvatelstva ve státě. Samotné prvky mají různou úroveň působení na obyvatelstvo.

Oblasti kritické infrastruktury v ČR:

- zemědělství a potraviny
- vodní hospodářství
- veřejná správa
- nouzové služby
- zdravotní péče
- telekomunikace
- energetika
- doprava
- bankovní a finanční sektor

2 Popis jednotlivých segmentů kritické infrastruktury v České republice

2.1 Energetika

Infrastruktura energetiky je pojem, který se zabývá celkovou energetikou ČR. Energie byla vytvořena, je a bude využívána. Záleží jen na dostupnosti materiálů nebo látek, ze kterých se určitá energie bude vytvářet a jestli jde o zdroje vyčerpatelné nebo obnovitelné. Pro teroristy je jedním z nejlepších cílů poškodit systém dodávky energie pro obyvatele demokratického státu a tomu tak poškodit celkový plynulý chod. Bez energie totiž v dnešní době nejde pracovat. Spousta hlavních systémů má samozřejmě zabudovaný záložní zdroj, ale i ten má stanovenou dodávku energie.

2.1.1 Elektřina

Elektroenergetiku je možné chápat jako celostátně plošný systém s vazbami na systémy okolních států.

Výroba elektřiny do výrovy menších a průmyslových a teplárenských celků a menších výrobců. Naproti tomu jsou zde celostátní výrobci elektřiny, kteří zabezpečují podstatnou část pokrytí ČR elektřinou. Největší podíl na výrobě v ČR má ČEZ, a.s.

Elektřina je také vyráběna v menších pomocí obnovitelných zdrojů, těmi jsou voda, slunce, vítr, biomasa. Výrobní zařízení může být ovlivněno nouzovými stavy. Mezi ně patří porucha zařízení, lidský faktor nebo živelná pohroma.

K přenosu napětí 400 a 220 kV slouží přenosový systém. Tento systém je zajištěn proti výpadkům. Přenosové systémy jsou většinou ovlivňovány živelnými pohromami, kdy například při vichřici hrozí pád stožáru vysokého napětí. Více používaný je systém s vedením venkovních sítí o napětí 22 nebo 35 kV. Vedení elektřiny je v ČR prováděno na sloupech či stožárech. Ty jsou velmi lehko dostupné a tudíž zranitelné. Kabelové vedení je zase vyústěno v transformátorech, kde je taky možný přístup.

2.1.2 Plyn

V dodávkách plynu je ČR zcela závislá na Rusku a Norsku. Pro uskladnění nadbytečného plynu slouží podzemní zásobníky plynu. Nadbytek plynu vzniká v letních měsících, kdy je spotřeba plynu nižší než v měsících zimních. Pro současnou spotřebu ČR je využíváno osm podzemních zásobníků plynu.

Plynárenská soustava je dělena podle tlakových úrovní, které se v potrubí nachází.

2.1.3 Tepelná energie

Teplárenství můžeme charakterizovat jako obor, který zásobuje spotřebitele teplem a vyrábí elektřinu. Hlavní prvek systému je teplárna, kde dochází k výrobě elektřiny a tepla. Elektřina a teplo jsou dodávány teplárně nebo spotřebitelům do rozvodné sítě. Teplo se v dnešní době přenáší pomocí páry nebo teplonosné vody. Dodávky teplé páry se používají převážně ve větších městech (Brno, Přerov, České Budějovice, atd.). Dnes se hojně využívá i v technologických odvětvích jako např. sušárny.

2.1.4 Ropa a ropné produkty

Ropa i výrobky z ní jsou základním palivem pro dopravu a surovinou pro výrobu plastů. Ropa je velice žádaná a díky omezeným zásobám její cena neustále roste. Mezi státy se dodává pomocí ropovodů a produktovodů. Při transportu ropy může dojít k haváriím a úniku nebezpečných látek, které mohou ohrozit zdraví lidí ale hlavně životní prostředí.

Potrubní systémy jsou uznávány jako nejbezpečnější a nejekonomičtější způsob přepravy nebezpečných látek. Úniky toxických a hořlavých materiálů může zapříčinit havárii s katastrofickými následky.

Vždy se musí počítat s možným rizikem úniku nebezpečné látky a proto se musí myslet na preventivní opatření. Preventivní opatření se odvíjí od místa, kde by k havárii mohlo dojít. Proto se provádí prostorové analýzy, díky kterým se zjišťují místa, kudy je vhodné vést ropovody.

2.2 Doprava

Jedná se o celý systém dopravního komplexu a vytváří se tak logistická přepravní síť. Dopravní logistická síť je v dnešní době hlavně využívána podnikatelskými činnostmi. Dnes už to není jen záležitost tuzemského trhu, ale jedná se o mezinárodní vztahy. Dopravní síť se skládá z více prvků systému, jde např. o prvky investiční, provozní, ale i administrativní. V dopravní síti se velmi prolíná soukromý i veřejný sektor. Každý dopravní systém je vybudován z více samostatných prvků a ty jsou spojeny v jeden hlavní systém. Hlavní základní kámen bývá většinou dopravní prostředek a zařízení potřebné k správné činnosti a dále soubor administrativních prvků, bez kterých se v dnešní době nic neobejde. Doručení zboží ve správném množství a v určeném čase je úkolem logistiky, která by zároveň snižuje dopravní náklady. Dopravní síť je propojena více druhy dopravy.V ČR se dopravní síť skládá ze čtyř oblastí:

- silniční
- železniční
- letecká
- vnitrozemská vodní

2.3 Zemědělství a potraviny

Potraviny jsou látky (výrobky) určené ke spotřebě a patří mezi životně důležité potřeby člověka. Jedná se o jídlo a nápoje. Potrava se před pozřením upravuje vařením, pečením. Výběr potravin závisí na preferenci a sociálním postavení konzumenta. Aby se potraviny uchovaly déle čerstvé, tak se skladují a konzervují. Na produkci potravin se používá velké množství nejrůznějších technologií.

Populace obyvatel roste rychleji než je tomu u produkce výroby potravin. Zemědělci se musí potýkat s dovozem levnějšího zboží z cizích zemí. V jarních měsících se musí potýkat s mrazíky a v létě s obdobím sucha. Zavlažovací systémy však mohou používat jen tehdy, pokud neohrozí dodávky pitné vody.

Zemědělci využívají pesticidy a postřiky, které ničí choroby a nežádoucí živočichy, ale dostávají se do půdy a ničí tak živé organismy. Dnešní doba nabízí tzv. bioprodukty, které jsou výsledkem ekologického zemědělství. Při vzniku těchto potravin nejsou

používány žádné chemické látky. Poptávka po tomto druhu zboží roste i přes jeho vyšší cenu. Ta je vyvážena zdravotní nezávadností.

Zabezpečení vysoké úrovně ochrany zdraví a posílení ochrany zájmů spotřebitele jsou základními podmínkami fungování trhu. Potraviny jsou kontrolovány od produkce přes distribuční sítě až ke spotřebiteli. Vše se řídí podle daných pravidel a předpisů. Bezpečnost potravin zajišťuje Ministerstvo zemědělství a Ministerstvo zdravotnictví.

Starají se o legislativní prostředky pro ochranu a bezpečnost potravin.

Hlavní dohled nad zemědělskou výrobou, zpracováním, přepravou a distribucí potravin a surovin živočišného původu vykonávají Krajské veterinární správy a Městská veterinární správa v Praze.

Zemědělskou výrobou, lesním a vodním hospodářstvím se rozumí: zemědělská prvovýroba, která zahrnuje rostlinnou výrobu a živočišnou výrobu. Dříve byly hojně používány postřiky a pole byla práškována. Dnes se EU snaží o ekologické zemědělství, které nepoškozuje životní prostředí.

2.4 Vodní hospodářství

Voda je jednou ze základních složek života na Zemi. Potřebují ji rostliny i živočichové. Lidé jsou hlavním spotřebitelem vody. Na některých místech planety jsou vážné nedostatky vody. Lidstvo tedy musí vodu obhospodařovat a starat se o její zásoby. Díky své důležitosti se voda může stát cílem teroristických útoků, proto je třeba ji chránit.

V důsledku mimořádných událostí mohou vzniknout stavy ohrožení, které ohrožují vodu. Zde může dojít k omezení, či úplnému selhání systému zásobování obyvatelstva pitnou vodou z veřejně dostupných zdrojů. Když dojde k tak rozsáhlé krizové situaci, že je zamezena dodávka pitné vody, tak musí být tento problém velmi rychle vyřešen nouzovým zásobováním pitnou vodou. Nouzové zásobování pitnou vodou lze zabezpečit pouze cestou vyhlášení krizového stavu. Havarijní plány se nemohou udělat jednotné pro celý stát, protože nikdy se nestane úplně stejná krizová situace nebo vždy nejsou stejné následky. Vždy se musí preventivně počítat se situací, která může ohrozit zdroj pitné vody a musí být zajištěn záložní zdroj. Záložní zdroj musí být zajištěn jak po technické tak i po právní cestě a vždy musí být náležitě proškolená osoba, která jej umí obsluhovat. Každá voda použitá jako nouzový zdroj vody musí být zdravotně

nezávadná a to jak z chemického tak biologického hlediska. Při krizových situacích nebo podobných stavech je dodávka vody zajištěna pomocí cisteren.

Odklízení odpadních vod trápilo obyvatelstvo už dříve, ale kvůli dřívější technické vyspělosti to bylo velmi náročné. Nejdříve se nedbalo na čistotu, ale kvůli nárůstu a možnému vzniku nebezpečí ze vzniku nemocí se začala odpadní voda odklízet.Většinou se všechny odpadní vody sloučily v celek a ten pak dále postupoval a znečisťoval. Nejdůležitější je tedy odpad uklízet u zdroje. Postupným rozrůstáním měst se musí řešit nárůst odpadních vod a tedy i jejich čištění.Systém odpadních vod neboli kanalizace byly vytvořeny k odvodu použité a znečištěné vody. Voda odteče do kanalizačních stok a poté se vrací do čističek a podobných pomocných zařízení a znovu k obnovení pitné vody.

2.5 Veřejné správa

Veřejnou správou se v dnešní moderní společnosti rozumí správa veřejných záležitostí. Tímto subjektem je stát a další subjekty jím určené nebo ze zákona zmocněné. Veřejná správa je tvořena dvěma subsystémy, a to státní správou a samosprávou. Pod veřejnou správu jinak spadá celé státní společenství. Jedná se o moc zákonodárnou, výkonnou a soudní. Veřejná správa vykonává řídící činnosti v demokratickém státě, která má zadané úkoly od ekonomických, sociálních a politických státních cílů. Bezpečnost a ochrana obyvatelstva spadá pod veřejnou správu. V dnešní době hrozí více nebezpečí, mají rozsáhlejší dopad a ničivé účinky jsou markantnější.

2.6 Nouzové služby

Mezi nouzové služby spadají složky na ochranu státu, obyvatel, zdraví a majetku. Slouží k udržování bezpečnosti z hlediska společnosti, pro odvrácení hrozícího nebezpečí a k odhalování kriminality. Na bezpečnost dohlíží stát, instituce, organizace a jiné podniky. Slouží k udržení bezpečnosti uvnitř státu, ale i proti hrozbám či rizikům z vnějšího ohrožení. Zřízeny jsou složky ozbrojených sil, záchranné systémy, výchovné i nápravné instituce, ale taky komerční subjekty. Neustále je potřeba předcházet rizikům, které si lidé tvoří sami a nejsou schopni se s nimi vypořádat. Ty postupně přerůstají a dělají mnohonásobně větší škody než kdyby byly eliminovány včas. Stát tedy tvoří ten

hlavní prvek, kdy by měl vychovávat obyvatele, tvořit organizace a instituce a snažit se umravnit obyvatele pomocí bezpečnostních složek. Každý obyvatel by měl dbát na bezpečnost svou a také ostatních spoluobčanů.

2.7 Zdravotní péče

V ČR je velmi dobře propracovaný zdravotnický systém. Občanům slouží krajské nemocnice, polikliniky a zdravotní zařízení. Lidé mají možnost zde navštívit lékaře k preventivním kontrolám a jiným zdravotním vyšetřením. Praktičtí lékaři mají zařízené své vlastní ordinace, kde se starají o léčení nemocí občanů. Všechny nemocnice, polikliniky, ale i praktičtí lékaři musí mít uzavřenou smlouvu se zdravotní pojišťovnou. Stejně jako jinde na světě i v ČR jsou výborní specialisté a zařízení pro nejsložitější operace a léčby těch nejzajímavějších a nejzrádnějších nemocí. Tak jako v jiných státech i zde probíhají výzkumy, kterými se vědci snaží přicházet na nové léčebné metody a nové léky. Výzkumy probíhají nejčastěji v Univerzitních laboratořích, kde se nachází spousta odborníků.

2.8 Telekomunikace

Informační systém (IS) je soubor všech prvků, které se podílejí na šíření informací v prostoru a čase a na jejich použití a zpracování. Komunikační systém je odvozená podmnožina daných prvků zaměřená na přenos informací. Pokud by došlo k omezení nebo ohrožení daných systémů, mělo by to samozřejmě vliv na chod dalších systémů, které jsou s IS propojeny.

Riziko IS může být v dnešní hektické době na denním pořádku. Jako vždy je potřeba vzniku možného nebezpečí předcházet preventivním opatřením. Na bezpečnost se myslí hned od první fáze budování IS a to od použitého zařízení, softwaru až po samotné zaměstnance, kteří musí dodržovat přísná opatření. Míra rizika je zde oceněna finančním hodnocením v měnových jednotkách. Vše je definováno vztahem **riziko x ztráta**.

Strukturu systému lze rozdělit do třech základních částí:

- **procesní struktura**: popisuje logiku informačního systému. Popisuje data a určuje jim, kam a kdy se budou šířit, jak se s nimi bude zacházet, jak budou zpracovávána a uchovávána

- **technická struktura** (hardware): popisuje technické prostředky, zařízení a prostředí informačního systému

- **programová struktura** (software): představuje vytvořené programy a aplikace realizující procesní struktury na technické struktuře

Jednotlivé části s prvky struktury systému jsou vzájemně provázány. Když nastane výpadek jedné části, ovlivní tak části zbývající. Při výpadku procesní struktury ztrácí technická i programová struktura svůj význam.

2.9 Bankovní a finanční sektor

Finanční systém je soubor trhů, zákonů, regulací a technik. Je nedílnou součástí ekonomického systému a jsou na něm závislí spotřebitelé, podnikatelé i řadoví občané, proto musí pracovat velmi rychle, přesně a efektivně. Finanční systém je velmi ovlivnitelný hospodářskými, sociálními a jinými změnami ve státě.
O ochranu finanční sektoru v České republice se stará Ministerstvo financí, které zabezpečuje správný chod financí a rozděluje státní rozpočet pro další ministerstva.

3 Bankovní sektor jako významný segment infrastruktury v České republice

Bankovní systém je souhrn všech bank v daném státě a uspořádání vztahů mezi nimi. Banky jsou organizace, které mají povolení provádět bankovní operace. Banky přijímají vklady, poskytují úvěry a provádějí další bankovní služby. Jsou to tedy instituce specializované na obchodování s penězi.

Do roku 1990 byl v ČR bankovní sektor jednostupňový s významným monopolem Státní banky Československé, která plnila zároveň funkci centrální banky. Přechodem na tržní hospodářství vznikla potřeba přeměnit bankovní sektor na konkurující si podnikatelské subjekty a oddělit centrální banku jako nástroj státu k regulaci tohoto trhu.

V roce 1990 vzniká v ČR dvouúrovňový bankovní systém:

- Centrální banka ČNB
- Obchodní banky

CENTRÁLNÍ BANKA - ČNB

Centrální banka se v ČR nazývá Česká národní banka, má sídlo v Praze, jejím nejvyšším řídícím orgánem je bankovní rada ČNB v čele s guvernérem. Centrální banka pečlivě sleduje a analyzuje množství peněz v oběhu i vývoj všech makroekonomických veličin. Má svůj vlastní tým špičkových odborníků, kteří sledují jak ekonomiku ČR, tak celosvětový vývoj a jeho možné vlivy na nás. ČNB má nezávislé postavení na moci zákonodárné a výkonné, do její činnosti lze zasahovat pouze na základě zákona.

Základní úkoly centrální banky:

- určuje a prosazuje vnitřní a vnější měnovou politiku

- sleduje množství peněz v oběhu, emituje nové peníze a opotřebované nebo neplatné peníze stahuje z oběhu
- dohlíží nad činností obchodních bank, poskytuje bankám úvěry a ukládá jejich depozita
- spravuje státní rezervy ve zlatě a devizách
- obchoduje s cennými papíry
- je vrcholnou institucí bankovního dozoru

Jak již bylo zmíněno, jednou z hlavních funkcí centrální banky v tržní ekonomice je měnová politika. K jejímu provádění používá centrální banka řadu nástrojů.

Nástroje centrální banky

- diskont – základní úroková sazba v ekonomice. Pokud je v ekonomice vysoká inflace, centrální banka udržuje vysoký diskont. Pokud chce naopak centrální banka podporovat rozvoj podnikání, diskont sníží.
- repo sazba – úroková sazba centrální banky pro reeskont směnek. Obchodní banky eskontují směnky od klientů, pokud však banka potřebuje peníze, může tuto směnku reeskontovat, tedy prodat centrální bance.
- lombardní sazba – úroková sazba na úvěry obchodním bankám se zástavou cenných papírů
- povinné minimální rezervy – centrální banka předepisuje obchodním bankám určité procento z vkladů, které si musí u ní bezúročně uložit.
- pravidla likvidity – centrální banka určuje bankám, jaký mají mít vztah mezi aktivy a pasivy
- operace na volném trhu – centrální banka obchoduje s cennými papíry na burze a tím zvyšuje či snižuje množství peněz v oběhu

Centrální banka slouží také jako banka vlády (státu), tzn. vede příjmové a výdajové účty státního rozpočtu, může poskytnout státu úvěr, spravuje státní dluh. Centrální

banka dále reprezentuje stát pravidelným zasedáním Mezinárodního měnového fondu a Světové banky.

OBCHODNÍ BANKY

Obchodní banky jsou podnikatelské subjekty vyvíjející činnost za účelem dosažení zisku. Zisk banky je dán úrokovým rozpětím, tzn. rozdílem přijatých úroků z poskytnutých úvěrů a úroků vydaných vkladatelům, banky tedy získávají peníze levněji, než je pak půjčují. Dalším významným příjmem bank jsou různé poplatky za služby, které klientům poskytují.

Banky poskytují své služby na základě obdržené licence. Za udělení licence a její následnou kontrolu je zodpovědná ČNB.

Mezi základní bankovní služby patří :

- zakládání a vedení účtů
- bezhotovostní platební styk domácí i zahraniční
- vydávání platebních karet
- směnárenská činnost
- zprostředkování obchodů s cennými papíry
- devizové operace
- bezpečnostní schránky a ukládání cenností
- přímé bankovnictví

Mezi další finanční instituce na českém trhu patří stavební spořitelny a hypoteční banky. Stavební spořitelny nabízejí stavební spoření, hypoteční banky poskytují hypoteční úvěry. Tyto úvěry slouží převážně k pořízení nemovitosti nebo ke stavbě nového domu.

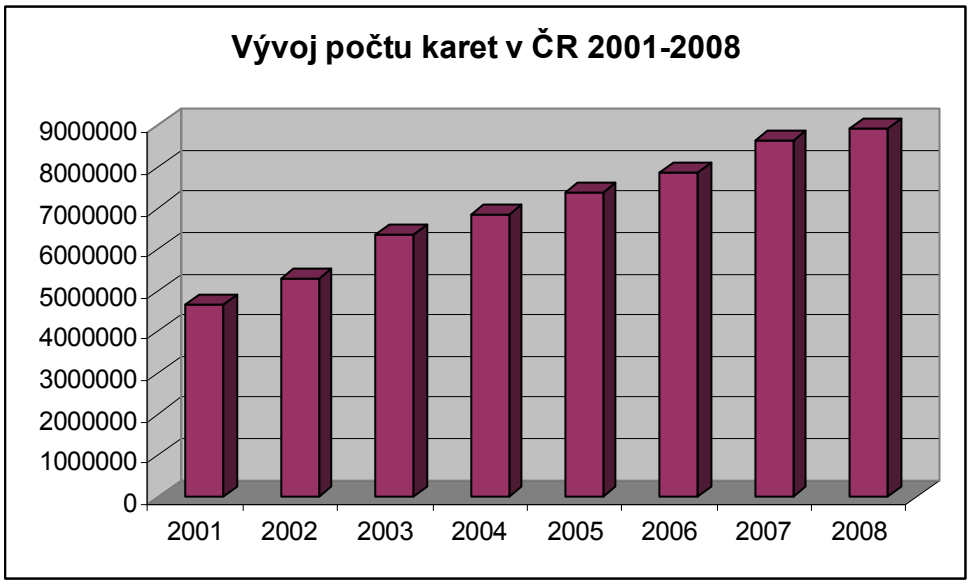
4 Způsoby ochrany bankovního sektoru

Bankovní sektor nám v dnešní době nabízí veliké množství produktů, které nám usnadňují život a stávají se jeho nedílnou součástí. Mezi tyto produkty patří platební karty. Platební karty nám umožňují nákup bez nutnosti nosit u sebe velkou hotovost. Dále pomocí nich můžeme vybírat hotovost z bankomatů a platit přes internet.

Vývoj platebních karet v ČR se datuje od roku 1988, kdy Živnostenská banka vydává první platební kartu. Jednalo se o dispoziční kartu k Tuzexovým účtům vedených v „bonech“. O rok později začíná Česká státní spořitelna vydávat svým klientům ke sporožirovým účtům karty k výběru z bankomatů.

Oblíbenost platebních karet roste, jsou instalovány nové bankomaty, v roce 1993 spouští Komerční banky první platební terminály. V roce 1998 patří mezi vydavatele sedm aktivních bank a počet vydaných karet dosahuje počtu 1 693 500 karet. V roce 2006 je na trhu bankovních karet 14 bank, v roce 2007 přibývá polská BRE Bank S.A., org. složka. Vedle bank vydává karty řada nebankovních subjektů.

Nárůst obliby platebních karet můžeme vidět na grafu vývoje počtu karet v letech 2001 – 2008. Počet karet se během osmi let zvýšil o více než 90%. Důvodem tohoto růstu byl rozšíření počtu bank, které vydávají platební karty ze 13 v roce 2000 na 19 v roce 2007.



Graf 1: Vývoj počtu karet v ČR v letech 2001 - 2008

V počtu karet na jednoho obyvatele, podle něhož je možné porovnávat rozvinutost kartového trhu a oblibu karet u spotřebitelů, patříme mezi nejrozvinutější trhy v Evropě.

	ČR		Velká Británie
	2000	2008	2005
Počet karet na obyvatele	0,43	0,87	2,36
Počet karet na obyvatele ve věku 15 – 64 let	0,6	1,22	3,5

tabulka 1: Počet karet na obyvatele

Avšak v porovnání se světem v bezhotovostních platbách zaostáváme. Český spotřebitel si zvyká na platbu kartou za nákupy zboží a služeb velice pomalu. V následující tabulce můžeme vidět, že výběry hotovosti jsou 3x větší než objemy plateb kartou. Ve světě je tomu právě naopak a bezhotovostní platby tvoří 65% kartových operací.

	Objem bezhotovostních plateb	Objem výběrů hotovosti
Svět	65%	35%
Česká republika	25%	75%

tabulka 2: Způsob využívání karet

Tyto hodnoty v ČR jsou způsobeny poměrně mladou historií platebních karet na našem území. Při pohledu na tabulku 1 : Počet karet na obyvatele a na graf 1 : Vývoj počtu karet v ČR je patrné, že platební karty si u nás získávají stále více příznivců a jejich počet neustále roste.

Ve své práci se budu zabývat platebními kartami, které se stávají bezesporu moderním trendem. Téměř každý ekonomicky aktivní člověk vlastní platební kartu.

Karty s sebou přinášejí nejen řadu výhod, ale také možná rizika, jako je například jejich zneužití. Zaměřím se tedy na jednotlivé druhy karet, jejich využití, bezpečnost a způsoby ochrany.

4.1 Druhy karet:

Platební karty se mohou třídit z různých hledisek, a to dle:

4.1.1 Vydávající asociace

- Eurocard / Mastercard / Maestro
- VISA
- American Express
- DCI (Diners‘ Club International)
- JCB (Japan Credit Bureau)

4.1.2 Typu zúčtování

- **Debetní** – k jejímu použití musíte mít na účtu dostatečnou sumu peněz k pokrytí platby či výběru z bankomatu. Peníze se Vám z účtu strhnou zpravidla krátce po provedení transakce.

- **Kreditní** – umožňuje nákup zboží a služeb na úvěr. Ke zúčtování obvykle dochází po určité době (zpravidla k určitému datu v měsíci). Zúčtování transakcí za Vás kryje finanční společnost (většinou banka), které pak musíte splácet vzniklý úvěr.

- **Charge** – podobně jako u kreditní karty dochází ke zúčtování transakcí po určité době (zpravidla k určitému datu v měsíci). Při zúčtování je třeba splatit dlužnou sumu peněz, nelze použít úvěr.

4.1.3 Použitelnosti

- **Domácí** (platby a výběry z bankomatů pouze v domácí zemi)
- **Mezinárodní karta**

4.1.4 Embossingu

- **embosované** - jedná se o platební karty s tzv. reliéfním (plastickým) písmem. Karty umožňují nakupovat i v prodejnách, které nejsou vybaveny elektronickým terminálem. Obchodník používá tzv. imprinter[3], který sejme otisk všech údajů vyražených na kartě a zákazník údaje potvrdí svým podpisem. Na základě toho pak obchodník zúčtuje platbu. Embosované karty lze používat na více místech než karty elektronické.

Obrázek 1: Imprinter

- **elektronické** – karty lze použít pouze v elektronických platebních terminálech, které umožňují on-line autorizaci a tudíž mohou být vydávány i méně bonitním klientům. Příklady zahrnují VISA Electron a Maestro.

3. [3] Mechanické zařízení umožňující přenesení informací z embosované karty na formulář potvrzující platbu kartou.

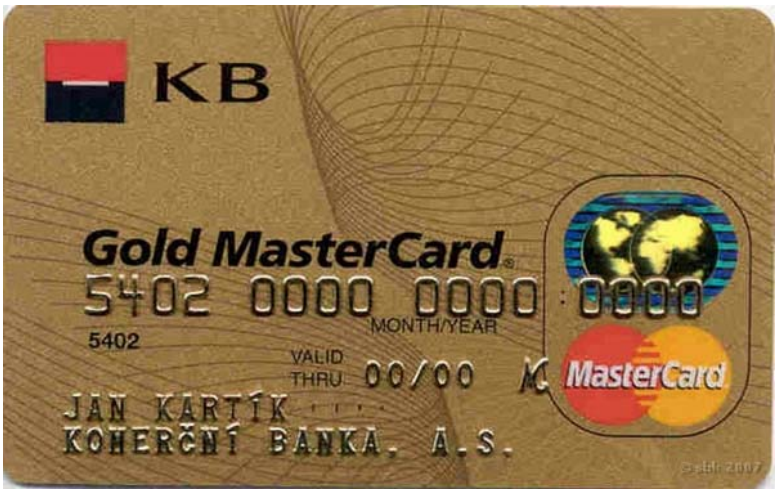
4.1.5 Bonity zákazníka

- **Standardní**

Standardní karta je platební karta vydávaná k běžnému bankovnímu účtu. Tato karta umožní svému majiteli výběr z bankomatů, bezhotovostní platbu na terminálech a platby přes internet.

- **Zlatá**

Zlaté karty jsou určeny pro prestižní klientelu. S tímto typem karty nezíská klient pouze platební kartu, ale také řadu exkluzivních výhod. Zlaté karta poskytuje vysoké finanční limity čerpání, různé druhy pojištění, slevy v hotelích a restauracích a autopůjčovnách po celém světě, předběžné odbavení na letišti a další výhody. Za tyto výhody musí klient ovšem ochotný platit roční poplatek, který se pohybuje mezi 3000 – 5000 Kč.



Obrázek 2: Zlatá karta MasterCard Komerční banky

- **Stříbrná**

Další kartou nabízenou českými bankami je karta stříbrná. Je podobná kartě zlaté s tím, že její výhody jsou menší. To se také odráží na ročním poplatku. Stříbrnou kartu lze pořídit za roční poplatek 1000 Kč. Tato karta je často také nazývána podniková, protože ji podniky využívají pro své zaměstnance.

Obrázek 3: Stříbrná karta MasterCard Komerční banky

- **Platinová**

Obrázek 4: Platinová karta VISA Živnostenské banky

Ještě o třídu výše než karta zlatá je karta platinová. Ze začátku se o platinovou kartu nedalo požádat a byla nabízena pouze nejlepším zákazníkům. Od roku 2000 je možnost

získat tuto kartu na požádání. Platinová karta je definovaná jako luxusní prestižní karta určená fyzickým osobám s nejvyššími nároky na špičkovou kvalitu služeb. Majitel této karty získá rozsáhlé cestovní a úrazové pojištění, které je platné celosvětově 24 hodin denně s vyššími limity pojistného plnění než u karty zlaté. Karta dále poskytuje výrazné slevy v mezinárodních hotelích a půjčovnách aut a umožňuje také vstup do VIP salonků na letištích. V České republice tuto kartu nabízí např. Živnostenská banka. Kartu může získat klient, který má u Živnostenské banky otevřený běžný účet v Kč nebo cizí měně s průměrným zůstatkem 1 000 000 Kč. Roční poplatek za vedení karty je 7 000 Kč.

- **Černá**

„Black card“ je určena pro nejnáročnější klientelu. Navazuje na platinovou kartu a nabízí ještě větší výhody. Držitel karty získává mimo jiné výhody exkluzivní právo při rezervaci vstupenek na významné sportovní akce a koncerty. V tuzemsku zatím černou kartu zatím žádná banka nenabízí.

Obrázek 5: „Black card“ American Express

4.1.6 Technologie (podle záznamu na kartě)

Dalším hlediskem, podle kterého můžeme rozdělit platební karty, je podle záznamu na kartě. Jedná se o karty s magnetickým proužkem, karty čipové a hybridní.

- **Karta s magnetickým proužkem**

Magnetický proužek se nachází na zadní straně platební karty a slouží jako médium pro záznam identifikačních údajů při elektronických transakcích. Funguje na principu magnetického záznamu, který se používá například u počítačových disket či magnetofonových kazet. Proužek obsahuje magnetické částice kovového základu schopných uchovávat údaje. Magnetický proužek má dvě nebo tři stopy pro záznam identifikačních dat. U platebních karet je zde elektronicky zaznamenáno číslo karty, její časová platnost, informace, zda se jedná o kartu tuzemskou nebo mezinárodní, zda je možné ji použít v platebních terminálech, v bankomatech nebo v obou zařízeních. Jsou zde i další doplňující údaje (bezpečnostní kód CVV[4] nebo CVC[5] a další). Celkem může být zaznamenáno až 1288 bitů.

- **Čipová karta**

Čipy v platebních kartách jsou multifunkční. Lze na ně nahrát nejrůznější informace od zdravotního stavu držitele karty přes elektronický podpis až po aplikace věrnostních programů, v jejichž rámci držitel karty například sbírá věrnostní body za nákupy v určité síti maloobchodních prodejen. Čipy jsou mimořádně cenné při vývoji nových způsobů akceptace karet a platebních metod bez fyzické přítomnosti karty. Poskytují efektivní nástroj ověření totožnosti držitele karty, zmenšují rizika plynoucí z ukládání citlivých dat v počítači a na jiných médiích a redukují náklady na certifikaci a distribuci digitální identifikace.

4. [4] Card Validation Value / Hodnota ověření karty. Název pro kontrolní kód používaný asociací VISA.
5.
6. [5] Card Validation Code / Kód ověření karty. Název pro kontrolní kód používaný asociací MasterCard.

U zrodu myšlenky zavedení čipové platební karty namísto karty s magnetickým proužkem stály karetní asociace Europay, MasterCard a VISA. Jedním z hlavních důvodů proč se hledala nová technologie, bylo rostoucí množství podvodů s platebními kartami. Test čipových karet ve Francii poté nastartoval mezinárodní diskuzi o standardu, který budou banky používat, aby byly karty, bankomaty a terminály vzájemně slučitelné. Tak vznikl tzv. **EMV standard** (zkratka zakládajících karetních asociací Europay, Master Card a VISA). Čipové karty, které tomuto standardu odpovídají, jsou někdy označovány právě jen zkratkou EMV. Čipová technologie umí zpracovávat data a spouštět programy, čímž poskytuje finančním institucím mnohem vyšší úroveň kontroly v oblasti řízení rizik. Hlavní devizou čipového zabezpečení je nemanipulovatelnost. Padělání vylučuje metoda autentifikace karty (CAM), zatímco zneužití zcizených čipových karet a terminálů zabrání metoda ověření držitele karty (CVM).

- **Hybridní karta**

Hybridní karty mají kromě čipu také magnetický proužek. Všechny čipové platební karty standartu EMV jsou vydávány jako karty hybridní. Lidé si často myslí, že banky vydávají karty čipové i karty hybridní, ale banky v České republice nabízejí svým klientům pouze karty, které obsahují jak čip tak magnetický proužek, tedy karty hybridní. Výjimkou jsou čipové karty neodpovídající standartu EMV, tedy neoznačené logem VISA nebo Mastercard. Mezi těmito specifickými produkty nalezneme i karty, které mají jenom čip. Vzhledem k množství platebních karet a množství akceptačních zařízení nemůže změna na čipovou technologii proběhnout jednorázově. Právě postupnost tzv. migrace na EMV si vyžádala kombinaci staré a nové technologie a tedy hybridní karty. Díky magnetickému proužku tak lze platební kartou zaplatit či vybrat peníze i tam, kde bankomat nebo terminál zatím nedisponuje čipovou technologií.

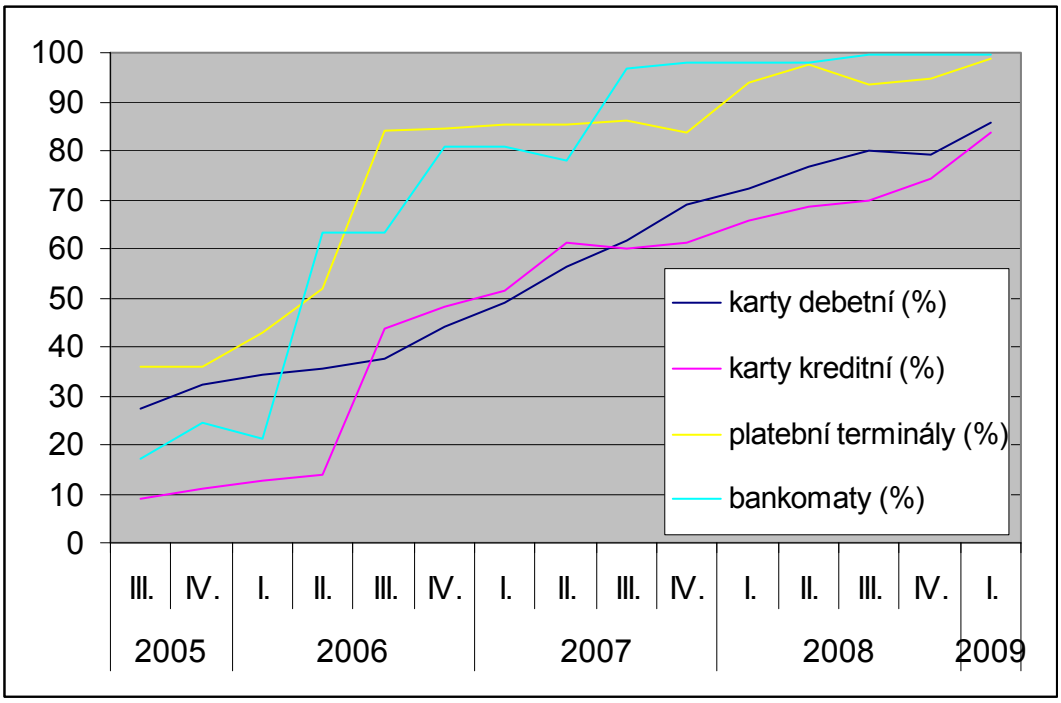
Migrace na čipovou technologii

V České republice byla historicky první čipovou kartou Maxkarta od Poštovní spořitelny. Tato karta však neodpovídá mezinárodním standardům EMV. První „pravou“ čipovou kartu, která splňuje standardy EMV, vydala Komerční banka v roce 2003. Původní termín, do kterého měly platební karty přejít na čipovou technologii, byl

leden 2005. To se nestihlo hned z několika důvodů. Hlavním důvodem jsou vysoké náklady na přeinstalování bankomatů a platebních terminálů. Zatímco ve Francie se stát aktivně podílí na financování konverze platebních karet na čipovou technologii, v ČR hradí banky veškeré náklady samy. Česká spořitelna, největší vydavatel platebních karet u nás, odhaduje, že vydávání nového typu karet a úpravy terminálů ji přijde na 450 milionů Kč. Celý přechod na novou technologii vyjde banky asi na miliardu korun.

V dnešní době je konverze u bankomatů prakticky dokončena a blízko dokončení je i u platebních terminálů. O něco málo pomalejší průběh u karet je dán ekonomickým přístupem bank spočívajícím v postupné výměně expirujících karet za čipové. Vzhledem k až tříleté expirační době mohou být některé karty vyměněny v průběhu příštích dvou let. Projekt SEPA (Single Euro Payment Area) sice stanoví určitý časový plán pro migraci na čipy, kdy by všechny karetní systémy měly odpovídat standardu EMV do konce roku 2010. Ovšem tento plán je závazný pouze pro země eurozóny. ČR jistě do roku 2010 do eurozóny nevstoupí, tzn. přechod českých bank na čipovou technologii je víceméně v jejich kompetenci.

V následující tabulce můžeme vidět konverzi na čipovou technologii od roku 2005.



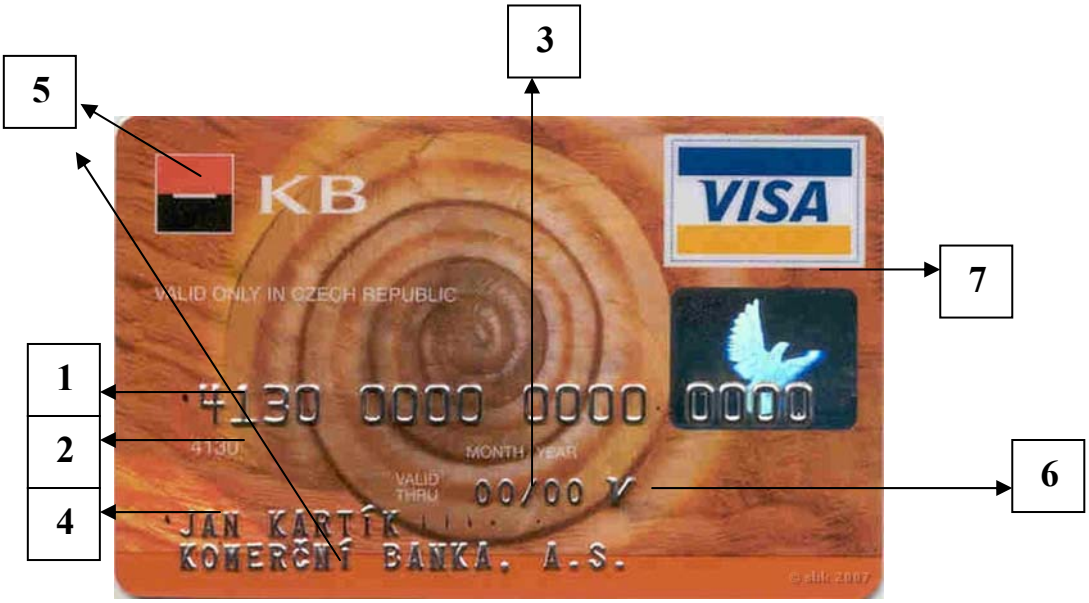
Graf 2: Konverze na čipovou technologii v ČR – vývoj od roku 2005 po kvartálech

4.2 Bezpečnost karet

Platební karty jsou vyráběny z odolných plastů a mívají standardní rozměry 85,5 mm x 54mm x 0,76mm. Karty jsou opatřeny grafickými a textovými symboly, které slouží k ověřování platnosti karet pohledovou kontrolou – jméno držitele, jméno vydávající banky, datum platnosti karty, značka karetní asociace, hologram, proužek s podpisem držitele, který porovnáním s podpisem na účtence umožní obchodníkovi ověřit držitelovu totožnost.

Na obrázku vidíme platební kartu Komerční banky : Bankokarta .

Jedná se o elektronickou platební kartu VISA Elektron s inteligentním čipem.



Obrázek 6: Bankokarta Komerční banky

Na přední straně platební karty jsou tyto bezpečnostní prvky :

1. **Číslo platební karty**

Číslo platební karty je na prvním řádku. První číslice (případně dvojčíslí) určuje druh karty. Tedy například číslo začínající čtyřkou nebo pětkou značí, že jde o odvětví bankovní či finanční (VISA, MasterCard). Dalších několik čísel (většinou pět) značí vydavatele karty. Posledních osm až třináct míst označuje klienta. Úplně poslední číslice má funkci kontrolní. Kontrolní funkce znamená, že pokud by byla omylem místo některé z číslic špatně zadána jiná, výpočet kontrolní číslice nebude souhlasit.

Toto platí pro většinu bankovních platebních karet, výjimkou jsou karty American Expressu. Ty mají trošku odlišné významy jednotlivých číslic.

Většina typů karet má číslo šestnáctimístné, výjimkou je American Express s patnácti číslicemi a Diners Club se čtrnácti. Obecně mohou existovat karty s třinácti až devatenácti číslicemi. Číslice jsou vyraženy ve skupinách, většinou po čtyřech, přičemž některá ze skupin nemusí být na kartě zobrazena. Dokonce Živnostenská banka nedávno začala vydávat elektronické platební karty Visa Electron, na kterých jsou vyobrazeny pouze čtyři poslední číslice z čísla karty. Je to opět z důvodu bezpečnosti.

U karet, na kterých je umístěn hologram[6], poslední čtyřčíslí zasahuje do tohoto ochranného prvku.

2. BIN

BIN (Bank Identification Number) je bankovní identifikační číslo, což je jedinečná série čísel přidělená kartovým platebním systémem hlavním členům asociace. BIN identifikuje typ kartového produktu a současně instituci, která kartu vydala.

3. Platnost karty

Na druhém řádku je vyznačena doba platnosti karty. Je to údaj vymezující období, kdy lze kartu použít. Na přední straně platební karty je uveden ve tvaru MM/RR a zároveň je uložen v elektronické podobě na magnetickém proužku nebo čipu. Když je na kartě tedy například uvedeno 03/09, platí karta do 31.3.2009.

4. Jméno držitele

7. [6] Laserem pořízený snímek, který vytváří trojrozměrný obraz

Na dalším řádku je uvedeno jméno a příjmení držitele karty. Držitel karty je fyzická osoba, které byla na žádost a se souhlasem majitele účtu vydána platební karta k používání. Podepsáním smlouvy se držitel karty zavazuje dodržovat obchodní podmínky vydavatele karty. Držitel karty je identifikován číslem karty (kartového účtu). Pod jménem držitele bývá zpravidla embosovaný název společnosti, k jejímuž firemnímu účtu je karta vydána.

5. Název a logo banky

Název a logo vydavatele karty bývá vyobrazeno v levém dolním rohu nebo v pravém horním rohu. Je to banka, úvěrová nebo jiná finanční instituce, která vydává platební kartu a má s držitelem karty smluvní vztah.

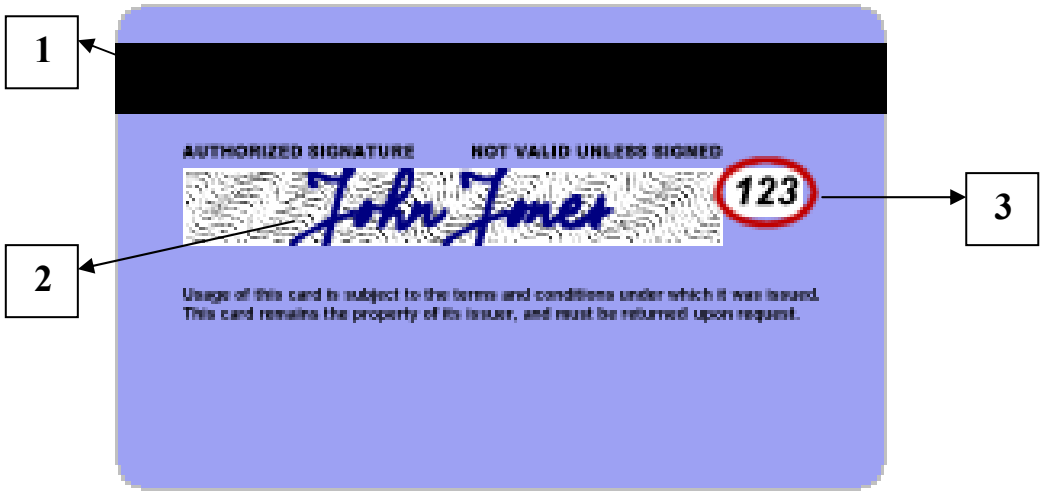
6. Embosovaný ochranný prvek

Ochranný prvek se u společností liší. U VISA se jedná o „letící v“. MasterCard používá spojené „MC“, karty JCB „J“, u Američan Expressu je to „AX“ a u Diners Clubu „DC“.

7. Název, logo a ochranný hologram karetní asociace

V pravé části karty je logo karetní asociace. Bývá ještě doplněno ochranným prvkem – hologramem (laserem pořízený snímek, který vytváří trojrozměrný obraz). Společnost American Express logo ani hologram na karty většinou neuvádí. Stejně tak i kartám společnosti Diners Club a elektronickým platebním kartám (např. VISA Electron, Maestro) hologram schází.

Zadní strana platební karty :



Obrázek 7: Líc platební karty

1. **Magnetický proužek**

Je součástí platební karty sloužící k záznamu elektronických údajů.

2. **Podpisový proužek**

Je určen pro záznam podpisového vzoru držitele karty. Tak, jak je zde podepsán, zákazník podepisuje stvrzenky při placení. Je zde jedna výjimka – u karet Maestro se od roku 2001 povinně používá PIN. Proti změně podpisu je proužek chráněn několika bezpečnostními technologiemi.

3. **Kód CVV** [7]

Bezpečností prvek určený k tomu, aby zabránil falšování nebo manipulaci s údaji na kartě. Je uložen na magnetickém proužku a vytištěn na podpisovém proužku karty.

8. [7] Card Validation Value / Hodnota ověření karty. Název pro kontrolní kód používaný asociací VISA.

Platební karty se často stávají terčem podvodníků. Zneužití karty poškozuje klienta, banku nebo obchodníka. Na ochraně platební karty má zájem její držitel, banka, obchodník a také karetní asociace.

4.2.1 Karetní asociace

Již karetní asociace, která kartu prostřednictvím banky vydává, může ovlivnit její ochranu. Jedná se bezpečnostní prvky (hologram, podpisový proužek, kód CVC), které jsem popsal v předchozí kapitole.

4.2.2 Držitel

Klient má bezpochyby zájem na ochraně platební karty, jelikož se jedná o jeho peníze. Ztráta nebo krádež je velice nepříjemná, ovšem karta může být zneužita, aniž by o ni držitel fyzicky přišel. Ne vždy je člověk dostatečně opatrný a tak je velká část podvodů způsobena nedbalostí samotného držitele karty . Stačí přitom dodržovat základní pravidla bezpečnosti.

Ke kartě se držitel musí chovat jako k hotovosti, být opatrný a nosit ji odděleně od dokladů. Klient banky spolu s kartou získává nejen právo ji užívat, ale i povinnosti zacházet s ní tak, jak banka stanoví ve svých Podmínkách.

Jednou ze základních povinností je, že „Držitel karty je povinen zajistit bezpečnost karty a zabránit prozrazení PIN další osobě. Držitel karty si nesmí PIN zaznamenat v žádné formě, která by jej další osobě umožnila odhalit a nesmí jej uchovávat společně s kartou“.

Nejvíce případů zneužití se děje právě tak, že se podvodníkovi podaří ukrást kartu spolu s PINem a pak mu stačí pouze přijít k bankomatu a prostředky vybrat. Za chybu klienta se v tomto případě nepovažuje pouze to, že měl PIN napsán dokonce přímo na kartě, ale i to, že ho měl ve stejném zavazadle jako kartu. Klient v těchto případech pak nese plnou odpovědnost za výběry, které se uskutečnily do stoplistace karty, přičemž se často stává, že držitel karty krádež či ztrátu nestačí nahlásit dříve, než dojde ke zneužití. Téměř všechny ilegální výběry se totiž uskutečňují do dvou hodin po získání karty neoprávněnou osobou.

V dnešním světě mobilních telefonů si lidé PIN karty nejčastěji zaznamenávají do adresáře telefonu. Zde je důležité, aby nenosili přístroj v kabelce či tašce spolu s kartou a pokud toto již dělají, aby PIN měli uložen zašifrovaně v podobě fiktivního telefonního čísla. Dále je velice účelné mít pro případ krádeže či ztráty poznamenáno telefonní spojení do banky, na kterém je možné provést stoplistaci. K této operaci potřebujeme ale ještě číslo karty, která byla ukradena. Obě tato čísla je tedy třeba si někam zaznamenat, aby v případě nutnosti nebyl zbytečně poskytnut zloději čas navíc ke zneužití karty.

V bankovních Podmínkách se dále píše, že „V případě skončení platnosti karty je její Držitel povinen znehodnotit ji (přestřihnout na dvě části) a uschovat po dobu šest měsíců. Pokud Majitel účtu kartu nepřestřihne a neuschová, nese odpovědnost za takové škody, které mají souvislost s tím, že tak neučinil."

Riziko prozrazení PINu

Získání PINu neoprávněnou osobou se nemusí odehrát pouze jeho krádeží. Zloději jsou v tomto směru velice vynalézaví a tak již jsou známy případy, kdy přes klávesnici ATM nalepili průsvitnou tepelně citlivou folii či ji posypali jemným práškem na pečení a poté byli schopni PIN zjistit. Asi pro podvodníky nejjednodušší způsob, jak si PIN k později kradené kartě opatřit, je nenápadné nahlížení přes rameno klienta při zadávání PINu. Výrobci bankomatů se snaží těmto nekalým praktikám předcházet a tak mění sklon klávesnic do vodorovné polohy a více naklánějí přední stěnu ATM, aby znesnadnili případnou instalaci kamery tak, aby si jí zákazník nevšiml. Proti instalaci folie na klávesnici jsou zaváděny plastické klávesy, které mají velký zdvih a jsou dostatečně daleko od sebe.

Žádné takovéto opatření však nezabrání nahlížení přes rameno tomu, kdo zadává PIN do klávesnice bankomatu či platebního terminálu. Zde by si dotyčný měl dávat veliký pozor a snažit se co nejvíce rukou nebo tělem kód uchránit před cizími zraky. V souvislosti s tímto je třeba upozornit, že zvláště v obchodech je riziko prozrazení PINu velké. Neexistuje tam totiž povinnost ani zvyklost odstupu od toho, kdo platí, jako je tomu na úřadech, v bankách, na poště nebo právě u bankomatu.

Fishing

Fishing (rybaření = chytání údajů) je další nástraha kladená na držitele karty Jedná se o nevyžádaný e-mail vypadající jako od kartové společnosti Visa, který vybízí ke sdělení údajů o účtu a kartě včetně její platnosti a PIN. Jako důvod žádosti o tyto soukromé informace je údajné podezření na zneužití karty. První případ fishingu se v ČR objevil na začátku roku 2004. Podobně se snaží získat údaje i lidé, kteří se vydávají za obchodní zástupce. Majitel karty by na takovéto výzvy neměl v žádném případě reagovat.

Libanonská smyčka

Již celkem starý trik je tzv. libanonská smyčka. Jde o jednoduché pouzdro se smyčkou, často z magnetofonové pásky, uchycené ve štěrbině pro vsunutí karty. Tato smyčka kartu zachytí a nepustí ji zpět ven z bankomatu. Klient sice obdrží peníze, ale kartu ne a podvodníci spoléhají na to, že si bude myslet, že bankomat ji zadržel a brzy odejde. Pokud se takto skutečně stane, zloděj přistoupí k bankomatu a kartu i se zařízením jednoduše vyndá. Pak již nenásleduje nic jiného, než neoprávněné výběry, popřípadě platby u obchodníků. PIN se zloději buď podařilo zjistit již při typování do klávesnice, nebo udělal to, že poradil držiteli kary ať zadá PIN znovu, že poté karta jistě vyjede.

Tato metoda se nazývá podle Libanonců, kteří ji úspěšně zavedli již na počátku 90. let v USA. Obranou proti tomuto ze strany majitele karty je snad jediné: neopouštět bankomat, pokud odmítá kartu vydat a zavolat do příslušné banky o pomoc.

4.2.3 Obchodník

Role obchodníka v ochraně platební karty je poněkud omezená. I přesto může obchodník dodržováním základních pravidel zabránit použití padělané nebo odcizené karty.

Při převzetí karty od zákazníka by si měl obchodník ponechat kartu v ruce až do dokončení celé transakce. Kromě platnosti karty kontroluje obchodník i ostatní bezpečnostní prvky a může tak předejít akceptaci padělané karty. Při provádění platby

sleduje obsluha zákazníka, jestli se nechová zákazník podezřele a nemůže se tedy jednat o podvodníka. Při nutnosti podpisu obchodník kontroluje, zda se shodují podpisy na prodejním dokladu a na platební kartě. V případě podezření, že se nejedná o právoplatného majitele karty, může obsluha požádat zákazníka o průkaz totožnosti k ověření shody s údaji uvedenými na kartě.

Z mé vlastní zkušenosti mohu říci, že prodejci často vůbec nekontrolují shodu podpisů na kartě a na účtence. Málokterý obchodník také věnuje pozornost zkoumání bezpečnostních prvků karty. Je pravda, že některé padělky mohou být velice kvalitní a obchodník falsifikát neodhalí. Ale přesto by měl obchodník dbát výše uvedených kroků, které ho stojí jen minimum úsilí a může tak předejít zneužití platební karty.

4.2.4 Banky

Část ochrany, kterou může zajistit banka, spočívá již v počátku vztahu banky a budoucího držitele karty. Další část závisí na technologii, pro kterou se banka rozhodne, a v neposlední řadě je důležitá i dostatečná bezpečnost bankomatů.

Obdržení nové karty klientem

Další okamžik, který časově následuje po podepsání smlouvy s klientem o užívání nové karty, je její obdržení. Již v tomto momentě se mohou objevit problémy s krádežemi. Riziko zcizení nastává v případě, že jsou karty klientům zasílány poštou. . Opatření proti tomuto riziku je jednoduché a v České republice ho provádějí, dá se říci, všechny banky. Karty jsou vydávány výhradně na pobočce a pouze PIN je sdělován pomocí bezpečnostní obálky zasílané poštou doporučeně.

Čip

Použitá technologie velice ovlivňuje bezpečnost karty. V posledních letech je realizován pomalý přechod na čipovou technologii, která by měla být mnohem bezpečnější z hlediska padělání a získávání údajů z karty. Současné platební karty jsou hybridní. Obsahují tedy jak čip tak magnetický proužek, u kterého je riziko zneužití větší. Snahou většiny bank v ČR i ve světě v současné době je přejít na čisté čipové karty, což s sebou ale nese nemalé finanční náklady.

Card skimming

Další oblastí, kterou by banka měla zajistit, jsou zabezpečené bankomaty. Bezpečnostní vybavení bankomatů je třeba stále zdokonalovat s rostoucí vynalézavostí podvodníků. Ti jsou v posledních letech schopni nainstalovat do čtecí štěrbiny bankomatu svou vlastní čtečku, pomocí které celý magnetický proužek okopírují a vzápětí díky tomu vyrobí vlastní falešnou kartu. PIN nasnímají při typování pomocí miniaturní kamery či fotoaparátu a pak již nezbývá, než díky této nové padělané kartě a originálnímu PINu provést nelegální výběry nebo platby v obchodech.

Přestože se případů skimmingu v ČR zatím neobjevilo nijak značné množství, snaží se ho již nyní banky řešit, protože za používání falešné karty zaplatí ona. Banka v tomto směru zavádí různá opatření. Mezi nimi jsou i nové bankomaty, které jsou vybaveny senzory schopnými zachytit cizí objekt vložený do čtečky a upozornit na to řídící centrum. Další možností je naprogramování bankomatu tak, aby se v případě problému sám na určitou dobu vypnul, přičemž se předpokládá, že podvodník ATM opustí v domnění, že se porouchal. V neposlední řadě je na některých bankomatech možné aktivovat funkci, která způsobí vibraci karty při jejím vtahování do ATM. Pomocí vibrace je znemožněno načtení obsahu magnetického proužku nelegálně nainstalovaným čtecím zařízením.

4.2.4.1 Přínosy čipové karty

U karty čipové je PIN vyžadován pro každou transakci, tedy PIN nebudete potřebovat pouze k výběru z bankomatu, ale i k platbě v obchodě. V případě krádeže nebo ztráty karty je tak vysoce eliminována možnost zneužití karty.

Další výhodou je, že čipová karta je v podstatě počítač. Zatímco u magnetické karty jsou pasivně načteny informace z magnetického proužku stejně jako třeba z magnetofonové pásky, čipová karta si s platebním terminálem „aktivně povídá“ a jeho prostřednictvím může počítač v platební kartě buď sám rozhodnout o realizaci či zamítnutí transakce, nebo si vyžádat spojení se svojí bankou a přímo si ověřovat údaje v bance, včetně aktuálního zůstatku na vašem účtu. Čipová karta zkrátka aktivně rozhoduje o tom, kdy transakce bude nebo nebude provedena a dokonce může

rozhodnout o tom, že sama sebe zablokuje. Banky tak mají daleko větší možnosti zabránit zneužívání karet i jejich oprávněnými držiteli například v případě, kdy klient je na svém účtu v mínusu a stále se pokouší platební kartou platit.

Mezi další rozdíl magnetické a čipové karty patří skutečnost, že u čipové karty není možné vytvořit plnohodnotný padělek. Lze sice zkopírovat obsah magnetického proužku, ale na vytvoření duplikátu čipu by bylo třeba vynaložit náklady mnohonásobně vyšší, než bude zisk z provedeného podvodu. Čipová karta tedy omezuje riziko tzv. skimmingu – vytvoření falešné karty.

4.2.4.2 Nevýhody čipových karet

Musíme si ovšem přiznat, že čipové karty přinášejí pro jejího držitele i některé nevýhody. Asi největší z nich je nutnost pamatovat si PIN k platební kartě a používat jej u každé transakce. Zejména při platbách v kavárnách a restauracích pocítíme úpadek komfortu, protože v podnicích, kde nemají přenosný platební terminál, musíme následovat číšníka k terminálu, kde zadáme svůj PIN. I v těchto nepříjemných situacích se člověk musí chovat rozumně a myslet na bezpečnost. Neměl by tedy sdělovat PIN obsluze nebo jiné přítomné osobě, když se mu k terminálu nechce.

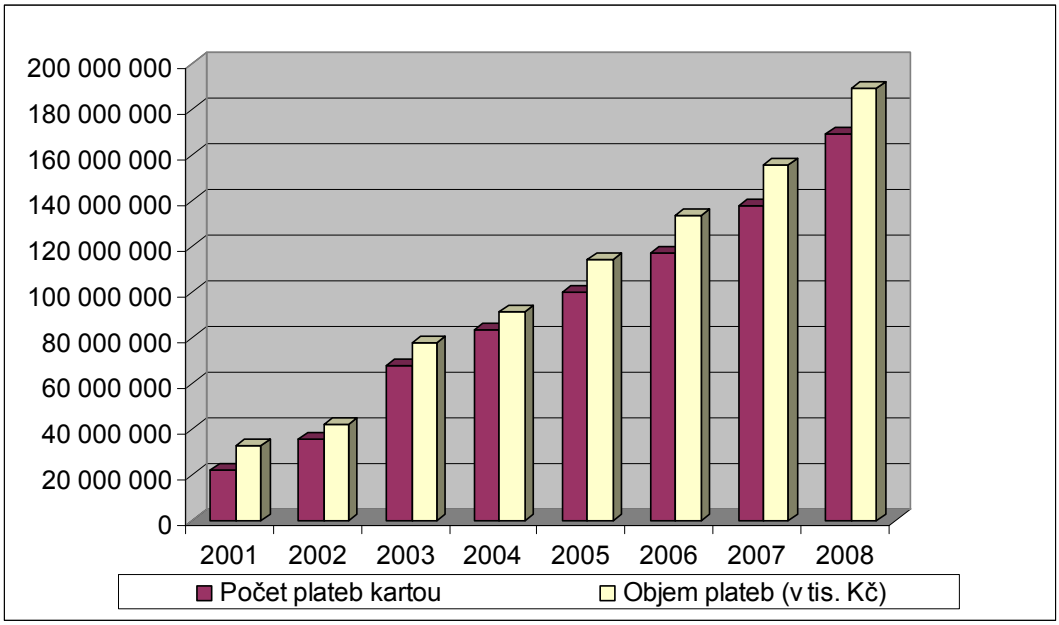
Obrázek 8: Přenosný platební terminál

Dalším problémem je prodloužení doby transakcí na některých terminálech. V České republice je několik desítek tisíc terminálů a ne všechny disponují dostatečně rychlým

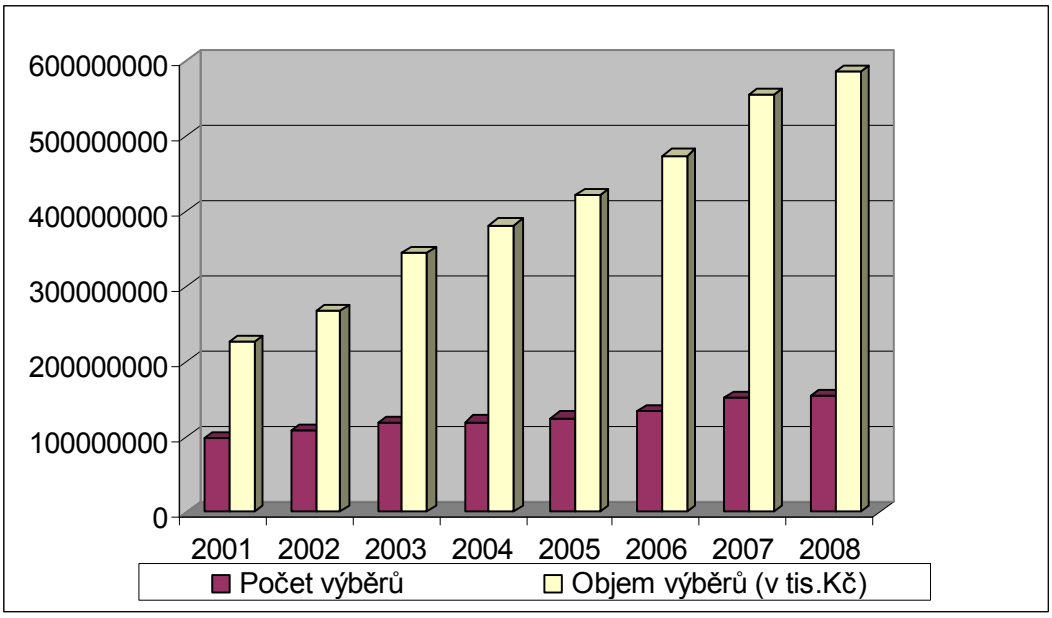
hardwarem a softwarem. Je nepředstavitelné a ekonomicky nemožné vyměnit všechna tato zařízení za nové a moderní. Proto se může stát, že finanční operace čipovou kartou bude na některém starším terminálu trvat déle, než by trvala karty s magnetickým proužkem. Jelikož terminál nedisponuje novou technologií, úplně nestíhá při komunikaci s čipovou kartou její myšlenkové pochody a dochází k prodloužení doby transakce. Vyšší bezpečnost, kterou poskytuje čipová technologie, ale určitě stojí za trochu trpělivosti při delším trvání transakce.

4.2.4.3 Statistiky zneužití platebních karet

Při nárustu trendu platebních karet rostou samozřejmě i objemy transakcí. Jak již bylo dříve zmíněno, v ČR převládají výběry nad platbami kartou. Více platebních operací samozřejmě skýtá více příležitostí pro podvody. Jak je vidět na následujících grafech, objem plateb kartou od roku 2001 vzrostl šestkrát a objem výběrů se zvýšil zhruba třikrát.



Graf 3: Počet a objem plateb kartou



Graf 4: Počet a objem výběrů

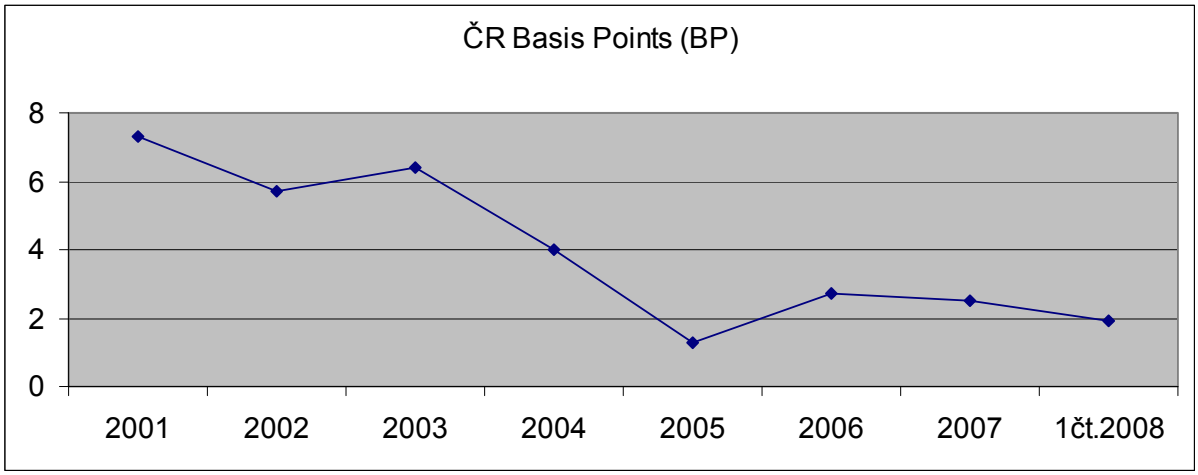
Sdružení pro bankovní karty ČR (SBK) uveřejňuje na svých stránkách roční statistiku tzv. Basis Points (BP). Jedná se o číselné vyjádření poměru objemu podvodných případů hlášených vydavatelskými bankami k celkovému objemu transakcí provedenými kartami v ČR za příslušný rok.

$$\frac{\text{Hlášené podvody v Kč}}{\text{Objem transakcí v Kč}} \text{‰}$$ [8]

Obrázek 9: Basis Points

Objem transakcí zahrnuje platby i výběry všemi kartami systémů VISA a MasterCard (vydanými v ČR i v zahraničí) provedené na území ČR. Basis Points je sestaveno na základě oficiálních statistik asociací VISA, MasterCard a SBK.

9. [8] mezinárodní vyjádření v Basis Points znamená stonásobek v %



Graf 5: ČR Basis Points

Jak vidíme na grafu 5: ČR Basis Points kleslo zneužití platebních karet mezi roky 2003-2004 o 2,4 bodu, což je o 37 %. V dalším roce opět ubývalo počtu zneužití ze 4 bodů na 1,3 bodu. Oproti roku 2004 to byl pokles o 67,5 %. Následující rok dochází k mírnému nárůstu podvodů na 2,7 bodu, ale v letech 2007 a v 1. čtvrtletí 2008 klesl zhruba na stejnou hodnotu jako v roce 2005. Z uvedených údajů můžeme vyčíst, jak zavádění čipové technologie snižuje množství zdařených podvodů s platebními kartami. Nová technologie je tedy účinnou zbraní proti nekalým operacím s kartami. Chrání finanční prostředky držitele karty a vydávajícím bankám snižují náklady na kompenzaci škod způsobených podvodníky. Jelikož je konverze na čipovou technologii u bankomatů a platebních terminálů téměř dokončena a v následujících letech by měla být dokončena i migrace samotných karet, mohou banky pomalu bilancovat, zda se jim prostředky, vynaložené do čipové technologie, vyplatí.

Pomocí lineární regrese jsem odhadl objemy transakcí provedených platebními kartami v budoucích 10 letech. Výsledky v jednotlivých letech jsem násobil průměrným Basis Points před realizací čipové technologie (v letech 2001 – 2004: průměr činil 5,85) a průměrným Basis Points v letech, kdy probíhá implementace čipové technologie (2005-2008 : 2,1). Vynásobením objemů v letech 2009 – 2018 Basis Points jsem získal objemy podvodů 690,9 mil. Kč v případě nečipové technologie a 248 mil. Kč v letech, kdy už byla čipová technologie využívána. Rozdíl činí 442,87 mld. Kč. V příštích deseti letech by tedy čipová technologie měla bankám ušetřit ztráty z podvodů téměř ve výši půl miliardy Kč. Celkové náklady při přechodu na čipovou technologii bankovní ústavy odhadují na 1 miliardu Kč. Nová technologie tedy v příštích 10 letech vrátí téměř polovinu investic do ní vynaložených. Když k tomu ještě přičteme snížení podvodů

v posledních 4 letech, které již bankám „ušetřilo“ peníze, zdá se být čipová technologie správnou cestou k omezení zneužití platebních karet.

5 Návrhy na zkvalitnění bankovního sektoru

Čipová technologie se v současné době jeví jako optimální forma ochrany platebních karet před jejich zneužitím. Ovšem jen aplikace nové technologie nezajistí dostatečnou ochranu. Velkou roli při zneužití karet sehrává také držitel karty a banka.

Držitel karty

Při převzetí karty by si měl majitel přečíst pravidla vydávající banky a seznámit se s nejčastějšími praktikami podvodníků. V mnoha případech totiž držitelé karty přicházejí o peníze jen díky své nevědomosti. Nejdůležitější je podle mého názoru ochrana PINU. Při platbě kartou či vybírání z bankomatu je dobré být opatrný a PIN zadávat na klávesnici tak, aby ho nikdo jiný nemohl vidět. PIN by si držitel karty měl pamatovat a v žádném případě ho nemít v peněžence nebo dokladech, kde má uschovanou i platební kartu. Při ztrátě nebo odcizení je karta snadno zneužitelná, protože případný pachatel má v rukou jak kartu tak PIN. Dále by měl mít držitel karty u sebe telefonní číslo instituce, která kartu vydala a kde se dá karta zablokovat.

Banka

Vydávající banka je zodpovědná za ochranu svých bankomatů. Instaluje na své přístroje ochranné prvky, které brání zneužití. I přesto dochází k případům, kdy je držitel karty okraden přímo u bankomatu. Dostane se například do situace, kdy mu bankomat odmítá vydat kartu. Může to být cílený útok podvodníka, který čeká až majitel karty od automatu odejde pro pomoc. V těchto případech by pomohlo, kdyby na bankomatu byl telefonní kontakt, kde by držiteli karty dokázali poradit.

Další slabinu vidím v bankomatech, které jsou umístěny v budovách bank a je k nim přístup 24 hodin denně. Mimo otevírací hodiny banky stačí ke vstupu projet magnetickým proužkem karty přístrojem umístěným na vstupních dveřích. Rozsvícené světýlko na přístroji a zvukový signál dává znamení, že jsou dveře odemčeny. A majitel karty může přistoupit k bankomatu. Zatímco na bankomatu uvnitř jsou nainstalovány

ochranné prvky, přístroj na dveřích není nijak chráněn. Přitom ke vstupu je nutné použití magnetického proužku, u kterého je snadné okopírovat data na něm uložená. Proto je nutné ze strany bank věnovat zvýšenou pozornost zařízení, které umožňuje vstup do prostoru s bankomatem.

Závěr

Tato diplomová práce se zabývala tématem „Ochrana bankovního sektoru jako segmentu kritické infrastruktury“.

Na počátku práce byly vymezeny tři hlavní cíle. První z nich spočívá v teoretickém popisu problematiky kritické infrastruktury. Druhým cílem je seznámení s vybranou oblastí bankovního sektoru a její analýza. Poslední cíl je zaměřen na vytvoření návrhu na příslušná opatření spojená se zvýšením ochrany dané oblasti.

V první zcela teoretické části se práce zabývá popisem základních pojmů z oblasti kritické infrastruktury. Čtenář je seznámen s nejdůležitějšími pojmy a je mu přiblížena problematika týkající se dané oblasti. První s cílů byl tedy splněn již v úvodní kapitole.

Druhá kapitola je tvořena popisem jednotlivých segmentů kritické infrastruktury. Segmenty jsou postupně stručně charakterizovány a jsou nastíněna rizika, kterým jsou dané segmenty vystaveny a měla by se jim věnovat větší pozornost.

Třetí část práce podrobněji představuje bankovní sektor, který je jedním ze segmentů kritické infrastruktury.

Čtvrtá kapitola se zabývá stručnou charakteristikou a následnou analýzou vybrané oblasti bankovního sektoru. Na základě provedené analýzy jsou aplikovány statistické metody. Dosažené výsledky jsou v této kapitole interpretovány a je patrné, jak může být zkoumaná oblast efektivně zabezpečena. Tímto je splněn druhý z určených cílů práce.

V poslední kapitole jsou sepsány návrhy a doporučení, které mají zlepšit ochranu zkoumané oblasti. Náplň této kapitoly byla i třetím cílem stanoveným cílem. Domnívám se proto, že v úvodu stanovené cíle byly naplněny.

Seznam použité literatury

Literatura

[1] ROUDNÝ, R., LINHART, P. Krizový management I. ochrana obyvatelstva, mimořádné události.1.vyd. Pardubice: Univerzita Pardubice, 2004. ISBN 80-7194-674-5.

[2] ROUDNÝ, R., LINHART, P. Krizový management III. Teorie a praxe rizika. Pardubice: Univerzita Pardubice, 2007. ISBN 80-7194-924-8.

[3] PROCHÁZKOVÁ. D. a ŘÍHA, J. Krizové řízení. Praha: MV – GŘ HZS ČR, 2004. ISBN 80-86640-30-2.

[4] BROUN, L. Application of Internet Technology to Enhance International Civil – Military Emergency Planning (CMEP). In: Sborník Současnost a Budoucnost krizového managementu. 3. konference. Praha 2000

[5] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 1/2004

[6] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 3/2005

[7] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 4/2005

[8] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 1/2006

[9] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 4/2006

[10] SBK – Sdružení pro bankovní karty: Cardmag – magazín SBK, No 2/2007

Internet

[11] Česká spořitelna, OBCHODNÍ PODMÍNKY České spořitelny, a.s., pro vydávání a používání debetních a předplacených karet

URL : <http://www.csas.cz/banka/content/inet/internet/cs/OP_DK_actual.pdf>

[12] Platební karta a její používání

URL : <http://www.financnivzdelavani.cz/webmagazine/page.asp?idk=318>

[13] Karty s magnetickým pruhem

URL : <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>

[14] Druhy platebních karet – iDnes.cz

URL:<http://finance.idnes.cz/viteze.asp?r=viteze&c=A001025_000001_viteze_118>

[15] Druhy platebních karet a zúčtování – Finance

URL : < http://www.sfinance.cz/osobni-finance/informace/platebni-karty/druhy-karet-zuctovani/>

[16] Čipové karty a vše o nich – FinExpert

URL : < http://www.finexpert.cz/Autori/Cipove-karty-a-vse-o-nich/sc-48-sr-1-a-16871/default.aspx>

[17] Výroční zpráva SBK 2005

URL:<http://www.bankovnikarty.cz/vyrocni_zprava/vyrocni_zprava_sbk_2005.pdf>

[18] Výroční zpráva SBK 2008

URL:<http://www.bankovnikarty.cz/vyrocni_zprava/vyrocni_zprava_sbk_2008.pdf>

[19] VALÁŠEK, J., Ochrana obyvatel 2007

URL:<
http://www.btv.cz/download/Ochrana_kriticke_infrastruktury_2007.pdf>

Kritická infrastruktura a možné hrozby, s.399

[20] HRDINA, P., Ochrana obyvatel

URL:<
http://www.btv.cz/download/Ochrana_kriticke_infrastruktury_2007.pdf>

Vzájemné vztahy v kritické infrastruktuře, s.73

[21] SBK – Bankovní karty

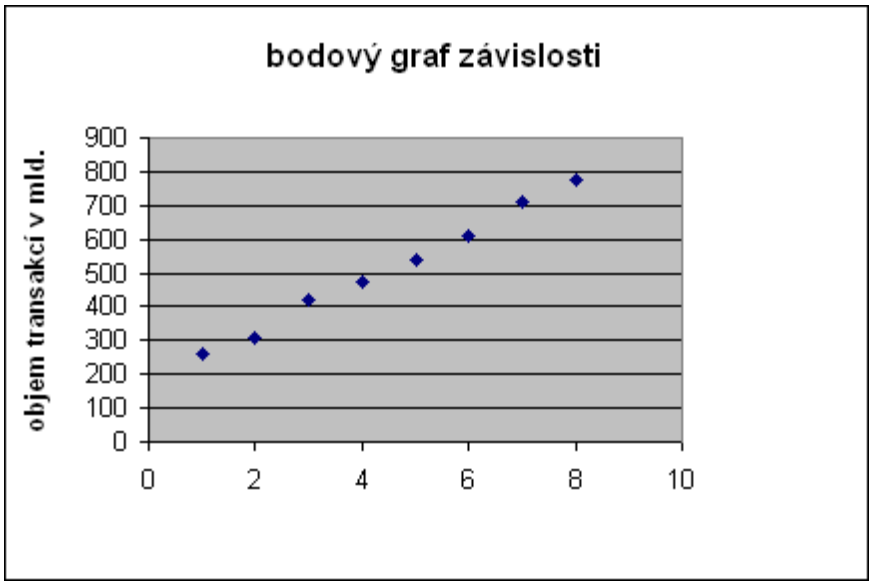
URL:< http://bankovnikarty.cz/web_sbk/main_page/czech/main_cz.htm >

Seznam příloh

Příloha A

Tabulka udávající objem transakcí v Kč v roce 2001 - 2008

rok	2001	2002	2003	2004	2005	2006	2007	2008
pořadí let :)	1	2	3	4	5	6	7	8
objem v mld.	259,75	310,79	422,44	474,16	536,76	608,94	710,82	776,45



$$B = \frac{n\sum_{i=1}^{n} y_i x_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}$$

$$A = \frac{1}{n}\left(\sum_{i=1}^{n} y_i - B\sum_{i=1}^{n} x_i\right)$$

x_i	y_i	(x_i)^2	x_i*y_i	y_i*y_i
1	259,75	1	259,75	67470,06

	2	310,79	4	621,58	96590,42		B	74,2756
	3	422,44	9	1267,32	178455,6		A	178,2736
	4	474,16	16	1896,64	224827,7			
	5	536,76	25	2683,8	288111,3			
	6	608,94	36	3653,64	370807,9			
	7	710,82	49	4975,74	505265,1			
	8	776,45	64	6211,6	602874,6			
Σ	36	4100,11	204	21570,07	2334403			

odhad: $\hat{Y} = A + Bx$

$\hat{Y} = 178,2736 + 74,2756\ x$

Odhad objemu	2009	2010	2011	2012	2013	2014
v mld.	846,7539	921,0295	995,30512	1069,58071	1143,856	1218,132

2015	2016	2017	2018	Σ
1292,408	1366,683	1440,9587	1515,23429	11809,94

	čip.technologie		bez čip. technologie
Basis Points	2,1		5,85
objem podvodů v mil. Kč	248,0088		690,8816
rozdíl		442,87279	