Globálne existenciálne riziká / Global existential risks ´2014
Zborník z medzinárodnej konferencie, 11. december 2014, Bratislava
Proceedings of the International Conference, December 11, 2014, Bratislava, Slovakia
■ RUSKO,M.- KLINEC,I.[Eds.] ■ Žilina: STRIX/*Edícia ESE-21*, ISBN 978-80-89281-99-2 ■

TENDENCIE VÝVOJA BEZPEČNOSTNÝCH RIZÍK V BANKOVOM SEKTORE A MOŽNOSTI ICH ELIMINÁCIE

Anton KORAUŠ

DEVELOPMENT TRENDS IN SECURITY RISKS IN BANKING SECTOR AND POSSIBLE WAYS OF THEIR ELIMINATION

Abstrakt

Riziká sa objavujú vo všetkých oblastiach ľudskej činnosti a predstavujú potenciálnu stratu. Tiež bankové inštitúcie sú vystavené rôznym druhom rizík. Medzi základné kategórie rizík, ktorým banky pri výkone svojej činnosti čelia, patrí riziko úverové, trhové, riziko likvidity a operačné riziko. Pre banky je veľmi dôležité, aby jednotlivé riziká dokázali presne rozoznať a odlíšiť 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: *bankové inštitúcie, bankové riziká, úverové riziko, trhové riziko, riziko likvidity, operačné riziko*

Abstract

The risks emerge in all fields of human activities and represent a potential loss. Likewise other institutions, the banking institutions are also exposed to various kinds of risks. The basic categories of banking risks include loan risk, market risk, liquidity risk and operational risk. In order to be able to deal with them, it is of great importance to be able to distinguish them. 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 banking institutions, banking risks, loan risk, market risk, liquidity risk, operational risk*

Úvod

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.

Základné riziká bankového podnikania sú determinované existenciou dôvery v stabilitu bankového systému. Polouček a kol. (2006) definuje dôveru komerčnej banky nasledovne: „Ve finanční teorii existuje celá řada funkcií důvěry v banku – v úvahu obvykle berou výši kapitálu banky, stabilitu výnosov, transparentnost banky a také státni garance (G).“ Podľa autora funkcia dôvery závisí od týchto faktorov:

$$\text{Dôvera} = f\,[\,NW, \sigma\,ROA, IQ, L\,(G, \sigma L, \sigma D)\,]$$

kde:

NW čistá hodnota (imanie) banky,
σ ROA stabilita výnosov meraná štandardnou odchýlkou výnosov z aktív,
IQ kvalita informácií (transparentnosť) týkajúca sa výnosov a kvality aktív,
L likvidita, ktorá je funkciou štátnych garancií (G), variability dopytu po úveroch (σL) a variability toku depozít (σD).

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, dodržovanie pravidiel obozretného podnikania bánk,
- legislatívne garancie pre vkladateľov (napr. zákon o ochrane vkladov),
- optimálny bankový marketing. (Belás a kol., 2010)

Bankový systém má svoje špecifické črty, ktoré významným spôsobom determinujú základné podmienky pre podnikanie obchodných bánk. Medzi najvýznamnejšie špecifické črty možno zaradiť: peniaze ako predmet podnikania, atypická štruktúra bilancie komerčnej banky a prísna regulácia bankového sektora.
Z tohto kontextu vyplýva, že kategória bezpečnosti je významnou úlohou pre bankový manažment. Existencia bezpečnostných problémov a ich medializácia môžu významným spôsobom ovplyvniť dôveryhodnosť komerčnej banky.

Charakteristika rizík v bankovníctve

Všeobecne rizikom rozumieme nebezpečenstvo vzniku škody, poškodenia, straty alebo zničenia, na rozdiel od neistoty u rizika sme schopní priradiť k budúcim situáciám ich pravdepodobnosti výskytu v oblasti ekonómie a financií je pojem riziko používaný v súvislosti s nejednoznačným priebehom ekonomických a finančných procesov a ich výsledkov.

Z hľadiska koncepčného a metodického musí charakteristika posudzovania rizík v bankovom sektore vychádzať rovnako, ako pri posudzovaní rizík všeobecne 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 obmedzovane 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)

Bezpečnosť je základným predpokladom pôsobenia komerčnej banky v bankovom prostredí a súvisí s celým radom bankových oblastí. Tak, ako všetky typické činnosti banky aj zaistenie bezpečnosti je ovplyvňované a podmieňované rôznymi faktormi.

Patria k nim subjektívne hľadiská, ktoré sú dané typom a veľkosťou banky, ako i objektívne hľadiská, ktoré sú dané legislatívnymi prostriedkami, t.z. platnými zákonnými normami a ďalšími hľadiskami vyplývajúcimi z vonkajšieho prostredia banky, akými sú napr. etické normy chovania jednotlivých podnikateľských subjektov.

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, trhové riziko, riziko likvidity, operačné riziko a obchodné riziko.

Olejár (2013, s. 27) uvádza, že po identifikácií 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 redukciu 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).

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, nezámerné poskytnutie alebo prijatie komodít a v neadekvátnej právnej dokumentácií,
- 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) udalosti v prípade výpadku systému alebo prenosu dát.

Trendy v oblasti bezpečnosti v e-bankovníctve

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 implementácií je potrebné zohľadniť bezpečnostné opatrenia a kontroly.

Bezpečná komunikácia v rámci elektronického bankovníctva je z pohľadu vyššieho manažmentu banky dôležitá, nakoľko môže prispieť k zlepšeniu bezpečnosti elektronického bankovníctva ako celku.

Korauš (2011, s.242) tvrdí, že 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. Štúdia švédskej spoločnosti Todos Data Systems (2009), ktorá sa zaoberá poskytovaním bezpečnostných riešení pre autentizáciu na diaľku, zistila, že široká verejnosť si je vedomá existencie rizík v súvislosti s používaním internetu na finančné transakcie. Napríklad štvrtina opýtaných Švédov plne neverí svojej internetovej banke, zatiaľ čo 10% užívateľov internetu vo Švédsku sa nazdáva, že sa stali predmetom snahy o nejaký druh podvodu po sieti.

Strach z krádeže identity potom vedie veľa ľudí k tomu, že majú obavy z používania internetových systémov kvôli predpokladanej nižšej bezpečnosti. Preto sa stáva kriticky dôležitou implementácia dvajfaktorových autentizačných riešení založených na niečom, čo užívateľ pozná v kombinácii s niečím, čo má pri sebe. Dvojfaktorová autentizácia, ktorá kombinuje stále heslo a meniaci sa PIN alebo heslo, je dosiahnuteľná napríklad pomocou PIN kalkulátorov.

Ďalšou možnosťou sú zariadenia pre autentizáciu s použitím vkladanej tzv. smart card. Zariadením môže byť prenosná čítačka. Tieto čítačky sú rovnaké pre všetkých klientov, čo znižuje náklady oproti autentizačným zariadeniam, vytvoreným špecificky pre každého klienta. Ochrana proti zneužitiu spočíva v unikátnosti karty pre každého klienta. Čítačku je možné poslať klientovi poštou alebo odovzdať mu ju na pobočke. Ak sú čítačky dostatočne jednoduché z hľadiska obsluhy, odpadajú náklady na informačnú podporu zo strany banky.

Podvodníci sú však vynaliezaví, a tak sa objavili aj prípady útoku na dvojfaktorovo zabezpečený prístup do banky, a to tým spôsobom, že podvodná stránka predstierala, že je stránkou danej banky a snažila sa o to, aby klienti vyplnili ako stále heslo, tak aj jednorazovo generovaný údaj do falošnej stránky.

Ak banka neplánuje vydávať tzv. smart card, má voľbu spomedzi ďalších možností:

- začať vydávať špecializované smart card len na účel generovania jednorazového hesla,
- používať špeciálne plošné heslá,
- zaviesť hardwérové tokeny,
- používať jednorazové heslá zasielané pomocou SMS správ.

Dôležité je vybudovať užívateľské rozhranie na vkladanie jednorazového hesla, ktoré bude rovnaké bez ohľadu na zariadenie, ktoré vygenerovalo heslo. V tomto prípade je jednoduchšie v neskoršom štádiu prechádzať k iným riešeniam vytvárajúcim jednorazové heslá. Server, ktorý overuje toto heslo, musí byť schopný overiť v rovnakom čase všetky zariadenia. Už prechod od statického hesla k jednorazovému je veľkým krokom vpred v oblasti bezpečnosti. Ďalším krokom môže byť požiadavka na koncového užívateľa, aby vpisoval do čítačky niektoré údaje, ktoré sa týkajú transakcie. Výsledok z čítačky bude záväzný pre užívateľa i banku.

Bezpečnosť operácií v rámci elektronického bankovníctva do veľkej miery ovplyvňuje aj medzinárodná, či lokálna regulácia menových autorít alebo štátu prostredníctvom zákonov a nariadení, tá však v súčasnosti v tejto oblasti absentuje.

Záver

Bankové podnikanie je spojene okrem špecifikácie rizík aj s rizikami, ktoré sú bežné v iných oblastiach podnikania, ako napr. riziko lúpeže, riziko požiaru alebo záplavy. Tieto riziká a aj celý rad ďalších rizík obdobného charakteru sú celkom alebo z časti poistiteľné, manažment banky musí garantovať snahu o minimalizáciu strát. Existujú aj riziká počítačovej defraudácie alebo defraudácie zamestnancov a členov vo vedení banky. Tieto riziká sú pochopiteľne veľmi závažné a vystavená je im každá banka. Pokiaľ v nej dôjde k javom podobného charakteru, dôsledky môžu mať veľmi negatívny dopad

na celkové aktivity banky a môžu sa odraziť v strate likvidity, solventnosti a dôveryhodnosti banky, resp. môžu viesť k jej bankrotu.

Komplexnosť rizík sa odráža v ich samotnej klasifikácii, ktorá je v jednotlivých štúdiách a výskumných prácach, rovnako ako v rôznych ekonomických a finančných teóriách, publikáciách a učebniciach a tiež v jednotlivých krajinách veľmi rôznorodá. (Polouček, 2006, s.283)

S ohľadom na vyššie uvedené môžeme konštatovať, že riadenie rizika v bankách podlieha prísnym regulačným opatreniam stanoveným všeobecne záväznými predpismi a požiadavkami regulačného orgánu. Ako dôsledok finančnej krízy vznikla potreba ešte viac posilniť kapitálovú vybavenosť finančných inštitúcií a tak sa diskusie zameriavajú na možnosti zavedenia alternatívnych ukazovateľov primeranosti vlastných zdrojov.

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. Bankovnictví. Praha : CH Beck, 2006, 716 s., ISBN 80- 7179-462-7
[12] ZIMKOVÁ, E. 2009. Bankovníctvo. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, 2009, 284 s., ISBN 978-80-8083-801-0.

ADRESA AUTORA

Anton KORAUŠ, Ing., PhD., LL.M.,MBA, Národná rada Slovenskej republiky, Námestie Alexandra Dubčeka 1, 812 80 Bratislava 1, Slovenská republika, e-mail: akoraus@gmail.com

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.