AZƏRBAYCAN RESPUBLİKASININ HÜQUQİ AKTLARIN DÖVLƏT REYESTRİ

Aktın növü	*MƏRKƏZİ BANKININ QƏRARI*
Qəbul edildiyi tarix	*10.12.2014*
Qeydiyyat nömrəsi	*26/4*
Adı	*"Banklarda informasiya sistemlərinin təhlükəsizliyinə dair Qaydalar"ın təsdiq edilməsi barədə*
Rəsmi dərc edildiyi mənbə	
Qüvvəyə minmə tarixi	*31.12.2014*
Azərbaycan Respublikasının Vahid hüquqi təsnifatı üzrə indeks kodu	*090.060.010*
Hüquqi Aktların Dövlət Reyestrinin qeydiyyat nömrəsi	*23201412100264*
Hüquqi aktın Hüquqi Aktların Dövlət Reyestrinə daxil edildiyi tarix	*30.12.2014*

"Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyinin yaradılması haqqında" Azərbaycan Respublikası Prezidentinin 2014-cü il 7 mart tarixli 326 nömrəli Sərəncamının 3-cü hissəsinin icrası və banklarda informasiya sistemlərinin təhlükəsizliyi ilə bağlı minimum tələblərin təkmilləşdirilməsi məqsədi ilə Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyəti "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 22.0.17-civə 44.5-ci, "Banklar haqqında" Azərbaycan Respublikası Qanununun 38.3-cü maddələrinə əsasən

Q Ə R A R A A L I R:

1.“ Banklarda informasiya sistemlərinin təhlükəsizliyinə dair Qaydalar” təsdiq edilsin (əlavə olunur);

2. Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyətinin 2006-cı il 13 marttarixli qərarı ilə (07 nömrəli protokol) təsdiq edilmiş (31.03.2006-cı il tarixli 3217 nömrəli şəhadətnamə) “Banklarda informasiya texnologiyalarının tətbiqi Qaydaları” və 2006-cı il 9 oktyabr tarixli qərarı ilə (32 nömrəli protokol) təsdiq edilmiş (31.10.2006-cı il tarixli 3244 nömrəli şəhadətnamə) “Banklarda informasiya texnologiyalarının tətbiqi Qaydaları”na əlavə ləğv edilsin;

3. Hüquq departamentinə (R.Məlikova) tapşırılsın ki, bu Qərarın 3 gün müddətində Azərbaycan Respublikasının Hüquqi Aktların Dövlət Reyestrinə daxil edilməsi üçün Azərbaycan Respublikasının Ədliyyə Nazirliyinə təqdim olunmasını təmin etsin.

Sədr **Elman Rüstəmov**

"Təsdiq edilmişdir"

Azərbaycan Respublikasının

Mərkəzi Bankı

Qərar № 26/4

"10" dekabr 2014-cü il

Banklarda informasiya sistemlərinin təhlükəsizliyinə dair Qaydalar

1. Ümumi müddəalar

Bu Qaydalar "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 44.5-ci və "Banklar haqqında" Azərbaycan Respublikası Qanununun 38.3-cü maddələrinə əsasən hazırlanmış və bank informasiyasının mühafizəsi məqsədilə banklarda informasiya sistemlərinin təhlükəsizliyinə dair minimal tələbləri müəyyən edir.

2. Anlayışlar

2.1. Bu Qaydalarda istifadə olunan anlayışlar aşağıdakı mənaları daşıyır:

2.1.1. avtorizə etmə - bank əməliyyatlarının yoxlanılmasının informasiya sistemlərində təsdiqi;

2.1.2. işçi stansiya –bankın informasiya sistemlərinə giriş imkanı verilmiş kompüter;

2.1.3 on-line rejimli interfeys - real vaxt rejimində iki və ya daha artıq informasiya sistemləri arasında birbaşa yaradılmış informasiya və kommunikasiya əlaqəsi;

2.1.4. sanksiya edilməmiş müdaxilə - informasiya sistemlərinə səlahiyyətsiz istifadəçinin daxil olma cəhdi;

2.15. istifadəçi–bankın informasiya sistemlərinə giriş səlahiyyəti verilmiş şəxs;

2.1.6. sistem inzibatçısı –bankın bir və ya bir neçə informasiya sistemlərində dəyişiklikləri tətbiq edən, sistemlərin ehtiyat surətlərinin yaradılması və sistemin fəaliyyətinin monitorinqini, habelə səlahiyyət bölgüsünə əsasən informasiya sistemi üzrə digər funksiyaları həyata keçirən bank əməkdaşı;

2.1.7. təhlükəsizlik inzibatçısı –bankın bir və ya bir neçə informasiya sistemlərinin mühafizəsinə və məlumatlara sanksiya edilməmiş müdaxilələrə məsul olan və bankın informasiya texnologiyalarının tətbiqinə cavabdeh olan struktur bölməyə tabeçiliyi olmayan bank əməkdaşı;

2.1.8. topoloji diaqram –informasiya texnologiyaları avadanlıqlarının şəbəkədə qoşulma sxeminin təsviri.

2.2. Bu Qaydalarda istifadə olunan "informasiya sistemi" və "informasiya texnologiyaları" anlayışları "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda, "verilənlər" anlayışı isə "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanununda verilən mənaları ifadə edir.

3. İnformasiya sistemlərinə və informasiya texnologiyalarına dair əsas tələblər

3.1. İnformasiya sistemlərinin fəaliyyətinin effektivliyini və təhlükəsizliyini təmin etmək məqsədi ilə bank aşağıdakı tələblərə riayət etməlidir:

3.1.1. bankın strateji planına uyğun olaraq informasiya sistemlərinin etibarlı və davamlı fəaliyyəti təmin olunmalıdır;

3.1.2. bankın informasiya sistemləri və ya informasiya texnologiyalarında baş verən problemlərlə əlaqədar yaranan risklər (İT riskləri) effektiv idarə olunmalıdır;

3.1.3. fövqəladə hallarda informasiya sistemləri üzrə fəaliyyətin davamlılığı prosedurları mövcud olmalıdır;

3.1.4. informasiya sistemlərinin və informasiya texnologiyalarının istifadəsi və idarəolunması üzrə bank işçiləri arasında səlahiyyət bölgüsü aparılmalıdır;

3.1.5. bankda sistem və təhlükəsizlik inzibatçısı (inzibatçıları) təyin olunmalıdır;

3.1.6. informasiya texnologiyaları avadanlıqlarının yerləşdiyi sahəni, sistemin elementlərinin birləşdirilməsi üçün istifadə edilən xətlərin yerini, dəstəkləyici xidmətləri (rabitə, elektrik enerjisi), ehtiyat vasitələri və sistemin təhlükəsizliyinin təmin edilməsi üçün lazım olan digər elementləri nəzərdə tutan topoloji diaqram tərtib olunmalıdır.

4. İnformasiya sistemlərində məlumatlara daxilolma

4.1. İstifadəçilərin informasiya sistemlərinə daxil olması bankda aparılan səlahiyyət bölgüsünə əsaslanmalıdır.

4.2. Bankda istifadəçilərin və sistem inzibatçılarının sistemdə uçotunun yaradılması, dəyişdirilməsi və ləğv edilməsi, habelə onların informasiya sistemlərinə daxilolma qaydalarını müəyyən edən prosedurlar mövcud olmalıdır.

4.3. İnformasiya sistemlərində istifadəçilərin yaradılması sistem inzibatçısı, səlahiyyətlərin təyin edilməsi, dəyişdirilməsi və istifadəçilərin fəaliyyətinin dayandırılması isə təhlükəsizlik inzibatçısı tərəfindən həyata keçirilməlidir.

4.4. Səhvləri, saxtakarlıq hallarını, sanksiya edilməmiş müdaxilələri, məlumatların səlahiyyətsiz şəxslər tərəfindən dəyişdirilməsi və silinməsi risklərini azaltmaq məqsədilə bankda sistemlərə daxilolma hüquqları ilə sistemlərə giriş qeydlərinin mütəmadi müqayisəsi aparılmalıdır.

4.5. İnformasiya sistemlərinə sanksiya edilməmiş müdaxilələrin qarşısını almaq məqsədi ilə bankda informasiya texnologiyaları avadanlıqları üzrə fiziki təhlükəsizlik və nəzarət qaydaları müəyyən olunmalıdır.

5. Fövqəladə hallar üzrə prosedurlar

5.1. Hər bir bankda informasiya sistemlərinin və informasiya texnologiyalarının zədələndiyi, dağıldığı və ya təhlükəyə məruz qaldığı hallarda fəaliyyətin fasiləsizliyi təmin edilməlidir.

5.2. Fəaliyyətin fasiləsizliyini təmin etmək üçün bank aşağıdakıları təmin etməlidir:

5.2.1. informasiya sistemlərinin ehtiyat surətlərinin saxlanılması və fəaliyyətin bərpası üçün bankın olduğu yerdən kənarda Ehtiyat Mərkəzinin yaradılmasını;

5.2.2. fövqəladə hallarda bankın fəaliyyətinin davamlılıq planının hazırlanması və təsdiq olunmasını. Fəaliyyətin davamlılığı planında fövqəladə hallar zamanı kommunikasiya tədbirləri müəyyənləşdirilməli, bankda fəaliyyətin bərpası, Ehtiyat Mərkəzə keçid və sonrakı bərpa prosedurları müəyyən edilməlidir;

5.2.3. fövqəladə hallar zamanı informasiya sistemlərinin bankın davamlı fəaliyyətini dəstəkləmək imkanlarının ən azı 6 aydan bir qiymətləndirilməsini və nəticələrinin rəsmiləşdirilməsini;

5.2.4. fövqəladə hallarda fəaliyyətin davamlılığını təmin etmək məqsədilə informasiya sistemlərində və informasiya texnologiyası avadanlıqlarında qəza zamanı riayət olunmalı prosedurlarla bağlı bankda əlaqədar işçilər üçün ildə bir dəfədən az olmayaraq təlim həyata keçirilməsini və nəticələrinin rəsmiləşdirilməsini.

6. Risklərin idarə edilməsi

6.1. Bankda İT riskləri Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyətinin 9 dekabr 2013-cü il tarixli 24/3 nömrəli qərarı ilə təsdiq edilmiş "Banklarda risklərin idarə olunması haqqında Qaydalar"a uyğun olaraq idarə olunmalıdır.

6.2. İT risklərinin minimallaşdırılması məqsədilə avtomatlaşdırılmış bank informasiya sistemi (bundan sonra - ABİS) üzrə aşağıdakı tədbirlər həyata keçirilməlidir:

6.2.1. verilənlər bazasının gündəlik, həftəlik, aylıq və illik ehtiyat surətlərinin saxlanması;

6.2.2. verilənlər bazasında aparılmış dəyişikliklər üzrə qeydlərin (loqların) saxlanması və ehtiyat surətlərinin yaradılması;

6.2.3. verilənlər bazasının gündəlik surətlərinin bir həftədən, həftəlik surətlərinin bir aydan, aylıq surətlərinin bir ildən və illik surətlərinin beş ildən az olmamaq şərti ilə saxlanması;

6.2.4. illik surətlərin bankın arxivinə təhvil verilməsindən əvvəl serverdə verilənlərin bərpasının yoxlanması;

6.2.5. ABİS-də sənədlərin avtorizə etmə mexanizmlərinin yaradılması və tətbiqinin təmin edilməsi;

6.2.6. ABİS ilə bankın ödəniş və digər informasiya sistemləri arasında ötürülən məlumatların dəyişdirilməsi imkanını istisna edən əlaqənin (interfeysin) yaradılması;

6.2.7. bankla onun filialları, şöbələri və valyuta mübadilə şöbələri arasında on-line rejimli interfeysin yaradılması;

6.2.8. informasiya sistemlərinin ehtiyat surətlərinin bankın Ehtiyat Mərkəzində saxlanılması.

7. İnformasiya təhlükəsizliyi

7.1. Bankda məlumatları emal edən serverlər aşağıdakı tələblərə cavab verməlidir:

7.1.1. təhlükəsizlik inzibatçısı və informasiya texnologiyalarının tətbiqinə məsul struktur bölmə ilə razılaşdırmaqla lisenziyalaşdırılmış, sərbəst və ya açıq lisenziya sazişi şərtləri ilə yayılan proqram təminatlarından istifadə edilməlidir;

7.1.2. serverlərdə tətbiq edilən proqram təminatları təhlükəsizlik inzibatçısı ilə razılaşdırılmalıdır;

7.1.3. informasiya sistemləri antivirus proqram təminatı vasitəsilə qorunmalı və bu proqram təminatı bazası gündəlik olaraq yenilənməlidir.

7.2. İnformasiya sistemlərində istifadəçilərin və sistem inzibatçılarının aşağıdakı tələblərə cavab verən eyniləşdirilməsi funksiyası təmin olunmalıdır:

7.2.1. hər bir istifadəçinin və sistem inzibatçısının şifrəsi mövcud olmalı;

7.2.2. şifrələrin istifadə müddəti maksimum 30 gün olmalı;

7.2.3. istifadəçilər üçün şifrə 8 simvoldan az olmamalı;

7.2.4. sistem inzibatçıları üçün şifrə 10 simvoldan az olmamalı;

7.2.5. sistemə ilk qoşulma zamanı şifrə istifadəçi tərəfindən mütləq dəyişdirilməli;

7.2.6. istifadəçi şifrəsinin 3 dəfə səhv yığılması cəhdlərindən sonra sistemə giriş məhdudlaşdırılmalı və yalnız təhlükəsizlik inzibatçısı tərəfindən sistemə giriş qadağalarının götürülməsi mümkün olmalı;

7.2.7. sistemdə istifadə olunmuş son 12 şifrənin təkrar istifadəsinin avtomatik olaraq qarşısı alınmalı;

7.2.8. sistem inzibatçıları digər istifadəçilərin şifrələrini əldə etmək imkanına malik olmamalı;

7.2.9. şifrənin həm hərfi (ən azı biri baş hərf olmaqla), həm də rəqəm simvollardan ibarət olması avtomatik olaraq yoxlanmalı;

7.2.10. şifrələr ekranda açıq əks olunmamalı;

7.2.11. şifrə ilə mühafizəyə malik ekran qoruyucusu mövcud olmalı;

7.2.12. bütün sistem inzibatçılarının şifrələri möhürlənmiş zərflərdə təhlükəsiz yerdə saxlanılmalıdır.

7.3. Kriptoqrafik mühafizə sistemlərinin tətbiqi zamanı aşağıdakı tələblərə riayət edilməlidir:

7.3.1. şifrələr kodlaşdırılmış vəziyyətdə saxlanılmalı;

7.3.2. şifrələr kodlaşdırılmış vəziyyətdə ötürülməli;

7.3.3. informasiya kənar rabitə kanallarına ötürüldükdə şifrələnməli;

7.3.4. informasiya kənar daşıyıcılara şifrələnmiş vəziyyətdə yazılmalı.

7.4. Hər bir bankda server otaqlarının mühafizəsi üçün aşağıdakılar təmin olunmalıdır:

7.4.1. otaqlar odadavamlı mebellər ilə təchiz edilməli;

7.4.2. server otaqlarında avadanlığın quraşdırılması, əvəz edilməsi, təmiri, otaqlardan avadanlığın çıxarılması, habelə kənar təşkilatların mütəxəssislərinin işi sistem inzibatçısı və (və ya) təhlükəsizlik inzibatçısının nəzarəti altında həyata keçirilməli;

7.4.3. otaqlar dayanıqlı materiallardan (daş, kərpic, beton) inşa edilməli;

7.4.4. eyni vaxtda bütün ərazisini çəkməyə imkan verən müşahidə kameraları ilə təchiz edilməlidir. Müşahidə kameralarının görüntüləri ən azı 6 (altı) ay müddətində təhlükəsizlik inzibatçısı tərəfindən saxlanılmalı;

7.4.5. otaqların qapıları daim bağlı vəziyyətdə saxlanılmalı vəotaqlara yalnız səlahiyyətli şəxslərin girişi təmin edilməli;

7.4.6. saz vəziyyətdə olan yanğından müdafiə sistemləri, o cümlədən ilkin yanğınsöndürmə vasitələri ilə təchiz edilməli;

7.4.7. olduqda, bütün xarici pəncərələri dəmir barmaqlıqlar və ya zirehli şüşə ilə təchiz olunmalıdır. Bütün xarici pəncərələr içərinin görünməməsi üçün daxildən örtük ilə üzlənməli;

7.4.8. fasiləsiz elektrik enerjisi ilə təmin edən qida mənbəyi və generator ilə təchiz edilməli;

7.4.9. otağın döşəməsi və tavanı antistatik örtüklə təmin edilməli;

7.4.10. havalandırma (kondisioner) avadanlıqları və istiliyin tənzimlənməsi üçün termometrlə təchiz olunmalı;

7.4.11. otaq rütubətlilik göstəricilərini ölçən cihaz və tənzimləyən avadanlıqlar ilə təchiz edilməli.