НАРОДНА БАНКА НА РЕПУБЛИКА МАКЕДОНИЈА

Врз основа на член 64 став 1 точка 22 од Законот за Народна банка на Република Македонија („Службен весник на РМ“ бр. 3/2002, 51/2003, 85/2003, 40/2004, 61/2005 и 129/2006) и член 68 став 1 точка 4 од Законот за банките („Службен весник на РМ“ бр. 67/2007), Советот на Народната банка на Република Македонија донесе

О Д Л У К А
за сигурноста на информативниот систем на банката
("Сл. весник на РМ" бр. 31/2008)

I. ОПШТИ ОДРЕДБИ

1. Со оваа Одлука се пропишува методологијата за сигурноста на информативниот систем на банката со која се воспоставуваат стандарди во поглед на сигурноста на информативните системи, преку дефинирање критериуми за воспоставување процес за управување со сигурноста на информативниот систем, за обезбедување континуитет во работењето, како и сигурносни стандарди во однос на системите за електронско банкарство и друштвата за помошни услуги на банката за информативниот систем.

Банката е должна да воспостави систем за идентификување, мерење, следење и контрола на ризикот од несоодветност на информативните системи.

Ризик од несоодветност на информативните системи, според оваа Одлука, е ризикот од загуба за банката поради губење, неовластено користење или нерасположливост на информациите, информативните средства и/или услугите што ги нуди банката.

2. Сигурноста на информативниот систем на банката, според оваа Одлука, се дефинира како исполнување на следните критериуми:

а) **Доверливост**: информативниот систем е достапен само за корисниците кои имаат овластен пристап до него;
б) **Интегритет**: заштита на точноста и комплетноста на информативниот систем;
в) **Расположливост**: непречен пристап до информативниот систем за овластените корисници.

II. ПРОЦЕС ЗА УПРАВУВАЊЕ СО СИГУРНОСТА НА ИНФОРМАТИВНИОТ СИСТЕМ

3. Заради постигнување и постојано одржување на сигурноста на информативниот систем, банката е должна да воспостави процес за управување со сигурноста на информативниот систем што опфаќа:

- Проценка на ризикот;
- Политика за сигурност на информативниот систем;
- Спроведување на сигурносни контроли;
- Тестирање на сигурноста;

- Следење и надградба и
- Поделба на надлежностите на органите на банката од аспект на управувањето со сигурноста на информативниот систем.

Банката е должна да воспостави процес за управување со сигурноста на информативниот систем кој одговара на природата, обемот и сложеноста на финансиските активности за чие вршење добила претходна согласност од Народната банка.

4. Под проценка на ризикот, според оваа Одлука, се подразбира воспоставување постојан процес кој опфаќа:

- идентификација на средствата на информативниот систем на банката;
- класификација на средствата на информативниот систем на банката, односно, доделување вредност на средствата според пропишаните критериуми наведени во точка 2 од оваа Одлука;
- анализа на веројатноста за појавата на закани и слабости на информативниот системот и идентификација на можните последици;
- доделување приоритет на ризиците во зависност од големината на потенцијалната загубата што може да ја предизвикаат за банката.

За извршената проценка на ризикот банката треба, најмалку еднаш годишно, да изработи извештај.

5. Банката е должна да донесе и да примени Политика за сигурност на информативниот систем со која се дефинираат основите на процесот за управување со ризиците по сигурноста на информативниот систем.

6. Политиката од точка 5 од оваа Одлука треба да ги содржи најмалку следните елементи :

- начин на класификација на информациите и информативните средства, според критериумите за сигурност дефинирани во точка 2 од оваа Одлука;
- заштита на личните податоци, во согласност со важечките прописи во Република Македонија;
- методологија за спроведување анализа на ризиците поврзани со сигурноста на информативниот систем во која се дефинирани нивоата на прифатливост на ризиците;
- примена на стратегија на банката за управување со идентификуваните ризици, преку воспоставување акциски план и буџет за обезбедување на сигурноста на информативниот систем;
- годишен план за обука на вработените и комитентите на Банката, за правилно користење на услугите кои се достапни преку информативниот систем на банката;
- управување со сигурносните инциденти и воспоставување соодветен механизам за нивното идентификување, пријавување и ефикасно отстранување на можните закани за сигурноста на информативниот систем;
- дефинирање на нивоа на сигурносни инциденти и соодветни активности кои треба да бидат преземени во случај кога банката ќе утврди сигурносен инцидент;

- дефинирање на улогата на организациската единица за информациска технологија во банката, која треба да поседува соодветен кадровски капацитет и интерни процедури за работа, во согласност со усвоените акти од областа на сигурноста на информативниот систем;
- дефинирање соодветна ревизорска трага за критичните делови од информативниот систем на повеќе нивоа, како што се оперативен систем, бази на податоци, телекомуникациска опрема, со цел да се потврди идентитетот и редоследот на активностите кои се извршувале на информативниот систем;
- дефинирање на улогата на внатрешната и надворешната ревизија од аспект на обезбедувањето на сигурноста на информативниот систем;
- дефинирање на начинот на управување со сигурносни надградби, надградби на нови верзии, промени во параметрите и кодовите на апликациите, подготовка и ставање на апликациите во употреба;
- дефинирање на начинот на воспоставување План за континуитет во извршувањето на деловните активности на Банката;
- начин на воспоставување антивирусна заштита;
- дефинирање на начинот на телекомуникациско поврзување и обезбедување заштита на податоците кои се трансферираат;
- дефинирање сигурносни зони во Банката преку што ќе се ограничи физичкиот пристап до информациите и информативните средства на банката и
- дефинирање на начинот на воспоставување дополнителни безбедносни механизми, како што се противпожарна заштита, заштита од поплава, следење, сензори и аларми.

За ефикасна примена на политиката од точка 5 од оваа Одлука, односно на елементите на политиката дефинирани во став 1 од оваа точка, банката е должна да воспостави соодветни процедури.

7. Политиката од точка 5 од оваа Одлука треба да содржи опис на административните, техничките и физичките сигурносни контроли и начинот на нивната примена во банката.

Сигурносните контроли од став 1 на оваа точка треба да одговараат на големината и сложеноста на банката, како и на видот на финансиските активности за кои добила претходна согласност од Народната банка.

Под административни сигурносни контроли, според оваа Одлука, се подразбира воведување политики, стандарди, упатства и процедури од страна на органите на банката преку кои се воспоставува рамката за управување со сигурноста на информативниот систем.

Под технички сигурносни контроли, според оваа Одлука, се подразбира употребата на сигурносни мерки кои се вградени во компјутерската опрема, системскиот софтвер, комуникациската опрема и апликативните програмски решенија.

Под физички сигурносни контроли, според оваа Одлука, се подразбира преземањето соодветни мерки за ограничување и контрола на физичкиот пристап до информациите и информативните средства, за да се заштити банката од шпионажа, саботажа, пожар, поплава, вандализам, природна катастрофа и од друг

вид на оштетување или уништување на целиот или на делови од информативниот систем.

8. Банката е должна да воспостави процес на професионално, независно и објективно тестирање на ефикасноста и на соодветноста на спроведените сигурносни контроли содржани во политиката за сигурност на информативниот систем.

9. Банката е должна да воспостави процес преку кој постојано ќе ги прибира и ќе врши анализа на информациите за настанатите загуби како последица на сигурносни инциденти при работењето.

Банката е должна да воспостави процес преку кој постојано ќе ги прибира и ќе врши анализа на информациите поврзани со нови слабости и закани за сигурноста на информативниот систем и врз основа на извршените анализи да ги мери потенцијалните загуби од нив коишто можат да настанат доколку навремено не бидат спроведени соодветни сигурносни контроли.

10. Банката е должна да воспостави соодветна организациска поставеност за управување со сигурноста на информативниот систем, што подразбира јасно дефинирани надлежности и одговорности на органите на банката во процесот за управување со сигурноста на информативниот систем.

Во смисла на став 1 од оваа точка Надзорниот одбор на банката е одговорен за:

- одобрување на политиката за сигурност на информативниот систем и следење на нејзиното спроведување;
- оценка на соодветноста на донесената политика, најмалку еднаш годишно, од аспект на настанатите промени во организациската структура и промените во информативниот систем на банката и
- следење на ефикасноста на воспоставениот процес за управување со сигурноста на информативниот систем, преку анализа на резултатите од тестирањето на воспоставените сигурносни контролни во информативниот систем, од страна на независен и соодветно обучен тим, посебно во случаите кога настанале позначајни измени во информативниот систем или во процесот за управување со сигурноста на информативниот систем;

Според став 1 од оваа точка Одборот за управување со ризици е одговорен за :

- следење на политиката за сигурност на информативниот систем и идентификување на случаите кога е потребно нејзиното ревидирање;
- оценка на воспоставениот процес на управување со сигурноста на информативниот систем;
- анализа на извештајот за извршената проценка на ризиците од точка 4 став 2 на оваа Одлука и следење на активностите кои се преземаат во врска со управувањето со сигурноста на информативниот систем и
- одредување и редовно ревидирање на дефинираните нивоа на прифатливост на ризиците;

Според став 1 од оваа точка, Управниот одбор на банката е одговорен за:

- воспоставување и спроведување процедури за управување со сигурноста на информативниот систем, во согласност со политиката

за сигурност на информативниот систем, одобрена од страна на Надзорниот одбор;
- воспоставување и одржување ефикасен систем за мерење, следење, контрола и систем за известување на раководството (менаџмент информативен систем) за ризиците поврзани со сигурноста на информативниот систем;
- воспоставување процедури за оценка на ризиците за сигурноста на информативниот систем што произлегуваат од воведување нови производи, сервиси и услуги;
- обезбедување соодветна организациска поставеност и воспоставување соодветни функции и овластувања за ефикасно и сигурно управување со информацискатa технологија и сигурноста на информативниот систем во Банката;
- изработка на оперативен план за спроведување на деловната стратегијата на банката во однос на информацискатa технологија и
- назначување одговорно лице за сигурноста на информативниот систем.

11. Одговорното лице за сигурност на информативниот систем управува со сигурноста на информативниот систем на банката и ги координира политиката за сигурност на информативниот систем и процесите поврзани со различните технолошки платформи и работни задачи.

Лицето од став 1 на оваа точка треба да биде независно од лицата кои работат во организациските делови на банката што преземаат ризици поврзани со сигурноста на информативниот систем.

Надзорниот одбор на банката, најмалку двапати годишно, добива известување за работите поврзани со сигурноста на информативниот систем.

12. Системот за известување на раководството (менаџмент информативниот систем) од точка 10 став 3 алинеја 2 треба најмалку да ги содржи следните елементи:

- податоци за идентификуваните ризици и нивната контрола;
- информации за договорите со друштвата за помошни услуги на банката за информативниот систем;
- резултати од извршените тестирања на сигурноста на информативниот систем, сигурносни инциденти и соодветни реакции од страна на органите на банката и
- идентификувани потреби за промените во политиката за сигурност на информативниот систем на банката, од аспект на нејзиното унапредување.

III. ОБЕЗБЕДУВАЊЕ НА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО

13. Банката е должна да развива и да спроведува сопствен план за континуитет во работењето, кој ќе се темели врз повеќе сценарија и ќе овозможи оперативност и минимизирање на загубите во случај на тежок прекин на деловните процеси.

14. Тежок прекин на деловните процеси, според оваа Одлука, претставува состојба во која банката не е способна да ги исполни преземените деловни обврски

поради причини кои не може да ги контролира, или во случаи кога банката е физички или телекомуникациски оштетена, односно не се достапни информациите и информативните системи на кои се одвиваат критичните операции на банката.

15. Планот од точка 13 на оваа Одлука, треба да овозможи идентификација на критичните операции на банката, вклучувајќи ги и оние кои зависат од надворешни друштва за помошни услуги или од трети лица. За тие процеси банката треба:

- да определи методологија за оценка на штетите и да дефинира коефициенти на максимално дозволено време на нефункционирање на критичните операции;
- да ги идентификува алтернативните механизми за континуитет во деловните процеси во случај на прекин на примарните механизми;
- да ја идентификува можноста за обнова на податоците кои се потребни за продолжување на деловниот процес;
- да ја идентификува секундарната локација на која ќе бидат заштитени податоците, која треба да биде на соодветна оддалеченост од примарната локација, со цел да се минимизира ризикот двете локации да бидат истовремено недостапни.

За ефикасна примена на планот од точка 13 од оваа Одлука, банката е должна да воспостави процедури преку кои соодветно ќе се применат елементите дефинирани во став 1 од оваа точка.

16. Банката треба да врши периодично тестирање на планот од точка 13 од оваа Одлука со цел тој да биде усогласен со тековните деловни операции и нејзината деловна политика.

IV. ЕЛЕКТРОНСКО БАНКАРСТВО

17. Под електронско банкарство, според оваа Одлука, се подразбира понуда на банкарски услуги и производи преку интерактивни електронски комуникациски канали, како што се пристап до финансиски информации, информации за производи и услуги, извршување банкарски трансакции и сл.

18. Покрај критериумите наведени во точката 2 од оваа Одлука, за системите на електронско банкарство кои вклучуваат и извршување трансакции, банката дополнително треба да ги обезбеди и следните критериуми за сигурност:

а) **потврда на идентитетот на корисникот:** системи за еднозначно идентификување и потврдување на идентитетот на корисниците на информативните системи;

б) **неотповикливост на трансакциите:** системи за проверка на интегритетот на информациите и обезбедување доказ за трансфер на одредени информации или трансакции извршени од одреден корисник.

19. Потврдувањето на идентитетот на корисникот, според ова Одлука, банката може да го врши со користење на следните методи:

- преку слог на знаци што му е познат единствено на корисникот, како што е лозинка, пин и сл.;
- преку уред што единствено корисникот го поседува, како што е електронска картичка, клуч (токен) и сл. и/или

- преку некоја од единствените лични физички карактеристики на корисникот, како што е отпечаток од прст, ирис, препознавање говор и сл.

20. Во системите за електронско банкарство, банката треба да примени сигурни и ефикасни методи за потврдување на идентитетот на корисниците и нивните овластувања.

21. Во системите за електронско банкарство кои вклучуваат извршување трансакции, банката мора да има вградено потврда на идентитетот на корисникот со комбинација од најмалку два од дефинираните методи во точка 19.

22. За системите за електронско банкарство кои се достапни преку јавната компјутерска мрежа - Интернет, банката е должна да обезбеди валидна потврда на својот идентитет преку преносниот канал, за да можат корисниците да го потврдат идентитетот на системот на банката.

23. Во системите за електронско банкарство банката треба да вгради соодветни ревизорски траги со кои ќе се обезбеди неотповикливост на трансакциите.

V. ДРУШТВО ЗА ПОМОШНИ УСЛУГИ НА БАНКАТА ЗА ИНФОРМАТИВНИОТ СИСТЕМ

24. Под друштво за помошни услуги на банката за информативниот систем се подразбира друштво кое врз основа на писмен договор извршува услуги за банката при извршувањето на банкарските и финансиските активности во делот на информативниот систем.

25. Пред да се изврши избор на друштвото од точка 24 од оваа Одлука, банката треба да ги преземе следните активности:

- да изврши длабинска анализа на работењето на друштвото од правен, финансиски и од аспект на начинот на кој управува со процесот за сигурност на информативниот систем дефиниран во оваа Одлука и
- да изврши анализа на ризиците врз работењето на банката што можат да произлезат од користењето на услугиите, при извршувањето на банкарските и финансиските активности во делот на информативниот систем.

Под избор на друштвото од точка 24 од оваа Одлука се подразбира склучување нов договор или продолжување на веќе постоечки договор за помошни услуги на банката.

26. Банката не смее да склучи договор со друштвото од точка 24 од оваа Одлука доколку со договорот на каков било начин се оневозможува, ограничува или се отежнува пристапот на Народната банка при спроведувањето на супервизијата и надзорот, во согласност со Законот за банките.

27. Друштвото од точка 24 од оваа Одлука не смее да користи услуги на други помошни друштва, односно подизведувачи, за извршување на оние услуги за кои е склучен договорот од точка 24 од оваа Одлука, доколку тоа експлицитно не е наведено во него.

28. Работењето на друштвото од точка 24 од оваа Одлука треба да биде усогласено со политиката на банката од точка 5 на оваа Одлука.

29. Банката што донела одлука да користи услуги од друштвото од точка 24 од оваа Одлука, покрај елементите на политиката дефинирани во точка 6 став 1 од оваа Одлука, треба да ги предвиди во политиката и следните елементи:

- да го дефинира начинот на утврдување на единствените принципи и правила за избор на друштвото;
- да ги дефинира заштитните механизми што треба да бидат содржани во договорите со друштвото, како што се клаузулата за неоткривање на информациите, клаузулата за нивото на квалитет на услугите, клаузулата за координирано управување со сигурносните инциденти, клаузулата за спроведување независна ревизија и сл.;
- да утврди стандарди кои треба да ги исполнува друштвото, а кои ќе бидат усогласени со планот за континуитет во работењето на банката;
- да го дефинира начинот на следење на квалитетот на услугите и работата на друштвото, неговата финансиска состојба и неговиот профил на ризик, преку периодично тестирање на неговата усогласеност со политиката за сигурност на информативниот систем на банката.

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

30. Банката е должна да ја извести Народната банка во случаите кога ќе идентификува дека се случило највисоко ниво на сигурносен инцидент во информативен систем, согласно со дефинираните нивоа на сигурносни инциденти од точка 6 став 1 алинеја 7 од оваа Одлука.

Банката е должна да го достави известувањето од став 1 на оваа точка до Народната банка, во рок што не е подолг од три дена од денот кога е утврдено дека настанал сигурносниот инцидент.

31. Банката е должна да ја извести Народната банка за промените во клучните делови на процесот за управување со сигурноста на информативниот систем, а посебно при промени на елементите од политиката дефинирани во точка 6 став 1 од оваа Одлука.

32. Оваа Одлука влегува во сила во рок од осум дена од денот на објавувањето во „Службен весник на Република Македонија“, а ќе се применува од 01.01.2009 година.

33. Со отпочнувањето со примена на оваа Одлука, престанува да важи Одлуката за дефинирање на стандардите за изготвување и спроведување на сигурноста на информативниот систем на банките („Службен весник на Република Македонија“, бр. 77/2003).

О.бр. 02-15/II-7/2008
28.02.2008 година
Скопје

м-р Петар Гошев
гувернер
Претседател
на Советот на Народната банка
на Република Македонија