V E S T N Í K

Národnej banky Slovenska

Čiastka 39 **Vydaná dňa 7. októbra 2004** **Ročník 2004**

NORMATÍVNA ČASŤ

ISSN 1335-3365

Cena čiastky: 38 Sk **Čiastka pre verejnosť – 13/2004**

Metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska z 1. októbra 2004 č. 7/2004

k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky

Účel usmernenia

Účelom usmernenia je v zmysle § 40 ods. 8 a 9 zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov stanoviť pre banky a pobočky zahraničných bánk (ďalej len „banky“):

a) predmet overenia stavu bezpečnosti informačného systému banky, ktorým sú spracúvané a uschovávané bankové údaje, a to z pohľadu zabezpečenia ochrany elektronického spracúvania a uschovávania údajov pred zneužitím, zničením, poškodením, odcudzením alebo pred stratou,
b) rozsah informácií poskytnutých bankou Národnej banke Slovenska o zabezpečení overenia bezpečnosti informačného systému banky.

Metodické usmernenie je zaradené do kategórie: **„Proces riadenia rizík“**.

Obsah usmernenia

A. Definícia overenia bezpečnosti informačného systému

1. Overenie bezpečnosti informačného systému banky je nezávislé, nestranné, nezaujaté a odborné posúdenie bezpečnostných vlastností informačného systému banky z hľadiska zabezpečenia celkovej bezpečnosti informačného systému najmä jeho efektívnosti, kvality a úrovne riadenia bezpečnostných rizík, dôvernosti, integrity, autenticity a dostupnosti informácií a spracúvaných údajov.

Definície pojmov

2. Pre potreby tohto metodického usmernenia sa rozumie:

a) aktívom informačnej bezpečnosti (ďalej len „informačné aktívum“) hmotný alebo nehmotný objekt, ktorý sa spolupodieľa na fungovaní a vytváraní informačného systému banky, najmä
   - údajové a dokumentačné aktíva najmä - databázy a dátové súbory, údaje a informácie, systémová dokumentácia, používateľské manuály, zácvikové materiály, prevádzkové alebo podporné procedúry, plány kontinuity, dohody o náhradných postupoch používaných v prípade zlyhania poskytovaných služieb alebo systému, archivované informácie,

- softvérové aktíva najmä - aplikačný softvér, systémový softvér, vývojové nástroje a pomocné programy, zdrojové knižnice programov, knižnice vykonateľných programov,
- fyzické aktíva najmä - počítačové vybavenie (procesory, monitory, laptopy, modemy), komunikačné vybavenie (smerovače, faxové prístroje, odkazovače), magnetické médiá (pásky, diskety, pevné disky, kompaktné disky), iné technické vybavenie (napájacie zdroje, klimatizačné jednotky), nábytok;

b) informačným systémom hmotné a nehmotné objekty, ktoré sú cielene vyberané alebo vytvorené a vzájomne cielene poprepájané za účelom zberu, výmeny, spracovania, uchovania, generovania a distribúcie informácií a údajov vo vopred definovanej štruktúre a čase, a to za účelom výkonu rozhodnutí, podpory rozhodovania a informovanosti.

B. Cieľ overenia bezpečnosti informačného systému

3. Cieľom overenia bezpečnosti informačného systému banky je poskytnúť primeranú istotu

- či bankou spracúvané a uchovávané údaje sú primerane zabezpečené pred zneužitím, zničením, poškodením, odcudzením, neoprávneným prístupom, zmenou alebo pred stratou,
- celkovú úroveň zaistenia bezpečnosti informačného systému a integrity, dostupnosti, dôvernosti a autenticity údajov z pohľadu domácej legislatívy a medzinárodne uznávaných štandardov,
- či informačný systém banky spĺňa náležitosti popísané v tomto usmernení a v akom rozsahu,
- či banka chápe bezpečnosť informačného systému ako nepretržitý každodenný proces, ktorý je vecou každého zamestnanca banky.

C. Frekvencia overenia bezpečnosti informačného systému

4. V zmysle ustanovenia § 40 ods. 8 a 9 zákona je banka povinná raz ročne zabezpečiť overenie bezpečnosti informačného systému a informovať o tom Národnú banku Slovenska.

D. Oprávnenosť k výkonu overenia stavu bezpečnosti informačného systému

5. Overenie bezpečnosti informačného systému môže vykonať odborne spôsobilá právnická osoba alebo fyzická osoba, ktorá sa nepodieľala na vypracovaní bezpečnostného projektu predmetného informačného systému, a u ktorej nie sú pochybnosti o jej nezávislosti, nestrannosti a nezaujatosti.

6. Osoba vykonávajúca overenie bezpečnosti informačného systému by mala byť vo svojich postojoch a výrokoch, týkajúcich sa overenia bezpečnosti informačného systému, objektívna a nezávislá od spoločností, ktoré sú v akomkoľvek záujmovom vzťahu k informačnému systému banky.

E. Predmet overenia

7. Predmetom overenia je celý informačný systém banky vrátane príslušnej dokumentácie a interných predpisov týkajúcich sa bezpečnosti informačného systému, prípadne jeho časť v zmysle plánu overenia stavu bezpečnosti informačného systému vypracovaného bankou.

F. Preverované oblasti

8. Banka môže v procese budovania, prevádzky a správy svojho informačného systému použiť aj niektorý z medzinárodne uznávaných štandardov pre zaistenie bezpečnosti

informačných systémov, pokiaľ obsahuje minimálne nasledujúce oblasti, ktoré sú predmetom overenia bezpečnosti informačného systému.

I. Bezpečnostná politika

9. Banka by mala mať predstavenstvom schválenú bezpečnostnú politiku, ktorá stanovuje ciele ktoré je potrebné v oblasti bezpečnosti informačného systému banky dosiahnuť a základné princípy a nástroje na dosiahnutie týchto cieľov.
Bezpečnostná politika by mala zahŕňať najmä:

- stanovenie cieľov, ktoré chce banka v oblasti informačnej bezpečnosti dosiahnuť,
- určenie základných princípov, nástrojov a postupov pomocou ktorých chce banka dosiahnuť stanovené ciele,
- určenie právomoci a zodpovednosti za dosiahnutie stanovených cieľov a za riadenie informačnej bezpečnosti,
- určenie osoby zodpovednej za bezpečnostnú politiku ako celok,
- plán aktualizácie bezpečnostnej politiky.

II. Organizácia a riadenie informačnej bezpečnosti v banke

10. Cieľom je zaistiť primeranú bezpečnosť informačných aktív a špeciálne tých, ku ktorým majú prístup tretie strany, zaistiť bezpečnosť informácií najmä ak sú spracúvané externou organizáciou. Organizácia informačnej bezpečnosti by mala zahŕňať:

- vytvorenie infraštruktúry informačnej bezpečnosti,
- zabezpečenie prístupu tretích strán,
- zaistenie bezpečnosti informačných aktív a informácií v prípade využívania outsourcingu.

11. Infraštruktúra informačnej bezpečnosti

Infraštruktúra informačnej bezpečnosti predstavuje cielene vytvorené riadiace orgány a pracovné skupiny, ktorých úlohou je riadiť a zaistiť požadovanú efektívnu úroveň bezpečnosti informačného systému (ďalej len „infraštruktúra“). Banka by mala mať predstavenstvom banky schválenú infraštruktúru pre riadenie informačnej bezpečnosti s jasne vymedzenými pracovnými činnosťami, právomocami a zodpovednosťami pre každý riadiaci orgán, pracovnú skupinu a pre každého ich člena. V rámci infraštruktúry by banka mala mať zabezpečený výkon najmä nasledovných činností:

- tvorba a aktualizácia bezpečnostnej politiky,
- celkové riadenie a koordinovanie projektovania, implementácie a údržby informačnej bezpečnosti v banke vrátane stanovenia právomocí a zodpovedností,
- monitorovanie a hodnotenie bezpečnostných incidentov a zmien vo vystavení informačných aktív ohrozeniam a následne prijímanie patričných rozhodnutí,
- zabezpečenie špecializovaného poradenstva pre informačnú bezpečnosť v rámci banky.

12. Zabezpečenie prístupu tretích strán

Na účely zaistenia bezpečnosti informačných aktív pred ohrozeniami vyplývajúcimi z prístupu tretích strán by banka mala:

- vypracovať procedúry pre riadenie rizík prístupu tretích strán k prostriedkom banky pre spracovanie informácií a k informáciám samotným,
- umožniť tretím stranám prístup len na základe platnej zmluvy s treťou stranou o jej prístupe k prostriedkom banky pre spracovanie informácií a k informáciám samotným,

- vyšpecifikovať tie informačné aktíva (technické zariadenia, dokumenty, informácie a pod.), ku ktorým by sa tretia strana nemala dostať za žiadnych okolností a prijať náležité opatrenia na ich ochranu,
- vytvoriť v zmluve s treťou stranou dostatočný priestor na operatívne opatrenia potrebné na riešenie nepredvídaných situácií a na koordináciu súbežného prístupu viacerých tretích strán.

13. Zaistenie bezpečnosti informačných aktív a informácií v prípade využívania outsourcingu
V prípade využívania outsourcingu by okrem ustanovení pre zabezpečenie prístupu tretích strán mala banka najmä:
- všetky dodávky zabezpečovať na zmluvnom základe,
- mať také metódy a procedúry pre hodnotenie a výber dodávateľa obstarávaných prostriedkov, ktoré zohľadňujú povinnosť zaistiť ochranu informačných aktív,
- mať procedúry pre výkon a hodnotenie testovania dodaných prostriedkov pred ich prevzatím a nasadením do produkčnej prevádzky,
- mať procedúry pre nasadenie a implementáciu dodaných prostriedkov.

III. Bezpečnostná klasifikácia informačných aktív a riadenie ich bezpečnosti
14. Cieľom bezpečnostnej klasifikácie informačných aktív a riadenia ich bezpečnosti je stanoviť a udržiavať efektívnu ochranu informačných aktív banky. Bezpečnostná klasifikácia informačných aktív a riadenie ich bezpečnosti zahŕňa:
- klasifikáciu informačných aktív,
- zodpovednosť za informačné aktíva.

15. Bezpečnostná klasifikácia informačných aktív
Na účely stanovenia spôsobu zaobchádzania s informačnými aktívami a zabezpečenia ich efektívnej ochrany by banka mala:
- vypracovať metodiku a procedúry bezpečnostnej klasifikácie (výber, zatrieďovanie, označovanie) informačných aktív,
- stanoviť a evidovať bezpečnostnú klasifikáciu vybraných informačných aktív v zmysle metodiky, jeho zreteľné označenie a umiestnenie,
- vhodným spôsobom oboznámiť zamestnancov s metodikou bezpečnostnej klasifikácie informačných aktív a s ich povinnosťami a zodpovednosťou, vyplývajúcimi z tejto klasifikácie,

16. Zodpovednosť za informačné aktíva
Na účely efektívnej ochrany informačných aktív by banka mala:
- stanoviť útvar zodpovedný za vedenie aktuálneho zoznamu významných informačných aktív,
- stanoviť vlastníka každého jednotlivého informačného aktíva a jeho zodpovednosť,
- stanoviť útvar zodpovedný za kontrolu dodržiavania bezpečnosti informačného aktíva vyplývajúcu z jeho bezpečnostnej klasifikácie.

IV. Personálna bezpečnosť
17. Cieľom personálnej bezpečnosti je znižovať riziko ľudského faktora (omyly, krádeže, podvody, zneužívanie), zabezpečiť dostatočnú informovanosť zamestnancov o hrozbách informačnej bezpečnosti a zaistiť ich pripravenosť na bezpečnostné incidenty a nesprávnu funkciu softvéru. Personálna bezpečnosť zahŕňa:
- bezpečnosť v definovaní práce a získavaní zamestnancov,

- školenie používateľov,
- reagovanie na bezpečnostné incidenty a nefunkčnosti.

18. Bezpečnosť v definovaní práce a získavaní zamestnancov
Na účely znižovania rizika ľudskej chyby, krádeže, podvodu a zneužitia prostriedkov a informácií by banka mala:
- vypracovať systém personálnej bezpečnosti banky pokrývajúci všetky obdobia a činnosti súvisiace so životným cyklom zamestnanca (nástup do zamestnania, zmena pracovnej náplne, zmena funkcie, ukončenie pracovného pomeru),
- previazať klasifikáciu informačných aktív a systém personálnej bezpečnosti,
- zahrnúť bezpečnostné požiadavky na konkrétne pracovné pozície do pracovných náplní týchto pracovných pozícií a do pracovných zmlúv,
- v odôvodnených prípadoch uzatvoriť dohody o zachovaní mlčanlivosti.

19. Školenie používateľov
Na účely oboznámenia používateľov informačného systému (zamestnanci a relevantné osoby z tretích strán) s ohrozeniami informačnej bezpečnosti by banka mala:
- oboznámiť používateľov informačného systému s aktuálnymi procedúrami pre bezpečnosť informačného systému, s ich zodpovednosťou a s právnymi dôsledkami vyplývajúcimi pre nich z nedodržania im stanovených povinností,
- školiť používateľov informačného systému na prácu s príslušnými zariadeniami a aplikačným programovým vybavením a overovať ich vedomosti.

20. Reagovanie na bezpečnostné incidenty a nefunkčnosti
Na účely minimalizácie škôd spôsobených bezpečnostnými incidentmi a nefunkčnosťami celého informačného systému alebo jeho častí, by banka mala mať vypracované procedúry pre zamestnancov a vedúcich zamestnancov v prípade výskytu:
- bezpečnostného incidentu,
- chyby softvéru,
- zlyhania softvéru,
- podozrenia, že niečo nie je v obvyklom poriadku,
- nevyhnutnosti začať disciplinárne konanie voči tým osobám, ktoré sú podozrivé zo spôsobenia a zodpovednosti za narušenie bezpečnosti.

V. Fyzická bezpečnosť a bezpečnosť prostredia
21. Cieľom je zabrániť neautorizovanému prístupu, poškodeniu a ohrozeniu priestorov banky, zabrániť poškodeniu informačných aktív a prerušeniu aktivít banky a zabrániť zneužitiu informácií a krádeži prostriedkov spracúvajúcich informácie. Fyzická bezpečnosť a bezpečnosť prostredia zahŕňa:
- vytvorenie zabezpečených oblastí,
- bezpečnosť zariadení.

22. Vytvorenie zabezpečených oblastí
Na účely zabránenia neautorizovanému prístupu, poškodeniu a ohrozeniu priestorov a informácií banky by banka mala:
- identifikovať a ohodnotiť riziká, ktoré sa viažu k informáciám, zariadeniam na spracovanie informácií a k fyzickým priestorom, v ktorých sú zariadenia na spracovanie informácií umiestnené a v ktorých sa informácie spracovávajú a uchovávajú,

- vypracovať procedúry pre umiestňovanie zariadení na spracovanie údajov a informácií,
- vypracovať procedúry na zaistenie ochrany budov a fyzických priestorov, kde sú umiestnené informácie a zariadenia na spracovanie informácií proti neautorizovanému prístupu, poškodeniu a ohrozeniu.

23. Bezpečnosť zariadení
Na účely ochrany údajov, informácií a udržania nepretržitej obchodnej činnosti by banka mala:

- vypracovať procedúry na komplexnú ochranu zariadení pre spracovanie, ukladanie a archivovanie údajov a informácií proti strate, poškodeniu, zneužitiu, rizikám prostredia a proti iným bezpečnostným hrozbám,
- vypracovať procedúry na komplexnú ochranu prenosových trás, po ktorých sa prenášajú údaje a informácie (ochrana proti neautorizovanému fyzickému prístupu, proti ich odpočúvaniu na diaľku a pod.),
- vypracovať procedúry pre záložnú dodávku elektrickej energie (UPS, záložný motorgenerátor),
- vypracovať procedúry pre prípad úplného výpadku všetkých variantov záložnej dodávky elektrickej energie,
- vypracovať formálne procedúry pre riadenie používania prenosných zariadení na spracovanie informácií ako aj samotné spracovanie informácií a údajov mimo priestorov banky.

VI. Riadenie komunikácie a prevádzky
24. Cieľom je zabezpečiť bezpečnú, spoľahlivú a plynulú prevádzku zariadení na spracovanie informácií, minimalizovať riziko zlyhania informačného systému alebo jeho časti, chrániť integritu softvéru, údajov a informácií, zabezpečiť dostupnosť spracovania informácií a komunikačných služieb, zaistiť bezpečnosť sietí a informácií v nich prenášaných, zabrániť prerušeniu obchodných aktivít banky a zaistiť bezpečnú výmenu informácií medzi organizáciami. Riadenie komunikácie a prevádzky zahŕňa:

- prevádzkové procedúry a zodpovednosť,
- plánovanie a akceptáciu informačného systému,
- ochranu voči škodlivému softvéru,
- zabezpečenie prevádzky,
- správu sietí,
- bezpečnú manipulácia s médiami,
- výmenu informácií a softvéru.

25. Prevádzkové procedúry a zodpovednosti
Na účely zaistenia bezpečnej a spoľahlivej prevádzky prostriedkov na spracovanie informácií by banka mala:

- vypracovať procedúry pre zabezpečenie prevádzky informačného systému, (najmä procedúry pre správu, štartovanie / vypínanie systému, zmeny v systéme, zálohovanie a archiváciu),
- vypracovať procedúry pre prevádzku aplikačného programového vybavenia,
- vypracovať procedúry pre monitorovanie, správu a riadenie bezpečnostných incidentov (najmä ich identifikovanie a oznamovanie, evidencia, časové rady, analýzy a závery, vyhodnocovanie efektívnosti bezpečnostného systému a rozdelenia zodpovedností),

- vypracovať procedúry na monitorovanie aktivít tretích strán,
- vypracovať procedúry pre monitorovanie využitia kapacity systému a úloh bežiacich v systéme,
- vypracovať procedúry pre vykonávanie zmien v produkčnom informačnom systéme,
- oddeliť produkčný systém, vývojový systém a zabezpečiť oddelený záložný spôsob spracovanie.

26. Plánovanie kapacity informačného systému a jeho akceptácia
Na účely zabezpečenia spoľahlivej a plynulej prevádzky svojho informačného systému bez jeho preťaženia a následného zlyhania by banka mala:
- vypracovať procedúry pre pravidelné monitorovanie a vyhodnocovanie jednotlivých parametrov informačného systému a kapacity informačného systému ako celku,
- zabezpečiť potrebné zvýšenie kapacity informačného systému s dostatočným predstihom,
- vypracovať procedúry pre komplexný postup a metodiku merania, monitorovania, vyhodnocovania, plánovania a akceptácie informačného systému vrátane rozdelenia zodpovedností a vyhodnocovania jeho efektívnosti.

27. Škodlivý softvér
Banka by mala mať vytvorené a implementované formálne procedúry na zabezpečenie integrity svojho informačného systému, softvéru, informácií a údajov proti vplyvom (pôsobeniu, účinkom) škodlivého softvéru. Procedúry by mali zahrnovať implementáciu a údržbu softvéru na zabezpečenie ochrany proti škodlivému softvéru.

28. Zabezpečenie prevádzky
Na účely zabezpečenia kontinuity činností banky, udržania integrity a dostupnosti spracovania informácií a komunikačných služieb po zlyhaní informačného systému by banka mala vypracovať procedúry:
- obnovy informačného systému,
- pre zálohovanie informačného systému,
- na oznamovanie chýb informačného systému alebo jeho častí a pre narábanie s takýmito oznámeniami,
- pre tvorbu a vyhodnocovanie záznamov o úkonoch zamestnancov zabezpečujúcich prevádzku a o chode a dôležitých udalostiach v informačnom systéme.

29. Správa sietí
Na účely zaistenia bezpečnosti údajov v sieťach a podpornej infraštruktúry sietí pred neautorizovaným prístupom by banka mala:
- vypracovať procedúry pre manažment vzdialených prostriedkov.
- vypracovať analýzu rizík súvisiacich so sieťami a procedúry pre ich riadenie,
- v prípade potreby oddeliť zodpovednosť za manažment sietí od zodpovednosti za prevádzku inej výpočtovej techniky a služieb,

30. Bezpečná manipulácia s prenosnými médiami
Na účely ochrany pred poškodením informačných aktív, prerušením obchodných činností a zaistenia bezpečného narábania s prenosnými médiami (diskety, magnetické disky, CD disky, pásky, kazety a tlačené dokumenty) by banka mala vypracovať procedúry pre manipuláciu s prenosnými médiami a ich likvidáciu.

31. Výmena informácií a softvéru
Na účely ochrany pred zneužitím, stratou alebo modifikáciou informácií, softvéru a údajov vymieňaných medzi bankou a inou externou osobou by banka mala:
- realizovať výmeny výhradne na zmluvnom základe,
- vypracovať procedúry pre výmenu informácií a fyzických nosičov údajov,
- vypracovať procedúry a opatrenia (v oblasti hardvérovej, softvérovej, personálnej a legislatívnej) na zmierňovanie a elimináciu rizík spojených s prevádzkovaním služieb elektronického bankovníctva po verejných sieťach (Internet),
- vypracovať procedúry pre zavedenie a používanie elektronických komunikačných kanálov (napr. elektronická pošta, elektronické kancelárske systémy a webová stránka),
- vypracovať procedúry, pre zaistenie informovanosti používateľov elektronických komunikačných kanálov o ich zodpovednosti za bezpečnosť údajov, informácií a softvéru v procese ich výmeny.

VII. Riadenie prístupu
32. Cieľom je riadiť prístup osôb k údajom a informáciám banky, prostriedkom na ich spracovanie, sieťovým službám, identifikovať neautorizované aktivity a zaistiť informačnú bezpečnosť v prípade mobilného spracovania a zamestnania na diaľku. Riadenie prístupu zahŕňa:
- vypracovanie zásad pre riadenie prístupu k informáciám,
- riadenie prístupu používateľov,
- zodpovednosť požívateľov,
- riadenie prístupu k sieťam,
- prístup k operačnému systému a jeho službám,
- prístup k aplikáciám,
- monitorovanie prístupu a používania informačného systému,
- mobilné spracovanie a zamestnanie na diaľku.

33. Zásady pre riadenie prístupu k informáciám
Na účely riadenia prístupu k informáciám by mala mať banka vypracované zásady riadenia prístupu k informáciám, ktoré obsahujú najmä:
- požiadavky na riadenie prístupu z pohľadu zabezpečenia bankových činností a bezpečnostných záujmov banky,
- pravidlá pre riadenie prístupu,
- pravidlá pre stanovenie prístupových práv a povinností pre jednotlivých používateľov a skupiny požívateľov informačného systému.

34. Riadenie prístupu používateľov k informáciám zahŕňa
- procedúry pre riadenie a udeľovanie prístupových práv a privilégií k aplikačným programovým vybaveniam a k službám zohľadňujúce všetky udalosti v pracovnom procese používateľa,
- procedúry pre správu používateľských mien a hesiel (prideľovanie, zmena, spôsob ich uloženia na pamäťovom médiu a pod.),
- proces registrácie a evidencie používateľov.

35. Zodpovednosť používateľov
Banka by mala zabrániť neautorizovanému prístupu používateľov k informáciám a k prostriedkom na spracovanie informácií. Za tým účelom by mala informovať

používateľov o ich zodpovednosti za udržiavanie efektívneho riadenia prístupu k údajom, informáciám, službám a k zariadeniam na spracovanie informácií.

36. Riadenie sieťového prístupu zahŕňa
- procedúru riadenia, zriaďovania, rozvoja, údržby a používania sietí,
- procedúru pre prístup a pripojovanie zariadení k prípojným portom k hardvérovým prostriedkom,
- procedúru pre riadenie rizík súvisiacich s pripojením externého používateľa.

37. Riadenie prístupu do operačného systému zahŕňa
- prihlasovaciu procedúru,
- procedúru pre stanovenie metódy identifikácie používateľov (napr. heslo, biometrické metódy, tokeny, kryptografické prostriedky, čipové karty, kombinácie),
- štandardný manažment zvolených metód na autorizáciu používateľa,
- riadenie prístupu k systémovým programom a ich používania,
- zabezpečenie neaktívnych zariadení a používateľov pred ich zneužitím (automatické odhlásenie používateľa, odpojenie zariadenia, zablokovanie úlohy alebo aplikácie, zablokovanie zariadenia a pod.).

38. Riadenie prístupu k aplikáciám zahŕňa
- zabezpečenie prístupu k aplikáciám na základe individuálnych požiadaviek v súlade s definovanou politikou riadenia prístupu a s politikou prístupu k informáciám,
- prideľovanie prístupových oprávnení a privilégií používateľom aplikačných programových systémov v súlade s bezpečnostnou politikou,
- procedúry a postupy na prideľovanie a schvaľovanie prístupových práv a privilégií.

39. Monitorovanie prístupu a používania informačného systému
Na účely zistenia neautorizovaných aktivít by mala banka:
- monitorovať odchýlky od zásad riadenia prístupu k informáciám v zmysle formálnych procedúr pre monitorovanie,
- automatizovane zaznamenávať informácie o dôležitých udalostiach v systéme (auditné záznamy) za účelom zaistenia dôkazov,
- archivovať auditné záznamy v súlade s archivačným poriadkom a bezpečnostnou politikou,
- pravidelne analyzovať a preverovať auditné záznamy za účelom odhaľovania prípadných bezpečnostných incidentov alebo neúspešných útokov,
- chrániť programy na vykonávanie auditných záznamov,
- oddeliť role tých, ktorí monitorujú a tých, ktorí sú monitorovaní.

40. Mobilné spracovanie a zamestnanie na diaľku
Na účely zaistenia informačnej bezpečnosti by banka mala:
- vypracovať politiku a procedúry pre riadenie mobilného spracovania a zamestnania na diaľku,
- umožniť mobilné spracovanie a zamestnanie na diaľku len na základe zmluvy a po povinnom školení a zácviku používateľov,
- identifikovať špecifické riziká spracovania a zamestnania na diaľku a prijať príslušné opatrenia na ich odstránenie alebo zníženie,
- zaistiť bezpečnosť v prípade pripojenia mobilných zariadení na sieť banky a to najmä prostredníctvom identifikácie a autorizácie používateľa.

VIII. Vývoj a údržba systému

41. Cieľom je zabudovať bezpečnosť informácií do samotného informačného systému, chrániť dôvernosť, integritu, dostupnosť a autenticitu údajov a informácií, zaistiť, aby projektovanie informačného systému prebiehalo bezpečným spôsobom a udržovať bezpečnosť aplikačného programového vybavenia. Vývoj a údržba systému zahŕňa:

- bezpečnostné požiadavky na informačný systém,
- bezpečnosť v aplikačných programových systémoch,
- kryptografické opatrenia,
- bezpečnosť systémových súborov,
- bezpečnosť vo vývoji a podporných procesoch.

42. Bezpečnostné požiadavky na informačný systém

Na účely zabudovania bezpečnosti do informačných systémov by mala banka definovať bezpečnostné požiadavky už vo fáze špecifikácie funkcionality informačného systému.

43. Bezpečnosť v aplikačných programových systémoch

Banka by mala zabrániť strate, modifikácii alebo zneužitiu údajov a informácií v aplikačných programových systémoch. Za tým účelom by banka mala začleniť do aplikačných programových systémov funkciu automatizovanej tvorby auditných záznamov.

44. Kryptografické opatrenia

Na účely ochrany informácií (dôvernosť, integritu, autenticitu a dostupnosť) by banka mala vytvoriť vlastnú politiku a formálne procedúry najmä pre:

- požívanie kryptografických techník,
- manipuláciu a správu s kľúčmi.

45. Bezpečnosť systémových súborov

Na účely zaistenia bezpečnosti projektovania informačného systému a podporných aktivít a minimalizácie rizika poškodenia prevádzkového systému by banka mala vypracovať procedúry pre:

- implementáciu prevádzkových softvérov,
- riadenie prístupu k systémovým súborom,
- zaistenie bezpečnosti už v priebehu projektovania informačného systému,
- manipuláciu a prístup k starým aj aktuálnym programovým knižniciam a k testovacím údajom,
- zmeny súborov v prevádzkovom (produkčnom) systéme.

46. Bezpečnosť vo vývoji a podporných procesoch

Na účely zaistenia bezpečnosti aplikačného programového vybavenia, údajov a informácií v ňom obsiahnutých, by mala banka vypracovať procedúry pre:

- riadenie bezpečnosti projektových a iných podporných prostredí a systémov,
- riadenie zmien v prevádzkovom (produkčnom) systéme,

IX. Manažment kontinuity činnosti banky

47. Cieľom je zabrániť prerušeniu obchodných činností banky. Na účely zaistenia nepretržitosti obchodných činností a ochrany svojich kľúčových obchodných procesov pred veľkými zlyhaniami a haváriami by banka mala:

- vypracovať plány udržania nepretržitej činnosti svojho informačného systému s rozdelením zodpovedností, ktoré budú v súlade s plánmi udržania nepretržitej obchodnej činnosti banky,
- plány udržania nepretržitej činnosti svojho informačného systému pravidelne testovať a aktualizovať,
- pre každý plán udržania nepretržitej činnosti svojho informačného systému definovať podmienky a postupy jeho aktivácie so stanovením zodpovedností.

X. Súlad s bezpečnostnými pravidlami

48. Cieľom je vyhnúť sa porušeniu záväzkov banky v oblasti informačného systému, zabezpečiť súlad informačného systému s bezpečnostnými pravidlami a štandardami banky. V procese budovania, prevádzky a správy informačného systému by banka mala dodržiavať záväzky, ktoré pre ňu vyplývajú z:

- všeobecne záväzných právnych predpisov,
- vnútorných regulačných predpisov,
- zmlúv,
- všeobecne uznávaných štandardov a bezpečnostných požiadaviek.

G. Rozsah informácií o overení bezpečnosti poskytnutých Národnej banke Slovenska

49. Banka zabezpečí, aby osoba vykonávajúca overenie bezpečnosti informačného systému vypracovala písomnú správu o vykonanom overení, ktorá poskytne dostatočné informácie pre predstavenstvo banky a Národnú banku Slovenska o stave bezpečnosti informačného systému banky.

50. Správa o overení bezpečnosti informačného systému banky pre informovanie Národnej banky Slovenska obsahuje minimálne tieto náležitosti:

- rozsah overenia bezpečnosti
- použité štandardy
- kto vykonal overenie,
- zoznam zistených nedostatkov s odôvodnením, prečo daná skutočnosť je chápaná ako nedostatok (odvolávka na záväzný dokument, medzinárodne uznávaný štandard, poukázanie na hrozby, možné dôsledky a škody, mechanizmus a pravdepodobnosť ich vzniku),
- odporúčania na odstránenie zistených nedostatkov,
- vyjadrenie k stavu bezpečnosti informačného systému banky s uvedením obmedzení a výhrad, ktoré negatívne ovplyvnili priebeh a výsledok overenia,
- stanovisko banky k správe.

v Bratislave, 1.10.2004

Milan Horváth v. r.
vrchný riaditeľ
úseku bankového dohľadu