

PROBLEMATIKA BEZPEČNOSTNÝCH RIZÍK V BANKOVOM SEKTORE

Anton KORAUS - Roman ŠÍP

SECURITY RISKS IN THE BANKING SECTOR

Abstrakt

Komerčné banky sú pri výkone svojej činnosti, či už z dôvodu poskytovania bankových produktov alebo využívania rôznych finančných nástrojov, vystavené množstvu rizík. Niektoré z nich ohrozujú banku podobne ako akýkoľvek iný podnikateľský subjekt, iné sú zase spojené s osobitosťami samotnej bankovej činnosti. Pre banky je veľmi dôležité, aby jednotlivé riziká dokázali presne rozoznať a odlišiť od ďalších rizík. Je nutné, aby bankové inštitúcie mali vytvorené mechanizmy, ktoré by riziká nielen identifikovali a vyčíslili, ale tiež aby boli schopné využiť účinné nástroje pre ich zamedzenie.

Kľúčové slová: banka, bankové riziká, identifikácia a kvantifikácia rizika, úverové riziko, trhové riziko, riziko likvidity, operačné riziko

Abstract

The commercial banks as providers of banking products and users of various financial tools are exposed to a number of risks. Some of them are a threat to the bank, similarly as they would be to any other entrepreneurial entity, while others are narrowly associated with the specifics of banking. For banks, it is necessary to have the tools to identify and quantify the risks, as well as use effective tools of risk prevention.

Key words: the bank, banking risks, identify and quantify the risks loan risk, market risk, liquidity risk, operational risk

Úvod

V dnešnej dobe technologické objavy akcelerujú už aj tak pomerne vysoké tempo, ktoré sa prejavuje aj v bankovom sektore napríklad v neustálom zdokonaľovaní jednotlivých ochranných prvkov uplatňovaných v bankovej činnosti. To čo bolo pred pár rokmi považované za neprelomiteľný bezpečnostný prvok je už dnes väčšinou zastaranou a absolútne nedostatočnou formou zabezpečenia. Primeraná úroveň bezpečnosti, reagujúca na aktuálne hrozby okolitého prostredia, je z tohto dôvodu v súčasnosti nevyhnutným predpokladom výkonu činnosti komerčných bánk. Technické a technologické zabezpečenie je fundamentálnym predpokladom ochrany bánk ako aj ich klientov.

Dnes sú popri technologických bezpečnostných prvkoch oprávnené záujmy bankových klientov zabezpečené celým radom ďalších inštitútov, ktorých primárnym cieľom je najmä budovanie vzťahu medzi bankou a klientom na princípe dôvery. Dôvera ovplyvňuje ľudské zmýšľanie a konanie mnoho krát do väčšej miery ako sama realita. Banková teória a prax vo všeobecnosti uznávajú základné determinanty budovania dôveryhodnosti bánk a bankového sektora v týchto oblastiach:

- dôveryhodný pôvod kapitálu a jeho primeraný objem,
- rentabilný manažment komerčnej banky, dodržiavanie pravidiel obozretného podnikania bánk,
- legislatívne garancie pre vkladateľov (napr. zákon o ochrane vkladov),
- optimálny bankový marketing. (Belás a kol., 2010)

Mnohé ochranné prvky vyžadujú súčinnosť samotných klientov. Bankový klient predstavuje najslabší článok celého bezpečnostného procesu, pretože ľudia nie vždy koná v súlade s bezpečnostnými zásadami, ktorých dodržiavanie je žiaduce v každodennom živote. Banky sú v súvislosti so sofistikovaným využívaním bezpečnostných opatrení vždy o krok dopredu. V prípade, že klient vystaví svoje finančné prostriedky riziku, banka je schopná poskytnúť klientovi odbornú pomoc a nevyhnutné dodatočné zabezpečenie.

Súčasný stav riešenej problematiky

V súčasnosti sa môžeme stretnúť s rôznymi definíciami pojmov základných bankových rizík. Vymedzenie obsahu jednotlivých rizík, ktorým je banka vystavená, je základom pre ich možnú kvantifikovateľnosť a následné monitorovanie a riadenie. Tieto definície zároveň slúžia ako východisko pre ochranu banky a jej účinný boj s rizikom.

Pod pojmom riziko, ktoré je nevyhnutnou súčasťou každého podnikateľského rozhodnutia, možno všeobecne chápať odchýlenie skutočne dosiahnutého výsledku od výsledku očakávaného, resp. vznik škody alebo straty. (Rusko-Králiková, 2013)

Riziko môže byť kvantifikované identifikáciou možných negatívnych dopadov na zdravie, majetok, prostredie a podobne so súčasným zhodnotením týchto dopadov, ich veľkosti, intenzity, amplitúdy, časového prehľadu týchto dopadov a ich následkov a pravdepodobnosti ich vzniku. (Rusko, 2006)

Z hľadiska koncepčného a metodického musí charakteristika posudzovania rizík v bankovom sektore vychádzať rovnako, ako pri posudzovaní rizík všeobecne z toho, že:

- riziko veľmi úzko súvisí s výnosmi, preto musí byť pri posudzovaní rizika braná do úvahy stabilita a štruktúra výnosov bánk,
- riziko veľmi úzko súvisí s transparentnosťou, preto musí jeho posudzovanie odrážať skutočnosť, ako a aké údaje banka zverejňuje a ako je otvorená voči verejnosti a orgánom a inštitúciám regulácie a dohľadu,
- riziká sú obmedzované realizáciou regulatívnych opatrení BIS, Direktív EU, resp. regulatívnych opatrení bankového dohľadu centrálnych národných bánk, preto musí byť riziko posudzované z hľadiska dodržiavania a rešpektovania jednotlivých opatrení a nariadení centrálnych národných bánk, ich zapracovanie do vnútorných bankových predpisov a postupov i dodržiavanie týchto predpisov a postupov ako v jednotlivých bankách, tak v bankovom sektore ako v celku. (Polouček, 2006, s.282)

Z pohľadu banky a bankového manažmentu je bezpečnosť kľúčovým faktorom pre získanie a udržanie si klienta. Riziká, ktoré podstupujú komerčné banky sú mixom faktorov vyplývajúcich z interného aj externého prostredia. „Cieľom banky, nie je len minimalizácia rizík, ale hlavne ich identifikácia, kvantifikácia, monitorovanie a riadenie. Je dôležité identifikovať, či ide o externý alebo interný zdroj vzniku rizika, ktorá oblasť podniku je bezprostredne ohrozená a aké prípadné straty môže dané riziko spôsobiť.“ (Zimková, 2009, s. 258).

Podľa Belása a Demjana (2009, s. 86) existujú na finančných trhoch riziká, ktoré sú všeobecne definované ako potenciálna finančná strata subjektu. V odbornej literatúre je uvedených viacero členení finančných rizík. Belás a Demjan (2009, s. 86), Kašparovská (2006, s.71) a Jíleka (2000, s.15) rozdeľujú riziká do piatich základných kategórií: úverové riziko, trhovú riziko, riziko likvidity, operačné riziko a obchodné riziko.

V spojitosti s činnosťou banky, ako špecifického podnikateľského subjektu, je významné finančné riziko, ktoré predstavuje hrozbu možnej finančnej straty vyplývajúcej z použitia príslušného finančného alebo komoditného nástroja či portfólia.

Pre potrebu bližšieho oboznámenia sa s rôznymi rizikami ohrozujúcimi finančné inštitúcie a následný rozbor v súčasnosti využívaných nástrojov a postupov, ktoré banky využívajú na ochranu pred týmito hrozbami, môžeme bankové riziká rozdeliť do dvoch základných skupín:

- **finančné riziká**, kam teória tradične zaraďuje najmä:
 - úverové (kreditné) riziko – ako interné bankové riziko, podmienené najmä vlastnou činnosťou finančnej inštitúcie, spočíva v hrozbe zlyhania zmluvnej strany pri plnení svojich záväzkov voči banke. Ide o jedno z najvýznamnejších rizík, ktorým je banka vystavená či už pri poskytovaní úverov, aktivitách na finančnom trhu alebo iných obchodných praktikách;
 - trhovú riziká – typický predstaviteľ externého bankového rizika, nakoľko vzniká nezávisle od aktivít finančnej inštitúcie. Napriek tomu má na jej podnikateľskú činnosť významný dopad. Základom týchto rizík sú možné nepriaznivé pohyby trhovými úrokovými sadzami, cenami akcií a komodít, ako aj devízovými kurzmi, ktoré môžu mať následný nežiaduci vplyv na výnosy banky, prípadne hodnotu finančných nástrojov v bankovom portfóliu. Na základe uvedeného pod pojmom trhovú riziká chápeme:
 - úrokové riziko;
 - akciové riziko;

- komoditné riziko;
- menové riziko.
- **operačné riziko** – „Operačné riziko je riziko finančnej straty vznikajúcej buď priamo (tzn. vznikajúcej ako priamy dôsledok operačného zlyhania), alebo nepriamo (tzn. vznikajúcej prostredníctvom trhového rizika, kreditného rizika, rizika likvidity alebo modelového rizika) ako dôsledok operačného zlyhania. Operačné zlyhanie, úmyselné zlé kroky alebo chyby zamestnancov, právne (dokumentačné) zlyhanie alebo nepriaznivé zmeny v regulačných požiadavkách, postihujúce príslušné transakcie“. (Belás, 2008 a, s. 68).

§ 23 ods. 6 zákona č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov operačné riziko definuje ako riziko vyplývajúce z nevhodných alebo chybných vnútorných postupov, zo zlyhania ľudského faktora, zo zlyhania používaných systémov alebo z vonkajších udalostí. (Medveď, 2012, s. 297)

Podľa Belása (2010, s. 162-163) je operačné riziko charakterizované:

- transakčným rizikom, ktoré je rizikom straty z uskutočňovania operácií v dôsledku chýb pri uskutočňovaní operácií, chýb vyplývajúcich zo zložitosti produktov a neschopnosti súčasných systémov ich uskutočňovať, chýb v zaúčtovaní obchodov, chýb pri vysporiadaní obchodov, nezámerne poskytnutie alebo prijatie komodít a v neadekvátnej právnej dokumentácii,
- rizikom operačného riadenia, ktoré je rizikom straty z chýb v riadení aktivít vo front, middle a back Office, ide o neidentifikovateľné obchody nad limit, neautorizované obchodovanie jednotlivými obchodníkmi, podvodné operácie vzťahujúce sa k obchodovaniu a spracovaniu vrátane chybného zaúčtovania a falšovania, pranie peňazí, neautorizovaný prístup k systému a modelom, závislosť na obmedzenom počte osôb personálu a o nedostatok kontroly pri spracovaní obchodov.
- rizikom systému, ktoré je rizikom straty z chýb v systémoch podpory, ide o chyby v počítačových programoch, o chyby v matematických vzťahoch modelov, o nesprávne a oneskorené podanie informácií vedeniu, o chyby v jednom alebo vo viacerých podporných systémoch, o chyby pri prenose dát a o nesprávne plánovanie nepredvídateľných (náhodných) udalostí v prípade výpadku systému alebo prenosu dát.

Z obsahu pojmu sú explicitne vylúčené strategické a reputačné riziko. Naopak jeho súčasťou je tiež:

- **právne riziko** - riziko straty vyplývajúcej najmä z nevymožiteľnosti bankových pohľadávok, hrozby neúspešných súdnych sporov alebo rozsudkov s negatívnym vplyvom na banku;
- **regulačné riziko** - riziko straty vznikajúcej v dôsledku náhlych zmien regulačných požiadaviek obsiahnutých v zákonoch, ale aj príslušných aktoch NBS a Ministerstva financií Slovenskej republiky, ako aj smerniciach Európskej únie;
- **riziko outsourcingu** - riziko vznikajúce v rámci procesu dlhodobého zabezpečovania činností slúžiacich na podporu výkonu bankových činností pre banku inou osobou na zmluvnom základe, s cieľom dosiahnutia vyššej efektívnosti výkonu bankových činností.¹
- **riziko likvidity** - zahŕňa schopnosť banky v prípade potreby zbaviť sa svojich aktív za čo najvýhodnejšiu cenu a v čo najkratšom časovom horizonte. Vo vzťahu k bankovému klientovi spočíva najmä v schopnosti banky vyplatiť mu na požiadanie jeho vklady riadne a včas, teda k okamihu, kedy o ich vyplatenie požiada a v plnej výške, resp. v rozsahu ním požadovanej sumy;
- **systémové riziko** - súčasťou sú potenciálne všetky skôr uvedené riziká. Jeho podstata spočíva v tom, že neschopnosť jedného z účastníkov bankového systému splniť si svoje záväzky voči inému účastníkovi v čase, keď sú splatné, môže spôsobiť podobnú neschopnosť ďalších účastníkov. V extrémnych prípadoch môže ísť teda o reťazovú reakciu s efektom ohrozenia stability celého platobného systému.
- **riziká vyplývajúce zo vzájomného vzťahu medzi bankou a jej klientom**, ktoré ohrozujú nielen samotnú banku, ale predovšetkým jej klientov a banka by im mala venovať prinajmenšom rovnakú pozornosť ako samotným finančným rizikám.

Jednotlivé banky v rámci komplexného procesu riadenia rizika zameriavajú svoju pozornosť na monitoring a analýzu krátkodobého vývoja jednotlivých rizík a ako dôsledok zistených skutočností priebežne upravujú svoje

¹ Metodické usmernenie Úseku bankového dohľadu č. 6/2004 k využívaniu outsourcingu bankami

procesy. Zmeny v organizácii, procesoch, ako aj kontrolách bankových inštitúcií sú zároveň podmienené zvyšujúcimi sa požiadavkami na bezpečnosť ako nevyhnutný atribút činnosti každej komerčnej banky

Olejár (2013, s. 27) uvádza, že po identifikácii rizík je potrebné rozhodnúť, akým spôsobom sa na vzniknuté riziká bude reagovať. Podľa autora existujú štyri možné riešenia:

- Redukcia rizika. V tomto prípade organizácia prijíma opatrenia (technické, organizačné, personálne a iné) zamerané na zníženie pravdepodobnosti naplnenia a/alebo dôsledkov hrozby tak, aby sa hodnota výsledného rizika dostala pod úroveň akceptovateľného rizika.
- Zachovanie rizika, ak je úroveň rizika nižšia ako úroveň akceptovateľného rizika, organizácia nemusí prijímať žiadne opatrenia.
- Vyhnutie sa riziku. Prichádza do úvahy vtedy, keď by opatrenia na redukcii rizika boli príliš nákladné, ale hodnota rizika je vyššia ako úroveň akceptovateľného rizika. Organizácia zmení podmienky, ktoré viedli k neprijateľne vysokému riziku, napríklad použitím iného riešenia.
- Prenesenie rizika. Organizácia môže preniesť riziko na iný subjekt, ktorý ho dokáže efektívnejšie riešiť. (Príkladmi prenesenia rizika sú napr. zmluvy s dodávateľom o skrátenej dobe servisného zásahu, outsourcing problematických činností, poistenie).

Samostatnou oblasťou, kde výrazne stúpa riziko je elektronické bankovníctvo. Podľa Koskosasa (2011, s. 82 - 83) poskytuje elektronické bankovníctvo obrovské výhody pre klientov bánk pokiaľ ide o jednoduchosť a náklady na transakcie, ale predstavuje tiež nové výzvy pre banky v oblasti bezpečnosti finančných systémov, pri ktorých navrhovaní a implementácii je potrebné zohľadniť bezpečnostné opatrenia a kontroly.

Kľúčovým faktorom ďalšieho rozvoja e-bankovníctva zostáva bezpečnosť a zaistenie dôvery. To je celosvetovým problémom, ktorý je rovnako naliehavý v USA, Európe i Japonsku. V minulosti bolo dostatočné zabezpečenie pomocou jednoduchých hesiel. Spolu s rastom počtu finančných transakcií vykonávaných cez internet rastie aj počet podvodov a krádeží, a preto musia banky venovať oveľa väčšiu pozornosť ochrane citlivých informácií tvrdí Korauš (2011, s.242).

ZÁVER

Na riadenie rôznych rizík sa v súčasnosti používa množstvo odlišných metód a techník. Smernice, normy a štandardy sú medzinárodne uznávané nástroje, ktoré môžu pomôcť organizáciám efektívnejšie implementovať tieto techniky. Banky majú osobitne definované zásady zaobchádzania s rizikami, procesy a technicko-organizačné štruktúry, ciele rizika a limity. Pravidelne ich identifikujú a následne riadia, sledujú, minimalizujú a vykazujú všetky riziká spojené s použitím finančných nástrojov. Monitorujú a analyzujú krátkodobý vývoj všetkých rizík, na základe čoho priebežne upravujú svoje procesy. Zároveň banky kladú veľmi veľký dôraz na riadenie rizika likvidity a dodržiavanie regulačných požiadaviek Národnej banky Slovenska pre túto oblasť.

Problematika bankovej bezpečnosti predstavuje vo svojej podstate oblasť obsahujúcu nespočetné množstvo aspektov, ktoré možno skúmať z rôznych uhlov pohľadu. Bankovú bezpečnosť a riziká s ňou spojené nemožno v praxi podceňovať ale naopak je potrebné venovať jej náležitú pozornosť.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] BELÁS J. a kol., 2008. Komerčné banky, teória, riadenie, obchody. 1. vyd. Žilina : Georg, 2008, 212 s. ISBN 978-80-969161-8-4.
- [2] BELÁS, J. - DEMJAN, V. 2009. Finančné riadenie komerčnej banky, Žilina: Georg, 2009, 155 s. ISBN 978-80-89401-06-2.
- [3] BELÁS J. 2010. Management komerčných bánk, bankových obchodov a operácií. 1.vyd. Žilina : Georg, 2010, 470 s. ISBN 978-80-89401-18-5.
- [4] JÍLEK, J. 2000. Finanční rizika. Praha: Grada Publishing, 2000, 635 s. ISBN 80-7169-201-8
- [5] KAŠPAROVSKÁ V. a kol., 2006. Řízení obchodních bank, 1. vyd., Praha : C.H. Beck, 2006, 330 s. ISBN 80-7179-381-7.
- [6] KORAUŠ, A. 2011. Finančný marketing. Bratislava: Sprint dva, 2011, 535 s. ISBN:978-80-89393-31-2
- [7] KOSKOSAS, I. 2011. E-banking security: A communication perspective In Risk management, ISSN 1460-3799, 2011, Vol. 13, s. 81-99.
- [8] MEDVEĎ, J. a kol. 2012. Banky teória a prax. Bratislava : Sprint 2 s.r.o., 2012, 576 s. ISBN 978-80-89393-73-2



- [9] OLEJÁR, D. 2013. Manažment informačnej bezpečnosti In Informačná bezpečnosť [online] Bratislava : Ministerstvo financií Slovenskej republiky, 12.12.2013 [cit: 2015-2-23] 287 s. Dostupné na internete: <http://www.informatizacia.sk/ext_dok-stud_2014_02_veduci/16985c>.
- [10] RUSKO, M. 2006. Bezpečnostné a environmentálne manažérstvo. 1.vyd. Žilina : STRIX, 2006, 389 s. ISBN 80-969257-9-2
- [11] POLOUČEK, S. a kol. 2006. Bankovníctví. Praha : CH Beck, 2006, 716 s., ISBN 80- 7179-462-7
- [12] RUSKO, Miroslav - KRÁLIKOVÁ, Ružena. Implementation of Environmental Oriented Monitoring in the Manufacturing Company. In Advanced Materials Research : 4th International Conference on Manufacturing Science and Technology, ICMST 2013, Dubai, United Arab Emirates, 3 - 4 August 2013. s.1225-1230. ISSN 1022-6680.
- [13] ZIMKOVÁ, E. 2009. Bankovníctvo. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, 2009, 284 s., ISBN 978-80-8083-801-0.

ADRESY AUTOROV

Doc. Ing. Anton KORAUS, PhD., LL.M., MBA

Vysoká škola ekonomiky a manažmentu verejnej správy v Bratislave, Katedra manažérskej informatiky, Furdekova 16, 851 04 Bratislava, Slovak Republic, E-mail: akoraus@gmail.com

Ing. ROMAN ŠÍP,

♦ SOŠP, Račianska 190, 835 26 Bratislava, sip@polygraficka.sk

♦ Fakulta podnikového manažmentu, Ekonomická univerzita v Bratislave, Dolnozemska cesta 1 852 35 Bratislava

RECENZIA TEXTOV V ZBORNÍKU

Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS

Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.