Univerzita Pardubice

Fakulta ekonomicko-správní

Ochrana kritické infrastruktury se zaměřením na bankovní sektor v České republice

Aneta Černá

Bakalářská práce
2014

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aneta Černá**
Osobní číslo:	**E11955**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management ochrany podniku a společnosti**
Název tématu:	**Ochrana kritické infrastruktury se zaměřením na bankovní sektor v České republice**
Zadávající katedra:	**Ústav regionálních a bezpečnostních věd**

Zásady pro vypracování:

V bakalářské práci bude nejprve obecně pojednáno o kritické infrastruktuře, jejím vymezení, významu a jednotlivých prvcích. Hlavní oblastí zájmu poté bude zkoumání kritické infrastruktury bankovního sektoru v České republice, její možné ohrožení a formy ochrany.

Zásady:
- Rešerše literatury.
- Formulace cíle práce a hypotézy, volba metod.
- Vymezení kritické infrastruktury.
- Význam a ochrana prvků kritické infrastruktury.
- Kritická infrastruktura bankovního sektoru v České republice, ohrožení, formy ochrany.
- Formulace závěru, návrhy, doporučení.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 30 stran**

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

Seznam odborné literatury:

FRIEBERG, F. Bankovnictví. Vyd. 1. Praha: ČVUT, 2000. 181 s. ISBN 80-01-02106-8.
MOZGA, J. a kol. Kritická infrastruktura společnosti. Vyd. 1. Hradec Králové: Gaudeamus, 2008. 156 s. ISBN 978-80-7041-299-2.
SEKERKA, B. Řízení bankovních rizik. Vyd. 1. Praha: Profess Consulting, 1998. 203 s. ISBN 80-85235-56-0.
ŠENOVSKÝ, M., ADAMEC, V., ŠENOVSKÝ, P. Ochrana kritické infrastruktury. Vyd. 1. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. 141 s. ISBN 978-80-7385-025-8.

Vedoucí bakalářské práce: **Ing. Zdeněk Matěja**
Ústav regionálních a bezpečnostních věd

Datum zadání bakalářské práce: **1. října 2013**
Termín odevzdání bakalářské práce: **30. dubna 2014**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Ivana Kraftová, CSc.
vedoucí ústavu

V Pardubicích dne 1. října 2013

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena 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 30. 4. 2014 Aneta Černá

PODĚKOVÁNÍ

Tímto bych ráda poděkovala svému vedoucímu bakalářské práce panu Ing. Zdeňku Matějovi za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Práce se zabývá problematikou ochrany prvků kritické infrastruktury. Problematika kritické infrastruktury je nejprve nastíněná obecně, jsou zde vysvětleny základní pojmy. Dále je v práci podrobněji popsán jeden z prvků kritické infrastruktury, a to bankovní sektor České republiky. V práci je analyzováno internetové bankovnictví, jeho možné ohrožení a dostupné možnosti ochrany internetového bankovnictví komerčních bank České republiky.

KLÍČOVÁ SLOVA

Kritická infrastruktura, ochrana kritické infrastruktury, bankovní sektor, internetové bankovnictví

TITLE

Protection of critical infrastructure, focusing on the banking sector in Czech Republic

ANNOTATION

This Bachelor´s work deals with a topic of protection of critical infrastructure. Problems of critical infrastructure and their protection are generally described in the first part of this word, there are described basic terms. Next part deals with of one of the elements of critical infrastructure- banking sector in the Czech Republic. Last part analyzes internet banking, protection options internet banking for commercial banks in the Czech Republic.

KEYWORDS

Critical infrastructure, protection of critical infrastructure, banking sector, internet banking

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

BRS	Bezpečnostní rada státu
ČR	Česká republika
ČNB	Česká národní banka
ČSOB	Československá obchodní banka
EKI	Evropská kritická infrastruktura
EU	Evropská unie
IB	Internetové bankovnictví
IS	Informační systém
KB	Komerční banka
KI	Kritická infrastruktura
Sb.	Sbírka zákonů
SBČS	Státní banka československá

ÚVOD

Tématem bakalářské práce je ochrana kritické infrastruktury se zaměřením na bankovní sektor v České republice.

Každý den se setkáváme s prvky kritické infrastruktury, ať už je to energetika, vodní hospodářství, potravinářství a zemědělství, zdravotní péče, doprava, komunikační a informační služby, finance a státní správa, nouzové služby nebo veřejná správa. Na těchto oblastech jsme ve velké míře závislí. Prvky kritické infrastruktury nám přinášejí značný pokrok, usnadňují nám život. Na druhé straně ale tento pokrok přináší řadu problémů. Vznikají nová rizika, která mohou vést až ke krizové situaci a mají tak negativní dopad na obyvatelstvo nebo životní prostředí.

Proto je důležité snažit se těmto možným problémům předcházet. Díky vymezení kritické infrastruktury má každý stát vytvořený vlastní systém ochrany, kterým se bude řídit v případě vzniklého nebezpečí.

První kapitola této bakalářské práce se bude zabývat popisem kritické infrastruktury a základních pojmů spojených s kritickou infrastrukturou, jako je veřejná kritická infrastruktura, evropská kritická infrastruktura, subjekty a objekty kritické infrastruktury, mimořádná událost, hrozba, riziko a další.

V druhé kapitole budou přiblíženy jednotlivé prvky kritické infrastruktury, které jsou nezbytné pro bezpečné fungování České republiky.

Třetí kapitola bude obsahovat podrobnější rozebrání bankovního sektoru České republiky, jako jednoho z prvků kritické infrastruktury.

Čtvrtá kapitola bude zaměřena na ochranu bankovního sektoru, zvláště pak na v dnešní době velmi využívanou oblast elektronického bankovnictví, formy elektronického bankovnictví a způsoby jeho zabezpečení v České republice.

Poslední pátá kapitola se bude zabývat zabezpečením internetového bankovnictví, dostupnou ochranou internetového bankovnictví a způsoby zabezpečení jednotlivých bank v České republice. Dále budou v této kapitole uvedeny závěry a doporučení, které by mohly vést ke zvýšení ochrany zkoumané oblasti bankovního sektoru.

Cílem práce je obecný popis problematiky kritické infrastruktury. Dále popis vybrané oblasti bankovního sektoru a jeho analýza. Třetím cílem je vyvození doporučení, které by přispělo k ochraně dané oblasti.

1 KRITICKÁ INFRASTRUKTURA

Kritická infrastruktura je v legislativě České republiky poměrně nový pojem. Oficiálně byla definována a vymezena až po implementaci směrnice Rady Evropské unie za dne 8. prosince 2008 do novely zákona č. 240/2000 Sb. o krizovém řízení (krizový zákon). Novelizovaný krizový zákon nabyl platnosti k 1. lednu 2011, s tím, že pojem kritická infrastruktura byl oficiálně zakotven v legislativě ČR [21].

V této kapitole budou vysvětleny základní pojmy v souvislosti s kritickou infrastrukturou.

1.1 Infrastruktura

Infrastruktura představuje v obecném smyslu slova množinu prvků, které jsou strukturované, navzájem propojené a poskytují určitému celku rámcovou podporu. Tento pojem se obvykle používá pouze pro struktury, které jsou vytvořeny uměle. Termín infrastruktura se používá v různém smyslu v řadě odvětví. Nejvíce se termín užívá v ekonomii, kde popisuje fyzickou infrastrukturu jako třeba budovy nebo silnice. Infrastruktura může být zřízena a spravována státem nebo soukromím sektorem [18].

Infrastrukturu lze rozdělit na veřejnou a kritickou.

1.1.1 Veřejná infrastruktura

V ČR se veřejnou infrastrukturou rozumí, podle zákona č. 183/2006 Sb., o územním plánování a stavebním řádu, pozemky, stavby a zařízení, a to:

- dopravní infrastruktura, jako například stavby pozemních komunikací, drah, vodních cest, letišť a s nimi souvisejících zařízení;
- technická infrastruktura, kterou jsou vedení a stavby a s nimi provozně související zařízení technického vybavení, např. vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby a zařízení pro nakládání s odpady, energetická vedení, trafostanice, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovody;

- občanské vybavení, což jsou stavby, zařízení a pozemky sloužící například pro vzdělání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, ochranu obyvatelstva;
- veřejné poradenství, zřizované nebo užívané ve veřejném zájmu [24].

1.1.2 Kritická infrastruktura

Kritické infrastruktury zasahují do mnoha sektorů ekonomiky, včetně bankovnictví a financí, dopravy a zásobování, energetiky, zdravotnictví, komunikačních služeb, potravinářství a komunikací, stejně jako do primární funkce vlády.

Definice používaná v České republice: Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažné důsledky pro bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva [24].

1.2 Subjekty a objekty kritické infrastruktury

Subjekty kritické infrastruktury jsou vlastníci a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby kritické infrastruktury. Subjekty odpovídají zejména za ochranu prvků KI a jsou povinny především vypracovat plán krizové připravenosti subjektu KI, umožnit provádění kontroly plánu krizové připravenosti a ochrany prvku KI, umožnit přístup na pozemky a do míst, kde se prvek nachází a bez zbytečného odkladu informovat o skutečnostech týkajících se organizačních, výrobních či jiných změn. Subjekty kritické infrastruktury jmenují orgány krizového řízení, kterými jsou ministerstva a další správní úřady [9].

Objekty (prvky) kritické infrastruktury jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické infrastruktury [24].

1.3 Další pojmy související s kritickou infrastrukturou

Mimořádná událost

Je škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také haváriemi, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací [25].

Krizová situace

Situace, které všeobecně nastávají, pokud nežádoucí situace svým rozsahem překročí určité všeobecné hranice. Dle zákona č. 240/2000 Sb., o krizovém řízení a dle zákona č. 110/1998 Sb., o bezpečnosti České republiky je krizová situace mimořádná událost, při které je vyhlášen stav nebezpečí, nouzový stav, stav ohrožení státu nebo stav válečný [26].

- stav nebezpečí – tento stav může vyhlásit vláda ČR, jsou- li ohroženy životy, zdraví nebo majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu, a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury [26].
- nouzový stav – tento stav může vyhlásit vláda ČR v případě živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného nebezpečí, které ve velkém rozsahu ohrožují životy, zdraví nebo majetek, anebo vnitřní pořádek a bezpečnost [23].
- stav ohrožení státu – stav ohrožení státu může na návrh vlády vyhlásit parlament ČR, je-li bezprostředně ohrožena svrchovanost státu nebo územní celistvost státu anebo jeho demokratické základy [23].
- stav válečný – tento stav vyhlašuje parlament ČR. Válečný stav je vypuknutí ozbrojeného konfliktu, a to bez ohledu na to zda byla vypovězena válka. Ústava ČR tento stav definuje jako situaci, kdy je ČR napadena, nebo je-li třeba plnit mezinárodní smluvní závazky o společné obraně proti napadení [19].

Fyzická ochrana kritické infrastruktury

Je soubor bezpečnostních opatření plánovaných a realizovaných k ochraně subjektů a objektů kritické infrastruktury před útoky fyzických osob [12].

Hrozba

Je jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby [16].

Riziko

Je možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit [16].

1.4 Význam kritické infrastruktury

Význam kritické infrastruktury je zejména pro zajištění bezpečnosti státu, fungování ekonomiky, výrobních, nevýrobních systémů a služeb, dále pro fungování veřejné správy a základních životních potřeb obyvatelstva. Poškození nebo narušení kritické infrastruktury má hospodářské, politické, sociální, psychologické dopady a také dopady životní prostředí. Ohrožení a hrozby pro kritickou infrastrukturu jsou terorismus, přírodní pohromy, nedbalost obsluhy, průmyslové havárie a nehody, dále počítačové hackerství, nebo organizovaný zločin a trestná činnost obecně [2].

Z pohledu funkcionality se kritická infrastruktura dělí na základní infrastrukturu (energetika, doprava, dodávky vody), socio-ekonomickou infrastrukturu (potraviny, zdravotní péče, záchranné služby, bankovnictví, poštovní služby, veřejná správa a socio-kulturní infrastrukturu, která zajišťuje a udržuje soudržnost společnosti [12].

Kritická infrastruktura byla definována jak na úrovni členských států, tak na evropské úrovni, proto dále lze kritickou infrastrukturu dělit na národní a evropskou KI.

1.5 Evropská kritická infrastruktura

Evropská kritická infrastruktura (EKI) je dle Směrnice Rady 2008/114/ES vymezena následovně: EKI je kritická infrastruktura nacházející se v členských státech, jejíž narušení nebo zničení by mělo závažný dopad pro nejméně dva členské státy [17].

V české legislativě tento pojem definuje krizový zákon: EKI je kritická infrastruktura nacházející se na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie [26].

Dle příkladu ČR lze usuzovat, že z této definice vychází a orientuje se na stanovení EKI na národní úrovni. Kritické infrastruktury jsou úzce provázané a vzájemně závislé.

1.6 Ochrana kritické infrastruktury

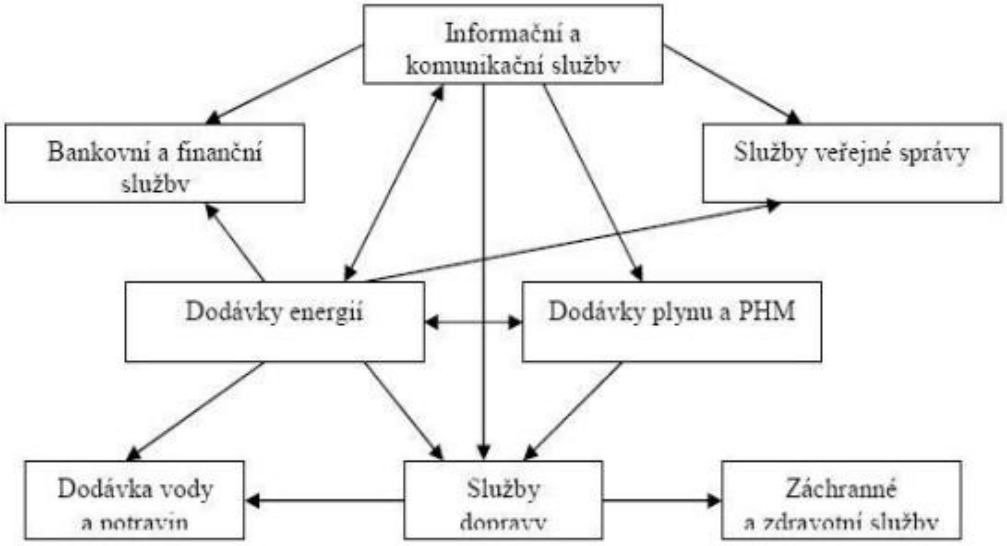
Ochrana kritické infrastruktury znamená proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů kritické infrastruktury a vazeb mezi nimi [10].

Úkolem společnosti je kritickou infrastrukturu chránit tak, aby fungovala za jakékoliv situace. Na ochraně kritické infrastruktury se podílí stát, soukromé subjekty a obyvatelstvo.

Cíle ochrany kritické infrastruktury jsou zabránit narušení nebo destrukce KI, případně minimalizovat dopady výpadků tak, aby případný výpadek postihl minimum obyvatelstva. Dále zabezpečení ochrany strategických a životních zájmů státu (základních funkcí státu) a jeho hospodářské, sociální a bezpečnostní stability. Ochrana KI je součástí programového prohlášení vlády [2].

Prvky kritické infrastruktury jsou navzájem provázané, jak znázorňuje obrázek číslo 1.

U kritické infrastruktury samotné je důležitá její komplexnost a provázanost jednotlivých prvků. Prvky nacházející se uvnitř kritické infrastruktury jsou propojeny vzájemnými vazbami. Shluky prvků nazýváme uzly, jež jsou důležitou součástí celé sítě kritické infrastruktury. Při poškození či výpadku některého z uzlů by došlo k vážnému narušení funkčnosti celé sítě a ke zhroucení kritické infrastruktury. Tyto uzly by tak měly být jedním z nejlépe chráněných míst kritické infrastruktury [12].



Obrázek 1: Kritická infrastruktura společnosti

Zdroj:[12]

1.7 Struktura kritické infrastruktury

Každá infrastruktura se skládá z několika odlišných položek, které jsou podstatné pro její funkčnost; důležité jsou objekty a sítě, které tvoří liniové struktury v území. Kritická infrastruktura v území je takový systém páteřních infrastruktur, které jsou velmi důležité pro chod území a zároveň jsou velmi zranitelné od očekávaných pohrom v daném území. Výběr se provádí na základě speciálních matematických metod, např. metod multikriteriální analýzy či metod operační analýzy založených na hledání kritické cesty [25].

2 OBLASTI KRITICKÉ INFRASTRUKTURY ČR

Zpráva Výboru pro civilní nouzové plánování z června 2007, schválena Bezpečnostní radou státu (BRS) usnesením č. 30 z července 2007 stanoví 9 oblastí KI a 37 podoblastí.

Oblasti kritické infrastruktury ČR jsou:

- energetika,
- vodní hospodářství,
- potravinářství a zemědělství,
- zdravotní péče,
- doprava,
- komunikační a informační služby,
- finance a státní správa,
- nouzové služby,
- veřejná správa.

Tyto oblasti následně blíže popisuji.

2.1 Energetika

Jedním z rozhodujících a nejdůležitějších prvků kritické infrastruktury je oblast energetiky. Bez energie se nedokážou obejít další prvky kritické infrastruktury, např. systém dodávky vody, přepravní síť, komunikační a informační systém, bankovní a finanční sektor apod., proto je důležité tuto oblast chránit. Ekonomika i každodenní běžný život lidí jsou závislí na souvislých dodávkách energie. Ministerstvo průmyslu a obchodu je úředním a správním orgánem pro energetiku.

V energetice jsou určovány prvky v těchto odvětvích:

- elektřina,
- zemní plyn,
- tepelná energie,
- ropa a ropné deriváty [18].

Pro teroristy je jedním z nejsnazších cílů poškodit systém dodávky energie pro obyvatele demokratického státu a tak poškodit celkový plynulý chod. Bez energie totiž v dnešní době pracovat nelze. Spousta hlavních systémů má samozřejmě zabudovaný záložní zdroj, ale i ten má stanovenou dodávku energie.

2.2 Vodní hospodářství

Do vodního hospodářství jsou řazeny:

- zásobování pitnou a užitkovou vodou,
- zabezpečení a správa povrchových vod a podzemních zdrojů vody,
- systém odpadních vod [18].

Vodní hospodářství je v České republice významným oborem s dlouholetou tradicí. Zajištění zásobování obyvatel pitnou vodou a zmírnění důsledků extrémních jevů počasí (povodně, sucho) patří mezi nejdůležitější úkoly vodohospodářství. Mimo zásobování pitnou vodou je ČR důležitým správcem významné říční sítě. Nejvýznamnějšími toky jsou Labe s Vltavou v Čechách, Morava s Dyjí na jižní Moravě a Odra s Opavou na severu Moravy a ve Slezsku.

Dodávky vody a kanalizace může selhat vlivem různých událostí, např. vlivem technologických závad, lidskou chybou, přírodních pohrom, haváriemi zařízení či objektů nebo teroristickým útokem.

Ministerstvo zemědělství je správcem většiny vodních toků v ČR. Ministerstvo životního prostředí se pak stará o zabezpečení a správu povrchových a podzemních vod.

2.3 Potravinářství a zemědělství

V současné době je společnost vystavena mnoho rizikovým faktorům, ke kterým patří i různé chemické škodliviny a karcinogenní látky v životním prostředí vznikající v důsledku lidské činnosti. Proto se zvyšuje zájem o bezpečnost potravin, které spotřebitelé konzumují.

Potravinářství a zemědělství zahrnuje tyto klíčové oblasti:

- produkci potravin,
- péči o potraviny,

- zemědělskou výrobu [18].

Problematiku potravinářství a zemědělství řeší v rámci České republiky Ministerstvo zemědělství. Prioritou ministerstva zemědělství je zajištění dostatečného množství kvalitních, plnohodnotných a bezpečných potravin pro všechny obyvatele státu.

2.4 Zdravotní péče

Poskytování zdravotní péče a ochrana veřejného zdraví patří mezi základní funkce státu, které stát zabezpečuje pro občany České republiky. Ministerstvo zdravotnictví je ústředním orgánem státní správy pro zdravotní péči a ochranu veřejného zdraví.

Do zdravotní péče patří tyto složky:

- přednemocniční neodkladná péče,
- nemocniční péče,
- ochrana veřejného zdraví,
- výroba, skladování a distribuce léčiv a zdravotnických prostředků [18].

K možným nebezpečím, která mohou ohrozit chod nemocnice, patří fyzické poškození budov (požár, povodně, bouře), výpadky kvůli místnímu narušení (výpadku) infrastruktury (elektrický proud, dopravní cesty), hromadný příjem pacientů, migrace z oblastí postižené katastrofou, vznik epidemie následkem dlouhodobého výpadku zásobování vodou. Pro snížení hrozby je přerušení provozu cílené zlepšení odolnosti zdravotnického zařízení vůči možným rizikům.

2.5 Doprava

Jedním z klíčových odvětví ekonomiky České republiky je oblast dopravní infrastruktury. Doprava je společně s energetikou považována za základ hospodářské prosperity státu a její ohrožení by mohlo způsobit narušení bezpečnosti, ekonomické a sociální stability společnosti a zachování nezbytného rozsahu dalších základních funkcí státu při krizových situacích. Poptávka po přepravě osob a zboží stále roste. Úkolem veřejné správy je proto vytvořit právní a ekonomické podmínky pro poskytování veřejných služeb a podnikání v dopravě. K tomu je nezbytné zajistit a trvale udržovat odpovídající dopravní infrastrukturu.

Dopravu lze rozdělit na:

- silniční,
- železniční,
- leteckou,
- vnitrozemskou vodní [18].

Tyto systémy mohou být ohroženy přírodními katastrofami, velkým dopravními nehodami, technologickými haváriemi objektů nacházejících se v blízkosti systémů, kriminálními činy, teroristickými útoky a válkou.

2.6 Komunikační a informační služby

Komunikační a informační služby zastávají v systému kritické infrastruktury ČR důležitou úlohu. Nepostradatelná je pro státní, podnikatelskou i soukromou sféru. Zajišťuje komunikaci mezi prvky kritické infrastruktury státu tak, aby se informace dostaly ve správný čas a na správné místo. Pokud by se tak nestalo, může toto selhání znamenat katastrofální následky pro obyvatelstvo a způsobit nemalé škody na majetku nebo na dalších prvcích KI státu.

Mezi komunikační a informační služby lze zařadit:

- služby pevných telekomunikačních sítí,
- služby mobilních telekomunikačních sítí,
- radiová komunikace a navigace,
- satelitní komunikace,
- televizní a rádiové vysílání,
- poštovní služby,
- přístup k internetu a k datovým službám [18].

2.7 Finance a státní správa

Finančním sektorem a jeho ochranou se zabývá Ministerstvo financí. Zabezpečuje správný chod financí a rozděluje pro další ministerstva státní rozpočet. Česká národní banka jako ústřední banka České republiky vykonává dohled nad finančním trhem.

Do této oblasti kritické infrastruktury patří:

- správa veřejných financí,
- bankovnictví,
- pojišťovnictví,
- kapitálový trh [18].

Veškeré tyto prvky jsou důležité pro chod ekonomiky státu a pro jeho ekonomické zdraví. Narušení tohoto prvku může způsobit pokles nebo naopak zvýšení cen, finanční nestabilitu, znehodnocení měny atd. Státní ekonomika by měla fungovat i při velkých katastrofách, kde je přesto možné, že se na nějaký čas zastaví její chod. Toto by přesto nemělo ohrozit fungování celého finančního sektoru a způsobit tak větší problémy.

2.8 Nouzové služby

Další z oblastí kritické infrastruktury jsou nouzové služby.

Mezi subjekty této oblasti kritické infrastruktury jsou řazeny většinou všechny složky ochrany a obrany státu. Jedná se o:

- Hasičský záchranný sbor České republiky a příslušné jednotky požární ochrany,
- Policie České republiky (vnitřní bezpečnost a veřejný pořádek),
- Armáda České republiky (zabezpečení obrany),
- radiační monitorování včetně podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření,
- předpovědní, varovná a hlásná služba [18].

Tyto subjekty byly zařazeny do kritické infrastruktury z toho důvodu, že slouží veřejnosti a jejich hlavním úkolem je mimo jiné je chránit obyvatelstvo, jejich zdraví, život a majetek.

Hasičský záchranný sbor ČR a Policie ČR má v kompetenci ministerstvo vnitra. O armádu ČR se stará ministerstvo obrany.

2.9 Veřejná správa

Do působnosti veřejné správy je řazena:

- státní správa a samospráva,
- sociální ochrana a zaměstnanost (soc. zabezpečení, stát. soc. podpora, soc. pomoc),
- výkon justice a vězeňství [18].

V době krizové situace je nutné zabezpečit základní funkce státu, dodržování zákonů a základních lidských práv a svobod. Je nutné, aby příslušné státní úřady koordinovaly záchranné práce. V případě krizové situace musí být funkční justiční orgány a musí fungovat zabezpečení věznic, občané musí dostávat své finanční jistoty a chod státu musí fungovat dál.

Sociální zabezpečení, státní sociální podporu a sociální pomoc v České republice zajišťuje ministerstvo práce a sociálních věcí. Výkonem justice a vězeňství je pověřeno ministerstvo spravedlnosti.

3 BANKOVNÍ SEKTOR ČR JAKO PRVEK KRITICKÉ INFRASTRUKTURY

Bankovnictví patří v dnešní době mezi odvětví s nejvyšší dynamikou rozvoje. Je jedním ze základních pilířů každé ekonomiky. Bez kvalitně fungujícího bankovního systému není možné docílit výraznějšího ekonomického pokroku. Proto vyspělá ekonomika potřebuje vyspělý bankovní systém, ale je tomu i naopak. Činnost bank se řídí zákonem č. 21/1992 Sb., o bankách.

Bankovní soustava je souhrn všech bank v daném státě a uspořádání vztahů mezi nimi. Až do 2. ledna 1990 v Československé republice fungoval jednostupňový bankovní systém s výrazným monopolem Státní banky československé (SBČS). V současné době existuje v České republice dvoustupňový bankovní systém [6].

Základní prvek bankovní soustavy jsou banky. Banky patří mezi instituce, jejichž hlavní oblastí činnosti jsou operace s penězi a obchody s nimi. S existencí a fungování bank jsou tedy peníze neodmyslitelně spojeny. Banky shromažďují dočasně volné peněžní zdroje a přerozdělují je. Banky tedy jsou prostředníky mezi nabídkou peněžních úspor a poptávkou po nich [8].

V České republice existuje dvoustupňový bankovní systém:

- centrální banka
- obchodní banky

První stupeň tedy tvoří centrální banka a druhý stupeň obchodní banky a spořitelny. Funkci centrální banky plní Česká národní banka. Funkci obchodních bank plní např. ČSOB, GE, KB… Banky druhého stupně tvoří výkonnou složku, které přijdou do kontaktu s klienty. ČNB plní funkci ústředního orgánu bankovnictví.

Činnost bank a spořitelen je zpravidla univerzální, protože poskytují veškeré bankovní služby pro své klienty. Klienti si mohou libovolně zvolit jakoukoliv obchodní banku nebo spořitelnu. Banky i spořitelny jsou povinny dodržovat bankovní tajemství o poskytnutých bankovních službách a obchodních operací.

Banky se od sebe mohou lišit některými podmínkami (např. při poskytování úvěrů), musí se ale řídit všeobecně platnými pravidly, které vyhlašuje Česká národní banka.

3.1 Česká národní banka

ČNB je centrální bankou českého státu a má sídlo v hlavním městě Praze. Má sedm regionálních poboček, které se nachází v Praze, Ústí nad Labem, Českých Budějovicích, Plzni, Hradci Králové, Brně a Ostravě. Nejvyšším řídícím orgánem je bankovní rada ČNB, jejímiž členy jsou guvernér, dva viceguvernéři a čtyři další členové bankovní rady. Všechny členy bankovní rady jmenuje prezident ČR. Současným guvernérem je Miroslav Singer.

ČNB má postavení ústředního orgánu státní správy v oblasti měny, bankovnictví a vydávání obecně platných předpisů. Je právnickou osobou, která usměrňuje peněžní trh z měnových hledisek, reguluje činnost bank a spořitelen bankovními ekonomickými nástroji, emituje peníze a hospodaří podle zásad stanovených vládou. Její postavení a funkce jsou především měnově řídící a nikoliv podnikatelské. ČNB nepracuje na komerčních principech. Její činnosti se řídí zákonem České národní rady č. 6/1993 Sb. ze dne 17. prosince 1992 o České národní bance platným od 1. května 2002 [4].

3.1.1 Funkce a cíle České národní banky

Mezi nejdůležitější funkce a cíle ČNB patří:

- zajištění měnové stability,
- podpora hospodářské politiky vlády vedoucí k udržitelnému hospodářskému růstu,
- podpora otevřeného tržního hospodářství,
- určování měnové politiky,
- emise bankovek a mincí,
- správa měnové rezervy ve zlatě a v devizách,
- řízení oběhu peněz, platebního styku a zúčtování bank, zajištění rozvoje a efektivnosti platebních systémů,
- vedení účtů státního rozpočtu, spravování státního dluhu,

- rozvoj bankovního systému ČR, vykonávání dohledu nad činností bank, poboček zahraničních bank a konsolidačních celků,
- spolupráce s ústředními bankami jiných států a mezinárodními organizacemi z finančního sektoru,
- obchod na finančních trzích, především se státními cennými papíry [15].

3.1.2 Nástroje České národní banky

ČNB disponuje řadou nástrojů, pomocí kterých plní své funkce, cíle a měnovou politiku. Tyto nástroje lze členit na přímé (administrativní, omezující volné tržní hospodářství) a nepřímé, které využívají tržních zákonů a plošně působí na ostatní subjekty finančního trhu.

Přímé nástroje České národní banky mají velký vliv na finanční hospodářství, proto jich banka využívá jen výjimečně a na přechodnou dobu. K těmto nástrojům patří:

- pravidla likvidity,
- povinné vklady,
- úvěrové kontingenty.

Mezi nepřímé nástroje centrální banky patří:

- diskontní sazba,
- repo sazba,
- lombardní sazba,
- operace na otevřeném trhu,
- povinné minimální rezervy,
- konverze a swapy [3].

3.1.3 Nezávislost České národní banky

Česká národní banka je do značné míry nezávislá na politických organizacích, aby mohla volně realizovat měnovou politiku. Měnová politika pak vede k dlouhodobé cenové stabilitě a neinflačnímu hospodářskému růstu. Nezávislost České národní banky je zakotvena v zákoně o ČNB č.6/1993.

I přes nezávislost musí být politika ČNB stále průhledná a veřejnost a politické subjekty jsou o ní průběžně informovány. Česká národní banka pořádá četné přednášky, přispívá do laického i odborného tisku a vydává pravidelnou zprávu o inflaci [8].

3.1.4 Bankovní regulace a dohled

Pro bankovní sektor je ve všech vyspělých zemích, tak i v ČR, typická přísnější míra regulace, než je tomu v ostatních odvětvích národního hospodářství.

Bankovní regulace a dohled se zaměřuje na čtyři prvky:

- regulace vstupu do bankovní sféry,
- stanovení základních pravidel činnosti obchodních bank a kontrola dodržování těchto pravidel,
- povinné pojištění vkladů fyzických osob,
- působení centrální banky jako věřitele obchodním bankám.

ČNB má zájem, aby tato kritéria byla nejen splněna, ale aby byla co nejnáročnější. Náročná kritéria totiž představují prevenci, která brání vstupu do bankovního sektoru nekvalitním subjektům.

Vysoká kvalita a důvěryhodnost je základním předpokladem stability bankovní soustavy a rovnovážného měnového vývoje.

Na základě zákona č. 21/1992 Sb., o bankách, vydává Česká národní banka opatření a vyhlášky, které obsahují podmínky pro vstup do bankovního sektoru a pravidla pro podnikání bank [3].

3.2 Obchodní banky

Bankovnictví tvoří jeden ze základních pilířů všech ekonomik. K tomu, aby bylo pilířem stabilním, je zapotřebí vytvořit kvalitní právní prostředí umožňující fungování, regulaci a dohled nad chováním bank. Základním předpisem pro právní regulaci bankovnictví je zákon o bankách č. 21/1992 Sb., dílčím způsobem novelizován v pozdějších letech [6].

Banky v České republice jsou právnické osoby založené jako akciové společnosti nebo jako státní peněžní ústavy, které přijímají vklady od veřejnosti a poskytují úvěry. Mají

povolení působit jako banka, v jehož rámci mohou vykonávat další činnosti. Banky jsou tedy jako podnikatelské subjekty zřízeny za účelem dosažení zisku [22].

Za udělení licence a její následnou kontrolu je zodpovědná Česká národní banka. V roce 2014 má povolení od ČNB provozovat bankovní činnosti na území České republiky 45 bank a poboček zahraničních bank.

3.2.1 Bankovní operace

Mezi základní bankovní operace 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 [8].

3.2.2 Druhy obchodních bank

Banky se liší druhem a rozsahem prováděných činností, velikostí, právní formou, územní působností aj.

Bankovní soustavu ČR tvoří značné množství různých bankovních institucí, jejichž činnost se může velmi odlišovat.

Téměř všechny bankovní instituce je možno rozdělit buď na univerzální banky, nebo specializované banky.

Univerzální banky, jak vyplývá z názvu, poskytují všechen sortiment bankovních služeb pro nejširší okruh klientů, zahrnující podnikatelské i nepodnikatelské subjekty, právnické i fyzické osoby. V dnešní době jde o nejčastější typ fungování bank. Tento typ v sobě spojuje

činnost komerčních a investičních bank. Na tomto principu funguje naprostá většina českého bankovního trhu, v čele s hlavními bankami.

Specializované banky jsou zaměřeny pouze na určitý druh bankovních služeb, obchodů, klientelu nebo obor podnikání. Ke specializovaným bankám patří:

- spořitelny - jsou to instituce specializující se na výběr vkladů od obyvatelstva. Mohou případně provádět některé další operace jako je vedení účtů, platební styk, poskytování půjček a úvěrů apod.,
- stavební spořitelny - jsou specializovanými institucemi zabývajícími se pouze stavebním spořením. Přijímají účelové vklady a za předem daných podmínek poskytují cílené stavební úvěry,
- úvěrová družstva - jsou v podstatě malé banky založené na družstevním principu. Soustřeďují své služby, zejména poskytování úvěrů, na omezený okruh klientů. Z některých úvěrových družstev se postupným vývojem staly velké univerzální banky,
- hypoteční banky - jsou speciální peněžní ústavy, které se specializují především na poskytování hypotečních úvěrů. Specifikou hypotečních úvěrů je jejich zajištění zástavním právem na nemovitost. Obvykle mohou hypoteční úvěry poskytovat banky na základě speciálně udělené licence,
- investiční banky - jsou specializované bankovní instituce, které se zabývají operacemi s cennými papíry. Jedná se především o obchody s cennými papíry, umisťování emisí cenných papírů na trhu, správa portfolií, poradenství a další služby,
- rozvojové banky - jsou bankovní instituce specializující se na financování rozvojových investic pro firmy či vybraná teritoria. Tyto služby mohou poskytovat jak v národním, tak v mezinárodním měřítku [6].

Vedle těchto bankovních institucí mohou na finančním trhu působit i některé další instituce, jejíž zaměření a existence může být spojeno se specifickými problémy dané země. Takovou institucí je např. v České republice Konsolidační banka vzniklá v roce 1991.

3.2.3 Zásady provádění bankovních operací

Aby banky dosahovaly zisků s minimálními riziky, měly by se řídit následujícími zásadami. Za účelem dosažení vyššího zisku může být v konkurenčním prostředí některá z těchto zásad porušena. Potom se ovšem banka vystavuje riziku, které by mohlo ohrozit její další podnikání.

- Zásada likvidity - banka by měla být schopna dostát všem závazkům vůči svým klientům, měla by být schopna vyplatit jim uložené vklady. Aktivní a pasivní operace banky by měly dosahovat přibližně stejné výše.
- Zásada rentability - banka by měla provádět jen ziskové operace, nikoliv investovat do neziskových projektů či projektů s nepřiměřenými riziky.
- Zásada jistoty - banka by měla minimalizovat možná rizika, jako jsou rizika úroková, devizová, úvěrová a inflační [3].

4 OCHRANA BANKOVNÍHO SEKTORU ČR

O ochranu bankovního sektoru v České republice se stará Ministerstvo financí, které zabezpečuje správný chod a rozdělování financí. Ochrana dat je samozřejmě zajištěna za pomocí informačních systémů, které spravují všechna data týkající se jak finančního, tak bankovního sektoru. Zvláště pak bankovní sektor musí být velmi silný vůči útokům na jeho IS. Ztráta dat by v takovém případě znamenala nedozírné finanční ztráty a nedůvěru obyvatelstva v bankovní organizace ČR, což by vedlo ke kolapsu.

Bankovní sektor nám dnes nabízí mnoho produktů usnadňující život. Mezi tyto produkty patří i elektronické, někdy také nazývané přímé bankovnictví. Elektronické bankovnictví umožňuje klientovi banky provádět bankovní operace na svém účtu či sledovat pohyby na účtu prostřednictvím telekomunikační či datové sítě z domova nebo kanceláře. V dnešní době tyto služby nabízí většina bank v ČR. Banky tyto služby nabízí především s cílem nabídnout klientovi pohodlnější způsob obsluhy účtu a hlavně snížit své náklady na přepážkový provoz. Produkty elektronického bankovnictví se liší u jednotlivých bank jak koncepcí či pojetím, tak i různým zabezpečovacím stupněm. S rozšiřujícími službami a možnostmi elektronického bankovnictví jsou totiž spojena i značná rizika [14].

Pro zajištění bezpečných služeb elektronického bankovnictví je nezbytné, aby každý článek v řetězci poskytovatelů elektronického bankovnictví tato rizika vyhledal, identifikoval, a minimalizoval možné hrozby.

Elektronické bankovnictví zvyšuje závislost banky na informačních technologiích, a tím i komplexnost technických a bezpečnostních řešení, komplexnost partnerských vztahů, aliancí, dodavatelských vztahů, outsourcingu a jiných vztahů banky se třetími stranami.

Internet je globální otevřená síť. Je přístupný téměř odevšud anonymním uživatelům. Tato skutečnost zvyšuje důraz kladený na bezpečnostní opatření, techniku a způsob autentizace uživatele a ochrany dat, standardy ochrany osobních údajů a procedury sběru a vyhodnocování auditních záznamů [20].

Principy řízení rizik

Mezinárodně uznávané a doporučované principy řízení rizik v oblasti elektronického bankovnictví lze rozdělit do tří vzájemně závislých oblastí:

- dohled nad elektronickým bankovnictvím prováděný vedením banky,

- bezpečnostní opatření,
- právní aspekty a zachování dobrého jména banky.

Důležitost určitého principu je vždy dána konkrétním prostředím banky, typem distribučního kanálu, individuálním profilem rizik, provozní a organizační strukturou, firemní kulturou a dalšími individuálními faktory [20].

4.1 Možnosti komunikace klienta a banky

Zavádění produktů elektronického bankovnictví, ještě však nikoliv s použitím internetu, u nás začalo v letech 1993 až 1995. V této době zejména malé banky bojovaly o získání nových klientů zaváděním moderních technologií. Zabezpečení však ještě bylo na nízké úrovni.

I dnes je zvykem českých bank nabízet v základní nabídce svého elektronického bankovnictví pouze omezené množství bezpečnostních mechanizmů. Za vyšší bezpečnost si klient musí připlatit. Dalším bezpečnostním omezením elektronického přístupu klientovo koncové zařízení, protože nelze očekávat stejné možnosti zabezpečení např. telefonického a internetového bankovnictví [20].

Základní formy služeb elektronického bankovnictví jsou znázorněny na následujícím schématu.

Obrázek 2: Možnosti komunikace klienta a banky

Zdroj: vlastní zpracování

4.2 Bezpečnostní zásady pro používání elektronického bankovnictví

Klienti by měli být opatrní na to, kam ukládají a vkládají svá důvěrná data. Použití již na pohled nedůvěryhodného zařízení se nemusí vyplatit. Aby bylo elektronické bankovnictví bezpečné, platí pro něj několik základních pravidel:

- chránit bezpečnostní údaje (hesla, PIN kódy, přístupové kódy atd.), nikomu je nesdělovat,
- pravidelně měnit tyto bezpečnostní údaje,
- používat bezpečný PC
- používat a mít aktualizovaný antivirový systém
- mít aplikované všechny bezpečnostní záplaty v operačním systému a instalovaných aplikací a programů,
- získávat aplikace a programy z důvěrných a osvědčených zdrojů,
- chránit připojení přes internet prostřednictvím firewallů,
- kontrolovat příchozí poštu a neotvírat podezřelé zprávy,
- číst varovná hlášení bankovního softwaru,
- v případě podezření nevkládat do aplikace nebo programu citlivá data,
- dodržovat zásady správné volby a používání hesel,
- při ukončení práce s internetovým bankovnictvím se vždy odhlásit a zavřít okno prohlížeče [14].

4.2.1 Telefonické bankovnictví

Telefonické bankovnictví, taktéž telebanking či phonebanking je služba využívající klasické telefonní linky či mobilní telefony.

Přes telefonní bankovnictví mohou klienti zadávat různé typy příkazů k úhradě, zjišťovat zůstatek na účtu i nejnovější úrokové sazby nebo kurzy měn. Klient tyto bankovní operace provádí po zavolání na speciální linku pro telefonní bankovnictví. Účet lze obsluhovat buď

přes automat telefonní linky tzv. IVR (Interactive Voice Response), nebo prostřednictvím telefonního bankéře, což je reálná osoba.

Operace prováděné prostřednictvím telefonu lze členit na pasivní a aktivní.

O pasivních operacích lze říci, že nemění stav účtu klienta. Řadíme mezi ně veřejně dostupné údaje o bance a jejich produktech a také chráněné informace pocházející z informačního systému banky:

- zjištění zůstatku na účtu,
- informace o pohybech na účtu,
- informace o zadaných a z různých důvodů neprovedených transakcích,
- informace o produktech a službách banky,
- úrokové sazby,
- kurzovní lístek.

Pasivní operace jsou u většiny bank první fází, jakmile je úspěšně zvládnuta, přichází druhá fáze, která je technicky náročnější po stránce zajištění bezpečnosti. Jsou to aktivní operace.

Aktivní operace se týkají provádění transakcí na účtu klienta a zůstatku na něm:

- příkaz k úhradě,
- trvalý příkaz k úhradě,
- příkaz k inkasu,
- trvalý příkaz k inkasu,
- zahraniční platební styk,
- založení, změna nebo zrušení termínovaného vkladu.

Zabezpečení telefonního bankovnictví

Pro pasivní operace, tedy zejména zjišťování zůstatku na účtu, se často využívá osobního čísla klienta. Může se jednat například o číslo účtu, pomocí kterého banka identifikuje klienta. Dále se jedná o číselné heslo (PIN). Toto zajištění lze využít i pro aktivní operace, ale riziko zneužití je zde poměrně vysoké. Z toho důvodu se proto využívá dvouúrovňový systém

ochrany. Klient při vstupu zadává osobní číslo i heslo, ale pro provedení aktivní operace musí zadat navíc i jednorázové heslo. Při zřizování telefonního bankovnictví získá klient sadu několika desítek hesel a při každé aktivní operaci jedno z hesel použije, čímž danou operaci autorizuje. Jednou zadané takové jednorázové heslo pak již nelze znovu použít, takže provedení operace jeho prostřednictvím už není možné.

Systém telefonního bankovnictví si také pro zvýšení bezpečnosti po určité době vyžádá změnu číselného hesla (PINu) pro vstup. Tuto operaci klient může také kdykoliv provést sám. Systém zcela zablokuje danému uživateli přístup v případě, že je opakovaně, zpravidla třikrát, zadáno špatné heslo [14].

4.2.2 GSM bankovnictví

GSM bankovnictví, také GSM banking, je další způsob elektronického bankovnictví. K fungování GSM bankovnictví je potřeba GSM telefon, nejlépe s podporou přídavných funkcí SIM karty, tzv. SIM toolkit. Základním prvkem je bankovní aplikace uložena na kartě, která zprostředkovává přes intuitivní rozhraní komunikaci mezi bankou a klientem [14].

Zabezpečení GSM bankovnictví

Přístup ke zprávám banky či operacím na bankovním účtu je zabezpečen přístupovým bankovním PINem. Dále je přenos zpráv mezi bankou a telefonem klienta šifrován pomocí certifikátu uloženého na SIM kartě. To znamená, že zprávy může číst pouze klient a banka, nikdo jiný.

Pokud klient zadá třikrát po sobě chybně bankovní PIN, bude přístup k bankovní aplikaci a chráněným položkám zablokován. Pro odblokování je třeba znát bankovní PUK. Pokud uživatel desetkrát zadá bankovní PUK chybně, nelze již SIM kartu pro bankovní služby použít.

GSM bankovnictví k jednomu bankovnímu účtu lze provozovat pouze z jedné SIM karty, což je určitě další přínos pro bezpečnost tohoto typu bankovnictví [20].

4.2.3 Mobilní bankovnictví

Chytré mobilní telefony i tablety zcela opanovaly český trh. Jejich rozšíření výrazně zvýšilo poptávku po mobilním bankovnictví, což je aplikace, kterou si klient nainstaluje do svého zařízení s iOS nebo Androidem. K obsluze této aplikace klient nepotřebuje internetový prohlížeč, avšak je nutné připojení k internetu. Aplikace je upravena tak, aby se snadno ovládala pomocí dotyků na displeji.

Důležitost mobilního bankovnictví proto možná brzy předstihne internetové bankovnictví. Není divu, že i české banky jsou ve střehu a drtivá většina z nich svým zákazníkům nabízí aplikaci pro přístup k jejich účtům prostřednictvím chytrých zařízení. Většina bankovních aplikací zvládá základní funkce, jako je zobrazení u banky vedených účtů včetně zůstatků. Většina potom umožňuje také přímé zadávání plateb [11].

Zabezpečení mobilního bankovnictví

Přístup do aplikace funguje přes přihlašovací jméno a heslo, transakce se autorizují za pomocí PIN kódu. Tyto prvky klient nastavuje v internetovém bankovnictví sám. U každého mobilního telefonu si lze nastavit možnosti zabezpečení, zda jeho prostřednictvím bude možné provádět aktivní operace, například platební operace. Data se přenášejí šifrovaně přes zabezpečené připojení s bezpečnostním certifikátem. Ztratí-li klient mobilní telefon, může ho jednoduše zablokovat v internetovém bankovnictví.

4.2.4 Domácí bankovnictví

Home banking, také nazývaný jako domácí bankovnictví, je způsob komunikace klienta prostřednictvím osobního počítače klienta, na kterém je nainstalovaný speciální software. Tento typ elektronického bankovnictví je možné využívat buď prostřednictvím pevného připojení, nebo přes internet. Domácí bankovnictví je tedy omezeno na rozdíl od internetového bankovnictví na jeden konkrétní počítač a instalaci softwaru.

Tato historicky nejstarší služba elektronického bankovnictví umožňuje 24 hodin denně zjišťovat zůstatek peněz na účtu, sledovat tok plateb, zadávat trvalé příkazy k převodu, k inkasu, provádět domácí i zahraniční platby a další. Kromě toho home banking nabízí přístup do databáze banky pro vyhledávání kurzovních lístků, úrokových sazeb, nabídky služeb atd. Výhodou zejména pro podnikatele a právnické osoby je možnost propojení tohoto

programu s vlastním účetním systémem, čímž se umožní automatické předávání platebních příkazů a výpisů z účtu.

Postupem času byl home banking téměř nahrazen internetovým bankovnictvím. Home banking tak dnes zůstává doménou převážně firemních klientů. U soukromých klientů preferují home banking ti, kteří z různých důvodů nechtějí nebo nemohou používat přístup do banky přes internet. Home banking je také řešením pro banky, které nemají vlastní internetové bankovnictví a vzhledem k počtu klientů se nevyplatí jeho vývoj a údržba. Levnější je proto koupě hotového programu v podobě home bankingu [14].

Zabezpečení domácího bankovnictví

Home banking nabízí jeden z nejlepších systémů zabezpečení ze všech forem elektronického bankovnictví. Pro jeho použití není nutné připojení k internetu. Proto je častým důvodem, proč velké firmy nebo majetní občané nechtějí internetové bankovnictví a stále využívají home banking. Přihlášení do bankovního systému probíhá pomocí hesla uživatele a autorizačního certifikátu a celá komunikace mezi klientem a bankou je šifrovaná, proto zajišťuje home banking vysokou úroveň bezpečnosti [20].

4.2.5 Internetové bankovnictví

Internet banking, česky internetové bankovnictví, je jedna z nejoblíbenějších metod obsluhy bankovních účtů a kontaktu klienta s bankou pomocí připojení k internetu. Službu internetového bankovnictví provozuje většina bank v České republice. Aby klient mohl této služby využívat, musí mít u banky založený účet a na pobočce si pak službu aktivovat.

Pomocí internetového bankovnictví klient může:

- zadávat příkazy k úhradě,
- zadávat povolení, změnu či zrušení inkas,
- zadávat, měnit a rušit trvalé příkazy,
- zobrazit historii pohybů na účtu,
- zobrazit zůstatek účtu,
- dostávat elektronické výpisy zdarma,

a to 24 hodin denně 7 dní v týdnu odkudkoliv, kde je kvalitní a bezpečné internetové připojení [14].

Zabezpečení internetového bankovnictví

Míra bezpečnosti závisí především na způsobu identifikace klienta. V zásadě existuje 5 úrovní ochrany vstupní identifikace klienta:

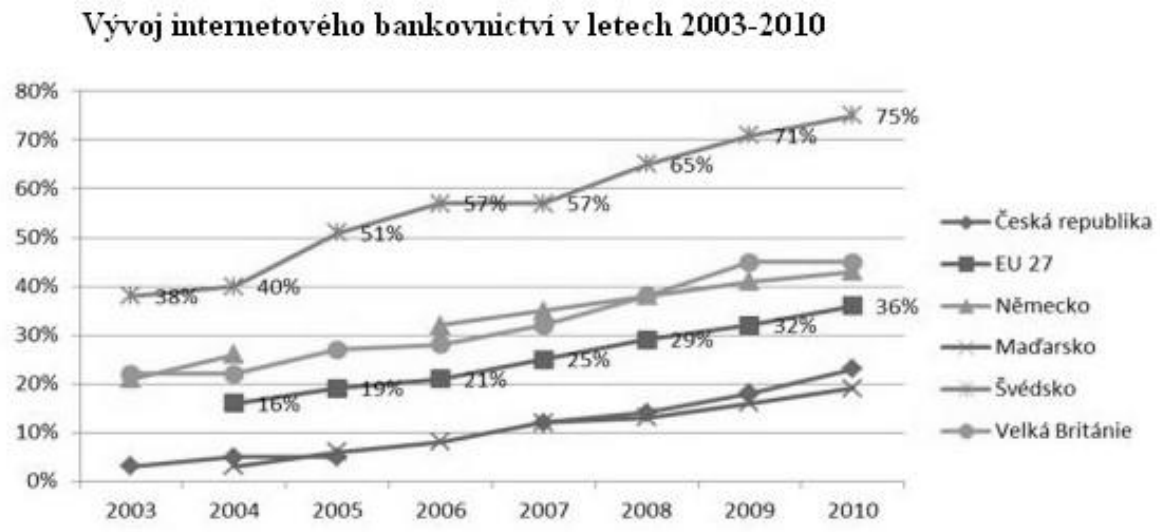
- uživatelské jméno (číslo) a heslo,
- autorizace SMS klíčem,
- certifikát v souboru,
- elektronický kalkulátor,
- certifikát čipová karta.

Podrobně budou tyto formy zabezpečení vysvětleny v následující kapitole.

5 ZABEZPEČENÍ INTERNETOVÉHO BANKOVNICTVÍ V ČR

S rozvojem internetu a jeho začlenění do běžného života téměř všech obyvatel se začalo internetu využívat i při bankovních transakcích. Již běžně se provádí mezibankovní operace pomocí internetového bankovnictví.

Není tomu tak ale ve všech evropských státech stejně. Někde internetové bankovnictví zaznamenalo velký nárůst a oblibu, jinde se však jeho využití zvyšuje jen pozvolna.



Obrázek 3: Vývoj IB v letech 2003 – 2010

Zdroj: vlastní zpracování podle [7]

Nejnižší užívání internetového bankovnictví zaznamenávají státy bývalého východního bloku a také státy, které mají v současné době problém se svou ekonomikou vůbec.

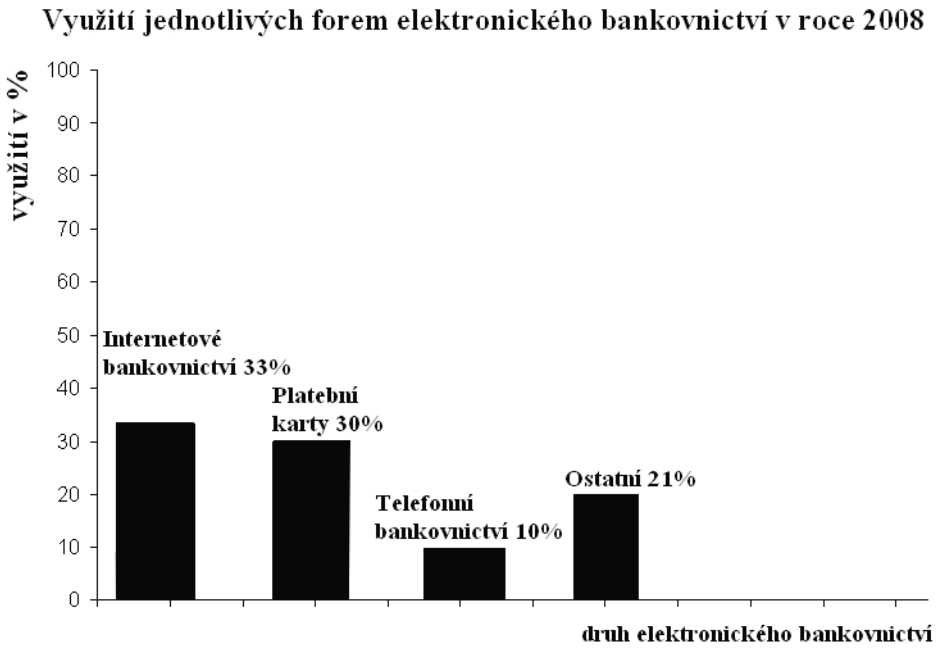
V Rumunsku se užití internetu zvyšovalo od hodnot pod jedním procentem v roce 2003 až do 3 % v roce 2010, Bulharsko je na tom s užitím internetu pro bankovnictví obdobně.

Německo je jedním ze států, kde se užití internetového bankovnictví zvýšilo nejvíce, vzrostlo z hodnoty 21 % v roce 2003 na více jak dvojnásobek (pro rok 2010 je hodnota 43 %).

Také pobaltské státy zaznamenaly enormní nárůst v užití internetového bankovnictví. V Litvě z 3 % pro rok 2003 na 37 % pro rok 2010 a v Lotyšsku z 12 % v roce 2004 na 47 %.

V České republice se hodnota zvyšovala od 3 % do 23% a v EU 27 z 16 % pro rok 2004 na 36 % v roce 2010.

Internetové bankovnictví je nejvyužívanější druh elektronického bankovnictví, jak vyplývá z obrázku č. 4. zpracovaného podle výzkumu z roku 2008. Všechny banky na českém trhu mají totiž alespoň jeden kanál elektronického bankovnictví, a tím je právě internetové bankovnictví.



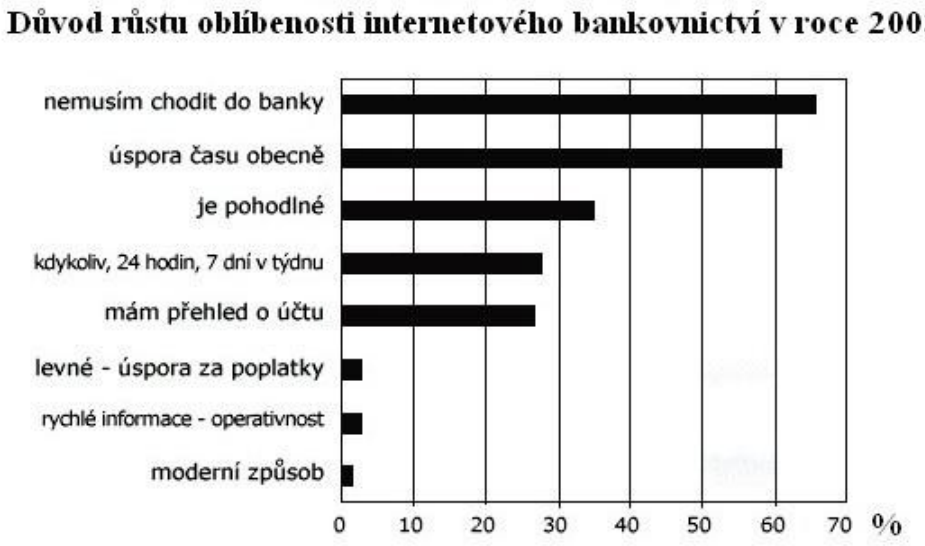
Obrázek 4: Využití jednotlivých forem elektronického bankovnictví v roce 2008

Zdroj: vlastní zpracování podle [20]

Banky tuto formu elektronického bankovnictví nabízejí svým klientům, aby jim poskytly jistý komfort obsluhy účtu na dálku, ale i nižší poplatky za provedené transakce.

Důvodů, proč počet uživatelů přímého bankovnictví roste, je několik. Výzkum z roku 2003 ukazuje, že jde především o výhodu přístupu ke kontu odkudkoliv a kdykoliv, tedy 24 hodin denně, 7 dní v týdnu a 365 dní v roce. Neopomenutelná je také široká škála bankovních operací, které lze realizovat.

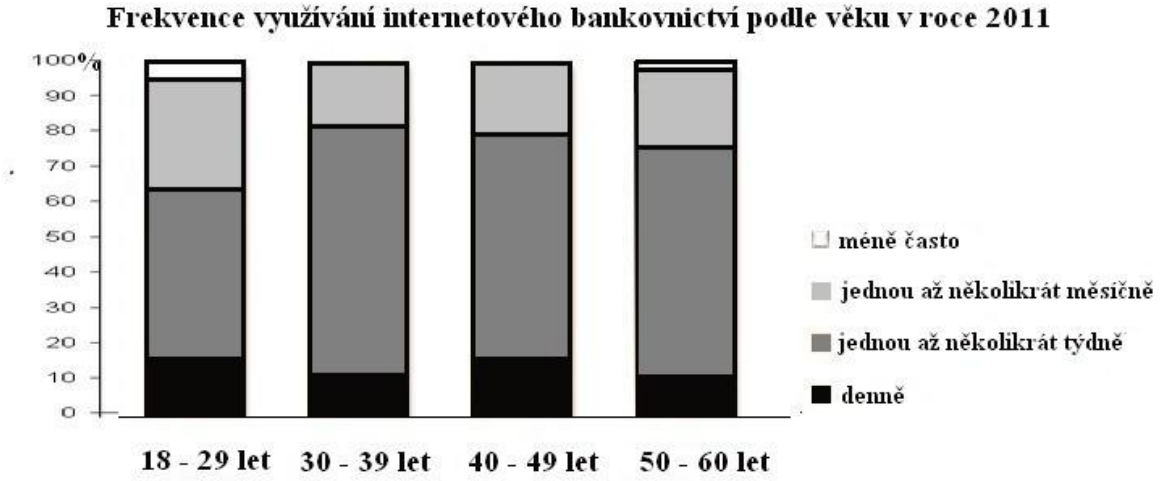
Další důvody oblíbenosti internetového bankovnictví jsou zaznamenané na následujícím obrázku.



Obrázek 5: Důvod růstu oblíbenosti internetového bankovnictví v roce 2003

Zdroj: vlastní zpracování podle [13]

Podle obrázku č. 6, který je zpracovaný podle dostupných dat z roku 2011, jsou nejčastějšími uživateli internetového bankovnictví lidé ve věku 30-40 let. Ti alespoň jednou za měsíc svůj účet zkontrolují téměř všichni (dokonce 81 % lidí ve věku 30-40 navštěvuje internetové bankovnictví alespoň jednou týdně), přičemž nejvíce oceňují jeho rychlost a především pohodlí ovládání účtu z domova (téměř 80 % z nich).



Obrázek 6: Frekvence využívání internetového bankovnictví podle věku v roce 2011

Zdroj: vlastní zpracování podle [5]

5.1 Rozdělení způsobů zabezpečení

Způsoby zabezpečení je možné rozdělit podle jejich úrovně.

Pro pasivní operace většina bank vyžaduje základní způsob zabezpečení pomocí uživatelského jména a hesla. Což je základní, nejméně bezpečný způsob ochrany. Poté je možné např. procházet zůstatky na účtu, operace na účtu apod.

Pro aktivní operace, jako je provádění plateb, již toto zabezpečení nestačí. Zde již po klientovi bude vyžadována další úroveň ověření, jako je například SMS klíč, elektronický certifikát nebo elektronický kalkulátor.

Tabulka 1: Aktivní a pasivní operace banky

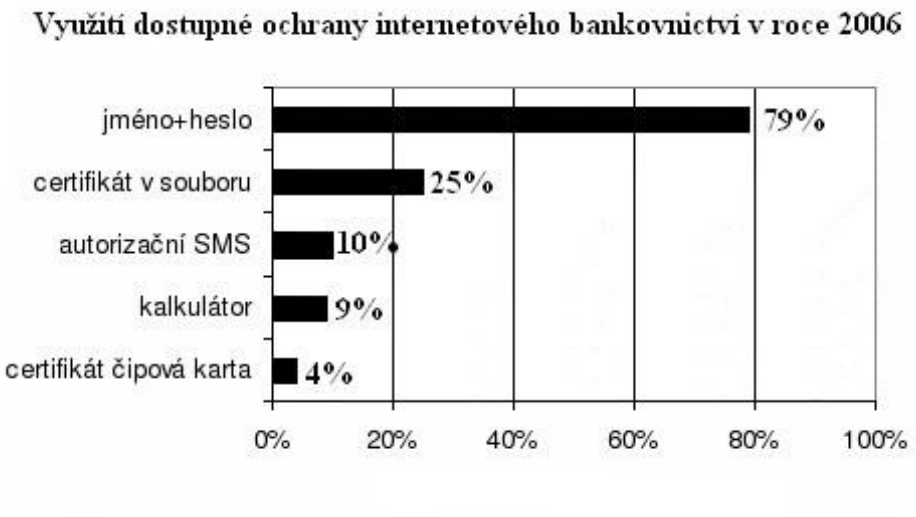
Aktivní operace	**Pasivní operace**
Zadání příkazu k úhradě	Zjištění zůstatku na účtu
Zadání příkazu k inkasu	Zjištění pohybů na účtu
Zřízení trvalého příkazu	Informace o produktech a službách banky
Zahraniční platební styk	Informace o aktuálních úrokových sazbách
Obsluha termínovaných účtů	Informace o aktuálních kurzech cizí měny

Zdroj: vlastní zpracování

5.2 Dostupná ochrana internetového bankovnictví

Jak již bylo zmíněno, banky se snaží zabránit útokům zaváděním bezpečnostních prvků. Mezi tyto prvky patří uživatelské jméno a heslo, certifikát v souboru, autorizační SMS, elektronický kalkulátor a certifikát na čipové kartě.

Mezi nejpoužívanější typ ochrany internetového bankovnictví patří ochrana pomocí uživatelského jména a hesla. Tento způsob využívá 79% klientů. Naopak nejméně používaný druh zabezpečení je certifikát uložený na čipové kartě, který využívá pouze 4% klientů. Všechny dostupné prvky jsou znázorněné na následujícím grafu a následně budou blíže popsány.



Obrázek 7: Využití dostupné ochrany internetového bankovnictví v roce 2006

Zdroj: vlastní zpracování podle [1]

Uživatelské jméno + heslo

Tento způsob přihlašování je nejjednodušší, avšak nejméně bezpečný. Nepomůže ani dostatečně dlouhé heslo. Dle průzkumu tuto metodu využívá téměř 80% uživatelů internetového bankovnictví v České republice.

Nevýhodou tohoto zabezpečení je, že případnému útočníkovi stačí znát pouze jméno a heslo, aby se dostal k účtu klienta. Napadne-li počítač škodlivý vir schopný sledovat stisknuté klávesy (keylogger), oba tyto údaje lehce získá a může je odeslat podvodníkovi. Pokud klient nemusí následnou platbu autorizovat, představuje to velké riziko. Některé banky zvyšují bezpečnost tak, že pro zadání hesla je možné použít grafickou klávesnici, která je ovládaná myší. Tento způsob ale dokáže trojský kůň také monitorovat [1].

Pokud klient zvolí tento základní způsob přihlášení, měl by se aktivně zajímat o doplňující bezpečnost, jako je např. automatické zasílání informačních SMS po každém zadání aktivní transakce či při změně zůstatku, nastavení denního limitu, možnost poskytování informací o provedených finančních transakcích (prostřednictvím e-mailu, SMS nebo faxu) [1].

Certifikát v souboru

Osobní certifikát je soubor, který obsahuje klientovi identifikační údaje. Slouží pro přístup k internetovému bankovnictví a k autorizaci plateb. Soubor s tímto certifikátem je uložený v klientově PC nebo na datovém médiu, jako je CD, USB flash disk a další. Přístup do certifikátu je chráněn heslem. Platnost certifikátu je 2 roky. Při využívání certifikátu k autorizaci plateb banka zasílá klientovi ještě prostřednictvím SMS autorizační kód sloužící jako dodatečné ověření klientovi totožnosti. Klientovo číslo lze změnit pouze na pobočce banky [20].

Autorizace SMS klíčem

K potvrzení každé bankovní transakce banka zašle unikátní kód v podobě textové zprávy na předem zaregistrované mobilní číslo. SMS klíč je nutný pro všechny transakce bez ohledu na jejich výši. Zabezpečení u autorizace SMS klíčem je takové, že pokud dojde k útoku hackera, bez mobilního telefonu klienta nemůže provést žádnou transakci [20].

Elektronický kalkulátor

Mezi bezpečné systémy patří elektronické kalkulátory, které vygenerují pokaždé jiný originální přístupový kód pro potvrzení transakcí. Klienti si nic nemusí instalovat do počítače, ale musí si koupit zařízení např. v podobě malé kalkulačky. Elektronický kalkulátor je přenosný a je chráněn čtyřmístným heslem. Po zadání hesla a stisknutí příslušného tlačítka vygeneruje šestimístný kód, který klient použije pro vstup do internet bankingu. Pro každou aktivní transakci musí být vygenerováno nové číslo [20].

Certifikát na čipové kartě

Osobní certifikát uložený na čipové kartě je určen především pro klienty, kteří požadují vyšší zabezpečení uložení certifikátu. Hlavní výhodou a vlastností čipové karty je, že certifikát z ní nelze žádným způsobem zkopírovat. Pokud tedy nedojde k fyzické ztrátě čipové karty, je zneužití certifikátu prakticky vyloučeno. Práce s certifikátem na čipové kartě je také mnohem snazší a rychlejší, neboť při využívání certifikátu na čipové kartě zadáváte pouze 4 místný PIN [20].

Jak již bylo řečeno, tyto různé způsoby zabezpečení internetového bankovnictví mají své výhody i nevýhody. V následujících dvou tabulkách je znázorněno, jak české banky vyvíjeli své zabezpečení internetové bankovnictví během let 2008-2014.

Tabulka 2: Zabezpečení bank v České republice v roce 2008

BANKA	Jméno a heslo	Certifikát	Čipová karta	SMS kód	Kalkulátor
Citibank	ano				ano
Česká spořitelna	ano		ano		ano
ČSOB	ano		ano		
E-banka		ano		ano	ano
GE Money Bank	ano	ano		ano	
UniCredit Bank	ano	ano		ano	ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano				
Volksbank	ano	ano			

Zdroj: vlastní zpracování podle [20]

V roce 2008 téměř všechny banky jako samozřejmost nabízeli svým klientům zabezpečení pomocí uživatelského jména a hesla, avšak jako velký nedostatek bylo zabezpečení pomocí certifikátu uloženého na čipové kartě. Tuto formu zabezpečení nabízely v roce 2008 pouze Česká spořitelna, ČSOB a Komerční banka.

Tabulka 3: Zabezpečení bank v České republice v roce 2014

BANKA	Jméno a heslo	Certifikát	Čipová karta	SMS kód	Kalkulátor
Citibank	ano	ano	ano	ano	ano
Česká spořitelna	ano	ano	ano	ano	ano
ČSOB	ano	ano	ano	ano	
E-banka	ano	ano	ano	ano	ano
GE Money Bank	ano	ano	ano	ano	
UniCredit Bank	ano	ano	ano	ano	ano
Komerční banka	ano	ano	ano	ano	ano
Poštovní spořitelna	ano	ano	ano	ano	
Volksbank	ano	ano	ano	ano	ano

Zdroj vlastní zpracování

V dnešní době je situace zcela jiná. Banky se svým klientům snaží nabídnout co nejlepší ochranu internetového bankovnictví, která je momentálně dostupná. Za tuto ochranu si ale klient musí připlatit.

V následující tabulce jsou uvedeny ceny nejbezpečnějšího zabezpečení internetového bankovnictví na českém trhu, a to certifikátu uloženého na čipové kartě. Jak již bylo zmíněno, k tomuto certifikátu je zapotřebí i zařízení čtečky čipových karet. V tabulce je také uvedena cena za roční prodloužení tohoto certifikátu.

Tabulka 4: Ceny čipových karet a jejich čteček v roce 2014

Banka	Vydání čipové karty	čtečka	Roční prodloužení
Česká spořitelna	350,-	350,-	350,-
Poštovní spořitelna	900,-	500,-	200,-
KB	390,-	300,-	-
ČSOB	400,-	500,-	200,-

Zdroj: vlastní zpracování

Rozhodujícím faktorem o použití zabezpečení internetového bankovnictví je cena. Ceny největších bank v České republice se pohybují od 350 Kč do 900 Kč za vydání čipové karty, dále od 300 Kč do 500 Kč za vydání čtečky čipových karet a roční prodloužení certifikátu uloženého na čipové kartě je v rozmezí od 200 Kč až 350 Kč.

Proto tuto metodu zabezpečení využívá jen minimum klientů internetového bankovnictví, a sice pouhá 4%, jak vyplývá z obrázku číslo 7.

5.3 Shrnutí a doporučení

Každá internetová komunikace je spojena s určitým rizikem, proto je vždy nutné najít vhodnou hranici mezi užitkem, mírou rizika a investicí do zabezpečení. Pokud se klient nebude spoléhat pouze na nejjednodušší způsob zabezpečení, ale bude aktivně využívat kombinaci možných bezpečnostních prvků internetového bankovnictví, rizika lze minimalizovat. Podle svých nároků i četnosti užívání internetového bankovnictví zvolí optimální způsob, kterým se bude do internetového bankovnictví přihlašovat.

Ať už je totiž internetové bankovnictví zabezpečeno sebelépe, bez dodržování základních pravidel bezpečnosti ze strany klientů se neobejde. Mezi nejčastější příčinu zneužití internetového bankovnictví patří nerespektování základních pravidel bezpečnosti, uživatelské chyby a vyzrazení přístupu k účtu.

Banky na svých internetových stránkách i na pobočkách nabádají klienta, jak se chovat a jak správně používat internetové bankovnictví. Klient by měl samozřejmě dbát i na zabezpečení svého počítače. Banky například nedoporučují používat k přihlášení na svůj bankovní účet počítače, o nichž klient nic neví. Například typicky v internetových kavárnách a jiných veřejných místech, kde klient nezná míru zabezpečení počítače a také jaké programy a viry může počítač obsahovat. Samozřejmostí by měl být také pravidelně aktualizovaný počítač s aktuální verzí antivirového programu, anti-spyware program a kvalitní firewall. Nesmírně důležitá je také ochrana přístupových údajů a zvolení silného hesla. Heslo by mělo být kombinací čísel a písmen, v žádném případě datum narození a podobně. Na internetu existuje plno nástrojů, které nabízí ověření kvalitního hesla.

Bezpečnost internetového bankovnictví by měla být prioritou jak pro klienty, tak pro banky. Je to prestižní záležitost disponovat kvalitním a bezpečným bankovnictvím. Nedá se samozřejmě dosáhnout stoprocentního zabezpečení, banky by však měly usilovat o včasnou reakci na vzniklé hrozby. Měly by investovat nejen do vývoje bankovních informačních systémů, ale také do lepší informovanosti svých klientů. Většina úspěšných útoků na internetové bankovnictví je totiž založena na oklamání důvěřivých klientů, kteří své přihlašovací údaje do internetového bankovnictví zadají na webových stránkách snažící se napodobit originální bankovní přihlašovací systém.

ZÁVĚR

Tato bakalářská práce se věnovala tématu „ochrana kritické infrastruktury se zaměřením na bankovní sektor v České republice“.

V úvodu práce byly vymezeny tři hlavní cíle práce. První z nich spočíval v teoretickém popisu oblasti kritické infrastruktury. Druhý cíl práce byl seznámení s vybranou oblastí bankovního sektoru a její analýza. Poslední cíl byl vyvození doporučení, které by přispělo k ochraně dané oblasti.

První kapitola se zabývala přiblížením základní problematiky oblasti kritické infrastruktury. Kritická infrastruktura je v legislativě České republiky poměrně nový pojem. Podrobně se problematikou kritické infrastruktury České republiky zabývá novelizovaný zákon č. 240/2000 Sb., o krizovém řízení, který nabyl platnost k 1. lednu 2001. V této kapitole byla infrastruktura vysvětlena z hlediska veřejné a kritické infrastruktury. Dále byly vysvětleny pojmy subjekty a objekty kritické infrastruktury a další základní pojmy, které jsou nezbytné pro pochopení dané problematiky. Dále byla věnována pozornost významu kritické infrastruktury, který spočívá především v zajištění bezpečnosti státu, fungování ekonomiky, výrobních a nevýrobních systémů a služeb, chodu veřejné správy a základních životních potřeb obyvatelstva. Ze schématu provázanosti kritické infrastruktury v této kapitole je patrné, že tyto oblasti jsou na sobě vzájemně závislé. Při poškození či výpadku některého z prvků by došlo k vážnému narušení funkčnosti celé sítě a ke zhroucení kritické infrastruktury. V této úvodní kapitole byl tedy již splněn první cíl bakalářské práce.

Druhá část popisovala podrobněji jednotlivé oblasti kritické infrastruktury České republiky. Zpráva výboru pro civilní nouzové plánování z roku 2007 stanovila 9 oblastí kritické infrastruktury, což jsou energetika, vodní hospodářství, potravinářství a zemědělství, zdravotní péče, doprava, komunikační a informační služby, finance a státní správa, nouzové služby a veřejná správa. Jednotlivé oblasti byly stručně charakterizovány a byla nastíněna rizika, kterým jsou dané oblasti vystaveny a měla by se jim věnovat vyšší pozornost.

Třetí kapitola podrobněji analyzovala bankovní sektor České republiky, který je jednou z oblastí kritické infrastruktury České republiky. Bankovnictví v dnešní době patří mezi odvětví s nejvyšší dynamikou rozvoje. Bez kvalitně fungujícího bankovního systému není možné docílit výraznějšího ekonomického pokroku. V této kapitole byl popsán dvoustupňový bankovní systém České republiky. První stupeň tvoří centrální banka, tedy Česká národní banka. Byly zde popsány základní funkce a cíle České národní banky, nástroje České národní

banky a nezávislost České národní banky. Veškeré tyto oblasti jsou obsaženy v zákoně č. 6/1993 Sb., o České národní bance. Druhý stupeň bankovního systému České republiky tvoří obchodní banky. Obchodní banky se řídí zákonem č. 21/1992 Sb., o bankách, kde jsou vymezeny bankovní operace, druhy obchodních bank a zásady provádění bankovních operací, které jsou rovněž popsány ve třetí kapitole práce.

Čtvrtá část se zabývala ochranou bankovního sektoru. O ochranu bankovního sektoru se v České republice stará Ministerstvo financí. Tato kapitola se zaměřovala převážně na oblast elektronického bankovnictví, byly zde vyjmenovány některé bezpečnostní zásady pro používání elektronického bankovnictví. Dále zde bylo nastíněno schéma rozdělení forem elektronického bankovnictví a způsoby zabezpečení, a to telefonické bankovnictví, GSM bankovnictví, mobilní bankovnictví, domácí bankovnictví a internetové bankovnictví. V této kapitole je patrné, jak může být zkoumaná oblast efektivně zabezpečena. Tím je tedy splněn i druhý cíl bakalářské práce.

Poslední pátá kapitola se věnovala zabezpečení internetového bankovnictví v České republice. Byl zde nastíněn vývoj internetového bankovnictví v letech 2003-2010, ze kterého bylo patrné, že vývoj internetového bankovnictví není ve všech státech Evropy na stejné úrovni. Další část byla věnována výzkumu z roku 2008, ze kterého vyplynulo, že internetové bankovnictví je nejvyužívanější druh elektronického bankovnictví. Důvodů oblíbenosti internetového bankovnictví je několik. Nejčastější důvod je ten, že klient nemusí do banky osobně, tím ušetří čas. Z dalšího průzkumu z roku 2011 se ukázalo, že nejčastějšími uživateli internetového bankovnictví jsou lidé ve věku 30-40 let. Dále zde byla uvedena a vysvětlena dostupná ochrana internetového bankovnictví. Nejpoužívanější ochranou je ochrana pomocí jména a hesla. Na druhém místě pak certifikát v souboru, dále autorizace pomocí SMS klíče, pak elektronický kalkulátor a nakonec certifikát na čipové kartě. Poslední částí této kapitoly byl výzkum zabezpečení komerčních bank v České republice v roce 2008 a v roce 2014. Z těchto tabulek lze vyvodit, že banky se v dnešní době snaží nabídnout co nejlepší ochranu internetového bankovnictví, která je momentálně dostupná. Za tuto ochranu si ale klient musí připlatit. Cena je tedy rozhodujícím faktorem pro použití zabezpečení internetového bankovnictví. Ceny čipových karet a čteček jsou vysoké, proto tuto metodu zabezpečení využívá jen minimum uživatelů internetového bankovnictví. Dále byly v této kapitole uvedeny shrnutí a doporučení, které by mohly vést ke zvýšení ochrany zkoumané oblasti bankovního sektoru. Tím byl tedy splněn i třetí cíl bakalářské práce. Domnívám se proto, že všechny cíle práce stanovené v úvodu byly naplněny.

POUŽITÁ LITERATURA

[1] *Bezpečnost internetového bankovnictví* [online]. 2006 [cit. 2014-03-07]. Dostupné z: http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/.

[2] BÍLEK, M., *Problematika kritické infrastruktury*. Dostupné z: ceses.cuni.cz/CESES-70-version1-KI_Bilek.pdf.

[3] BLAŽEK, J., UKLEIN, J., *Bankovnictví,* Masarykova Univerzita, 1997. ISBN 80-210-1715-5.

[4] Česká národní banka. *O ČNB* [online]. 2014 [cit. 2014-02-10]. Dostupné z: http://www.cnb.cz/cs/o_cnb/.

[5] *Češi v síti a internetové bankovnictví* [online]. 2011 [cit. 2014-03-07]. Dostupné z: http://www.novinky.cz/internet-a-pc/245053-cesi-v-siti-a-internetove-bankovnictvi.html.

[6] FREIBERG, F., *Bankovnictví*, ČVUT v Praze, 2000. ISBN 80-01-02106-8.

[7] *Jak moc se používá internetové bankovnictví ve světě* [online]. 2011 [cit. 2014-03-07]. Dostupné z: http://firmy.finance.cz/zpravy/finance/321135-jak-moc-se-pouziva-internetove-bankovnictvi-ve-svete-/.

[8] KAMPF, R. Financování a bankovnictví. Pardubice: Univerzita Pardubice, 2005. 80-7194-745-8.

[9] KOLEKTIV AUTORŮ. *Ochrana kritické infrastruktury*. Česká asociace bezpečnostních manažerů, 2011. ISBN 978-80-260-1215-3.

[10] *Ministerstvo vnitra ČR* [online]. 2010 [cit. 2014-02-06]. Dostupné z: http://www.mvcr.cz/clanek/pojmy-kriticka-infrastruktura.aspx.

[11] *Mobilní bankovnictví* [online]. 2014 [cit. 2014-03-07]. Dostupné z: http://www.penize.cz/mobilni-bankovnictvi.

[12] MOZGA, J., VÍTEK, M., KOVÁŘÍK, F. *Kritická infrastruktura společnosti.* Univerzita Hradec Králové, 2008. ISBN 978-80-7041-299-2.

[13] *Počet příznivců přímého bankovnictví roste* [online]. 2003 [cit. 2014-03-07]. Dostupné z: http://www.penize.cz/bezne-ucty/16321-pocet-priznivcu-primeho-bankovnictvi-roste.

[14] PŘÁDKA, M., KALA, J., *Elektronické bankovnictví rady a tipy*, Computer Press, 2000. ISBN 80-7226-328-5.

[15] REVENDA, Z. *Centrální bankovnictví*. 2. rozšířené vydání, Management Press, 2001. ISBN 80-7261-051-1.

[16] ROUDNÝ, R., LINHART, P. *Krizový management I.*, Univerzita Pardubice, 2005. ISBN 80-7194-674-5.

[17] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. In:Úřední věstník Evropské unie. 2008.

[18] ŠENOVSKÝ, M., ADAMEC, V., ŠENOVSKÝ, P. *Ochrana kritické infrastruktury*. Edice SPBI Spektrum, 2007. ISBN 978-80-7385-025-8.

[19] Ústavní zákon č. 1/1993 Sb., *Ústava České republiky.*

[20] VAŠEK, M., KRHOVJÁK, J., *Autorizace elektronických transakcí a autentizace dat i uživatelů*, Masarykova Univerzita, 2008. ISBN 978-80-210-4556-9.

[21] VILÁŠEK, J., FUS, J. *Krizové řízení v ČR na počátku 21. století.* Karolinium, 2012. ISBN 978-80-246-2170-8.

[22] Zákon č. 21/1992 Sb., *o bankách.*

[23] Zákon č. 110/1998 Sb., *o bezpečnosti České republiky.*

[24] Zákon č. 183/2006 Sb*., o územním plánování a stavebním řádu (stavební zákon).*

[25] Zákon č. 239/2000 Sb., *o integrovaném záchranném systému a o změně některých zákonů.*

[26] Zákon č. 240/2010 Sb., *o krizovém řízení a o změně některých zákonů (krizový zákon).*

SEZNAM PŘÍLOH

Příloha A

Schválené oblasti kritické infrastruktury v EU

	Sektor	**Produkt nebo služba**
I	Energie	1 Produkce ropy a plynu, úprava, zacházení a skladování včetně produktovodů 2 Výroba elektřiny 3 Přeprava elektřiny, plynu a ropy 4 Distribuce elektřiny, plynu a ropy
II	Informační, telekomunikační technologie, ICT	5 Ochrana informačních systémů a sítí 6 Použití nástrojů automatizačních a kontrolních systémů (SCADA = Systém kontroly a sběru dat atd.) 7 Internet 8 Zabezpečení pevných telekomunikací 9 Zabezpečení mobilních telekomunikací 10 Radiová komunikace a navigace 11 Satelitní komunikace 12 TV vysílání
III	Pitná voda	13 Zajištění pitné vody 14 Kontrola kvality vody 15 Zachycování a kontrola objemu vody
IV	Potraviny	16 Zajištění potravin a zabezpečení jejich nezávadnosti a bezpečnost
V	Zdraví	17 První pomoc a lékařská pomoc 18 Léky, séra, vakcíny a léčiva 19 Bio-laboratoře a bio-agens
VI	Finanční	20 Platební služby/struktura plateb (soukromé) 21 Systém převodů veřejných financí
VII	Veřejný a legislativní pořádek a bezpečnost	22 Udržování veřejného a legislativního pořádku, bezpečí a bezpečnosti 23 Soudní správa a vazba
VIII	Civilní správa	24 Vládní funkce
		25 Ozbrojené složky
		26 Státní správa
		27 Nouzové služby
		28 Poštovní a kurýrní služby
IX	Doprava	29 Silniční doprava 30 Železniční doprava 31 Letecká doprav 32 Říční doprava 33 Námořní doprava

X	Chemický a jaderný průmysl	34 Doprava, výroba a skladování/nakládání s chemickými a jadernými látkami 35 Doprava všech typů včetně produktovodů pro nebezpečné výrobky (chemické a jaderné látky)
XI	Vesmír a výzkum	36 Vesmír 37 Výzkum

Příloha B

Schválené oblasti kritické infrastruktury v ČR

Poř.	Oblast KI	Produkt nebo služba
1	Energetika	1.1. Elektřina
		1.2. Plyn
		1.3. Tepelná energie
		1.4. Ropa a ropné produkty
2	Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou
		2.2. Zabezpečení a správa povrchových vod a podzemních zdrojů vody
		2.3. Systém odpadních vod
3	Potravinářství a zemědělství	3.1. Produkce potravin
		3.2. Péče o potraviny
		3.3. Zemědělská výroba
4	Zdravotní péče	4.1. Přednemocniční neodkladná péče
		4.2. Nemocniční péče
		4.3. Ochrana veřejného zdraví
		4.4. Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5	Doprava	5.1. Silniční
		5.2. Železniční
		5.3. Letecká
		5.4. Vnitrozemská vodní
6	Komunikační a informační systémy	6.1. Služby pevných telekomunikačních sítí
		6.2. Služby mobilních telekomunikačních sítí
		6.3. Radiová komunikace a navigace
		6.4. Satelitní komunikace
		6.5. Televizní a radiové vysílání
		6.6. Poštovní a kurýrní služby
		6.7. Přístup k internetu a k datovým službám
7	Bankovní a finanční sektor	7.1. Správa veřejných financí
		7.2. Bankovnictví
		7.3. Pojišťovnictví
		7.4. Kapitálový trh
8	Nouzové služby	8.1. Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany
		8.2. Policie ČR (vnitřní bezpečnost a veřejný pořádek)
		8.3. Armáda ČR (zabezpečení obrany)
		8.4. Radiační monitorování včetně podkladů pro rozhodování o opatření vedoucích ke snížení nebo odvrácení ozáření
		8.5. Předpovědní, varovná a hlásná služba

9	Veřejná správa	9.1. Státní správa a samospráva
		9.2. Sociální ochrana a zaměstnanost (sociální zabezpečení, státní sociální podpora, sociální pomoc)
		9.3. Výkon justice a vězeňství