Acta oeconomica et informatica 1
Nitra, Slovaca Universitas Agriculturae Nitriae, 1999, s. 14—16

BEZPEČNOSŤ INFORMAČNÉHO SYSTÉMU KOMERČNÝCH BÁNK
INFORMATION SYSTEM SECURITY OF COMMERCIAL BANKS

Marián KOČNER, Ondrej BULIK
Slovenská poľnohospodárska univerzita v Nitre

The aim of this work is to solve problems concerning the bank information system of commercial banks, where a big emphasis is laid on the security of the information system. At the present time, not only bank specialists but also top experts in creation and implementation of bank softwares are engaged in the solution of these problems. The paper advances from empiric analyses of the information system security to general theoretical starting-points and theses. It focuses on the problems of data protection by minimalising and/or excluding the possibility of leakage of information and its subsequent misuse, as well as on information security, and defines the levels of security usable in building the information system. Also, it deals with assessing the bank information system through an external audit with the aim to analyse the regularity of operations and reliability of the information system in terms of the criteria required, and through an internal audit, which is an important security component of the information system.

Key words : financial market, bank, information system, security, data protection, reliability, audit

Vznik a súčasný dynamický rozvoj slovenskej štátnosti otvoril perspektívy novej kvality rozvoja spoločnosti vo všetkých oblastiach národného hospodárstva. To sa plne vzťahuje na bankovú sféru, v ktorej sa veľký dôraz kladie aj na bezpečnosť informačného systému. Pod pojmom informačný systém rozumieme funkčný celok, ktorý zabezpečuje cieľavedomé a systematické zhromažďovanie, spracovávanie, uchovávanie a sprístupňovanie informácií. Zahŕňa informačnú základňu, technické a programové prostriedky, technológie, procedúry a komunikačné cesty. Efektívne využívanie informačného systému však vyžaduje okrem efektívne vybudovaného informačného systému aj jeho zabezpečenie komplexnou ochranou.

Materiál a metódy

Bankové informácie, s ktorými banka vstupuje do kontaktu so zákazníkmi a partnermi, majú vzrastajúcu hodnotu a sú priamo úmerné aktívam banky. Väčšina týchto informácií má dôverný charakter, čo si vyžaduje primeranú ochranu a bezpečnosť vo všetkých fázach ich spracovania.

Z tohto pohľadu je cieľom zhodnotiť bezpečnosť a spoľahlivosť informačného systému, riešiť problémy bezpečnosti a spoľahlivosti informačného systému v komerčných bankách. Postupuje sa od empirických analýz bezpečnosti informačného systému, ktoré smerujú k všeobecným teoretickým východiskám a tézam, vychádza sa z nasledujúcich okruhov problematiky, ako sú:

- ochrana dát,
- informačná bezpečnosť,
- úroveň bezpečnosti,
- audit informačného systému.

Dosiahnuté výsledky a diskusia

Informačnú bezpečnosť chápeme ako proces, t.j. ochranu informácií proti strate dôvernosti, integrity a dostupnosti počas ich spracovávania, ukladania a prenosov prostredníctvom fyzických, technických a organizačných opatrení. Informácie musia byť zabezpečené voči úmyselnému, ale i náhodnému zneužitiu a nehodám. Pri akomkoľvek spôsobe úniku rastie riziko finančných strát. Možnosť straty dôvernosti informácie je najviac vnímanou hrozbou. Všeobecne sa hodnota informácie vzťahuje hlavne k jej dôvernosti. Daná informácia je výlučná a je určená len vymedzenému okruhu ľudí.

Cieľom ochrany dát je zaistenie bezpečnosti takým spôsobom, aby sa minimalizovala, prípadne vylúčila možnosť úniku informácie a jej následného zneužitia. K ochrane informačného systému existuje celý rad závažných dôvodov, ktoré vyplývajú z:

- použitého programového vybavenia,
- použitých komunikačných prostriedkov a komunikačných komponentov,
- organizácie práce užívateľov (rôzne oprávnenia),
- pôsobenia vonkajších vplyvov (napájanie, prepätie, mechanické vplyvy, cielené útoky),
- druhu ohrozenia,
- dôsledku ohrozenia.

Úrovne bezpečnosti informačného systému

Viacúrovňové zabezpečenie informačného systému zaisťuje, že aj v prípade porušenia určitej bezpečnostnej úrovne ostávajú ďalšie úrovne aktívne. Preto možno použiť pri budovaní informačného systému tieto úrovne bezpečnosti:

1. úroveň - Fyzický prístup k miestu možnej práce s informačným systémom

Táto úroveň zahŕňa fyzické opatrenia, ktoré súvisia s ochranou objektov a budov, ale aj riadenia vstupov do nich a do ich okolia. Môžu sa tu uplatňovať tak mechanické zábrany, ako aj systémy elektronického zabezpečenia, signalizácie a strážna služba.

2. úroveň - Lokálny prístup pre prácu s PC

Patria sem autentizačné prostriedky a metódy vrátane digitálneho podpisu a prostriedky pre ochranu telekomunikácií. Cieľom

autentizácie je zabrániť neautorizovaným užívateľom v prístupe k počítaču a jeho zdrojom (k spracovaným, ukladaným a prenášaným informáciám) a ovplyvňovaní prebiehajúcich procesov. Väčšinou sa využíva autentizácia prostredníctvom hesiel, ktoré sa zadávajú z klávesnice počítača. Tento spôsob je lacný a málo bezpečný. Okrem tohto spôsobu autentizácie existuje aj možnosť využívať predmety, ktoré sú vo vlastníctve užívateľa, ako sú magnetické a čipové karty a prenosné bezpečnostné moduly (s výnimkou magnetických kariet sú vysoko bezpečné) a najmodernejšie spôsoby zabezpečenia prostredníctvom rôznych biometrických charakteristík človeka, ako je odtlačok prsta, obraz očnej sietnice, biomotorická charakteristika podpisu a pod. (drahé, ale pohodlné a prakticky neprekonateľné). Digitálny podpis je považovaný za "tvrdú" formu autentizácie, ktorá umožňuje zaručiť neodvolateľnosť príkazu alebo požiadavky. Dovoľuje autentizovanému subjektu označiť alebo overiť údaje, ktorých pôvod nemožno poprieť.

Súčasná bezpečnosť informačného systému najviac využíva spôsoby zabezpečenia prostredníctvom hesiel a v niektorých komerčných bankách, prevažne na centrálach, zabezpečenie pomocou čipových kariet. Samotný lokálny prístup pre prácu s PC je zabezpečený spoľahlivým softvérom, ktorý zabráni prípadné nepovolené vstupy do lokálnej stanice, ale i do celého informačného systému banky. Takýto softvér vo väčšine prípadov dovoľuje aj zadefinovanie povolených prístupov jednotlivých aplikácií k daným užívateľom. Napríklad:

- možnosť pracovať len s konkrétnym programovým vybavením, ktoré užívateľ nemôže nijako modifikovať,
- možnosť pracovať len v povolených dňoch a dennej dobe,
- možnosť pracovať len z konkrétnej pracovnej stanice,
- možnosť kopírovania diskiet len v rámci siete pobočiek konkrétnej banky, čím sa zabraňuje prieniku informácií z banky alebo do banky.

3. úroveň - Prístup do lokálnej počítačovej siete banky

Pre prácu v sieti je potrebná ďalšia autorizácia, nezávislá od predchádzajúcej úrovne. Táto umožní užívateľovi prácu s informačným systémom a zdieľanie sieťových služieb, ako sú:

- zasielanie internej pošty,
- zdieľanie tlačiarní a sieťových diskov,
- sieťová inštalácia a iné.

4. úroveň - Prístup do aplikačného softvéru informačného systému

Tak ako v predchádzajúcich úrovniach, aj tu je potrebná autorizácia užívateľa pred vstupom do aplikačného softvéru. Okrem tejto úrovne ochrany je aj možnosť využitia prístupu iba do niektorých modulov, tabuliek alebo konečných volieb pre konkrétneho užívateľa.

5. úroveň - Prístup do operačného systému

Táto úroveň je zabezpečená a garantovaná samotným operačným systémom a prístup do nej majú len informatici alebo správcovia bankového systému.

Audit informačného systému

Audit informačného systému je overenie, či skutočný stav systému a jeho bezpečnostný subsystém zodpovedajú stavu predpokladanému, respektíve predpísanému. Stav takéhoto bankového informačného systému treba priebežne vyhodnocovať vnútorným auditom a pravidelne vonkajším auditom.

Vnútorný audit informačného systému

Dôležitým bezpečnostným prvkom informačného systému je jeho vnútorný audit. Ide o historické zaznamenávanie jednotlivých činností a dôležitých udalostí, ktoré majú vplyv na bezpečnosť systému. V prípade mimoriadneho stavu musí audit zabezpečiť jednoznačnú identifikáciu udalostí, čo znamená priradiť udalosti dátum, čas a odkiaľ čo a kto vykonal. Napríklad na úrovni prístupu pre prácu s PC je dôležité vykonať audit:

- prihlásenia užívateľa do PC,
- aplikácií spustených užívateľom a
- odhlásenie užívateľa.

Na úrovni prístupu do aplikačného softvéru je dôležité vykonať audit:

- prístupu užívateľa do aplikácie,
- použitých volieb,
- vykonaných zmien,
- vykonaných transakcií a
- odchodu užívateľa z aplikácie.

Informačný systém komerčných bánk je budovaný z hľadiska bezpečnosti ako systém viacúrovňový so selektívnym prístupom a s maximálne možnou mierou zabezpečenia auditu dôležitých činností pri práci s informačným systémom.

Vonkajší audit informačného systému

Podľa zákona č. 58/1996 Z.z., ktorým sa mení a dopĺňa zákon č. 21/1992 Zb. o bankách v znení neskorších predpisov, sú banka a pobočka zahraničnej banky povinné raz ročne zabezpečiť overenie spoľahlivosti informačného systému, ktorým sú spracúvané bankové údaje. Pod pojmom overenie spoľahlivosti možno chápať posúdenie dodržiavania určených kritérií a predpisov, ktoré by mali vychádzať zo všeobecne prijatých medzinárodných štandardov, aplikovaných na naše podmienky. Zmyslom auditu v tejto podobe je analyzovať správnosť fungovania a dôveryhodnosť informačného systému z hľadiska požadovaných kritérií na spoľahlivý a bezpečný proces prenosu a spracovania informácií, ako aj ochranu pred nečakanou poruchou, haváriou, prípadne pred iným nežiaducim vonkajším vplyvom. Overenie spoľahlivosti informačného systému poskytujú aj slovenské pobočky medzinárodných audítorsko-poradenských firiem, ako je napríklad Arthur Andersen, Deloitte - Touche, KPMG a iné.

Záver

Informačné systémy v súčasnej dobe zaisťujú chod tak výrobných podnikov, ako aj štátnej správy, zdravotníctva, finančníctva i terciárnej sféry. Bez informačných technológií je práca s informáciami dnes nielen neefektívna, ale aj nepredstaviteľná. Klient má právo na istotu, že prostriedky zverené banke a operácie s nimi sú maximálne zabezpečené. Pojem spoľahlivosť informačného systému zahŕňa riešenie otázok dodávateľov jednotlivých súčastí, servisu, otázky podpory zo strany špecializovaných pracovísk banky, zaškolenie užívateľov a samozrejme i otázky celkovej bezpečnosti.

Súhrn

Ide o riešenie problémov bankového informačného systému v komerčných bankách, kde sa veľký dôraz kladie na bezpečnosť informačného systému. Touto problematikou sa v súčasnej dobe zaoberá celý rad bankových špecialistov, ale aj špičkoví odborníci z oblasti tvorby a realizácie bankového softvéru. Postupuje sa od empirických analýz bezpečnosti informačného systému, ktoré smerujú k všeobecným teoretickým východiskám a tézam. Konkrétne ide o okruhy problematiky ochrany dát minimalizovaním, prípadne vylúčením možnosti úniku informácie a následného zneužitia informačnej bezpečnosti. Vymedzujú sa úrovne bezpečnosti, ktoré možno použiť pri budovaní informačného systému a vyhodnocuje sa bankový informačný systém, vonkajší audit, ktorého zmyslom je analyzovať správnosť fungovania, dôveryhodnosť informačného systému z hľadiska požadovaných kritérií a vnútorný audit, ktorý je dôležitým bezpečnostným prvkom informačného systému.

Kľúčové slová: finančný trh, banka, informačný systém, bezpečnosť, ochrana dát, spoľahlivosť, audit

Literatúra

BORÁK, P.: IS Audit - služba nového veku. In: Trend, 1997, č. 12, s. 3c.
BREZINA, Ľ.: Chúlostivá spoľahlivosť bankových systémov. In: Infotrendy, príl. Trend, 1996, č. 2, s.16-17.
KOČNER, M. — SERENČÉŠ, P. — BULIK, O.: Informačný systém finančného trhu. In: Acta operativo oeconomica, 51. Nitra : VŠP, 1996, s. 137-141.
KOČNER, M.: Informačná funkcia kapitálového trhu. In: Acta operativo oeconomica, 50. Nitra : VŠP, 1995, s. 227-229.
MAKÚCH, J. a kol.: Komerčné banky: Bankové operácie: Styk s bankou. Bratislava: SOFA, 1994. 160 s.

Kontaktná adresa:
doc.Ing. Marián Kočner, PhD.
Katedra informačných systémov a financií, Fakulta ekonomiky a manažmentu, Slovenská poľnohospodárska univerzita v Nitre, Tr. A. Hlinku 2, 949 76 Nitra, tel.: 087/60 11 51
Ing. Ondrej Bulik
ČSOB, ul. F. Mojtu 4, 949 01 Nitra

Acta oeconomica et informatica 1
Nitra, Slovaca Universitas Agriculturae Nitriae, 1999, s. 16—18

FÁZY EKONOMICKEJ ŠKODY VO VZŤAHU K ROVNICI BILANCII IMISIÍ

THE RELATIONSHIP BETWEEN PHASES OF ECONOMICAL DAMAGE AND THE EQUATION OF IMISSION BALANCE

Ondrej HRONEC, Anton SELVEK
Slovenská poľnohospodárska univerzita v Nitre

The production of exhalation from different industrial and energy resources in Slovakia shows a decreasing trend. At present, domestic exhalation resources produce 330,000 t SO_2 225,000 t nitrogen x-oxids (NO_x), and 250,000 t fly ashes per annum. About 160,000 ha of agricultural soil is contaminated, and 30,000 ha is metallized and alcalized. The amount of damage from exhalations per hectare ranges from Skk 880 to 3, 500. In order to assess and quantify objectively the damage, it is necessary to know the equation of imission balance and the progress of the phases of economical damage.

Key words: exhalations, imission balance, phase of economical damage

Imisie sú závažným ekologickým a ekonomickým problémom aj preto, že Slovensko sa nachádza na okraji oblasti s najväčším diaľkovým prenosom škodlivín ovzdušia. Ide hlavne o plynné častice, kde sú zastúpené oxidy síry a dusíka. Významný podiel majú aj aerosoly, ktoré sú nositeľmi rizikových prvkov, hlavne ťažkých kovov.

Slovenské exhalačné zdroje (EZ) znížili ročnú produkciu SO_2 zo 660 tis. ton (r.1989) na súčasných 330 tisíc. Táto tendencia poklesu bude mať priaznivý priebeh, keď v zmysle protokolu podpísanom v Osle v roku 1994 by produkcia SO_2 v roku 2005 mala byť pod množstvom 300 tis. ton. Emisie oxidov dusíka (NO_x) predstavujú okolo 225 tis. ton ročne. Pochádzajú z teplární, dopravy a z elektrární. Tuhé úlety (prach a popolček) sa produkujú v množstve okolo 250 tis. ton ročne a ich pôvod je v metalurgii, v chemickom priemysle, pri výrobe vápna, cementu, magnezitových materiálov. Exhaláty spôsobujú vážne ekologické problémy s ekonomickými dôsledkami v poľnohospodárskej výrobe.

Materiál a metódy

Príčiny poškodzovania vegetácie imisiami z priemyslu aj vo väčších vzdialenostiach od EZ možno vysvetliť použitím rovnice bilancie imisií (Q_i) a jej členov, ktorú prvýkrát definovali HAJDÚK a KRCHO (1972) a hlbšie ju rozvíjajú HRONEC a HAJDÚK (1988), keď využívajú výsledky vlastného výskumu. Tieto poznatky aplikujeme pri stanovení výšky ekonomickej škody v poľnohospodárskej výrobe. Opierame sa o teóriu HADRABOVEJ (1991), ktorá priebeh ekonomickej škody v dôsledku vplyvu exhalátov rozdeľuje do piatich fáz. Tieto fázy porovnávame s rovnicou Q_i (HRONEC 1996).