AZƏRBAYCAN RESPUBLİKASI MƏRKƏZİ BANKININ İDARƏ HEYƏTİNİN

Q Ə R A R I

20/1

Bakı şəhəri **14 iyul 2021-ci il**

"Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası"nın təsdiq edilməsi barədə

Banklarda informasiya təhlükəsizliyi ilə bağlı tələblərin beynəlxalq standartların tələblərinə uyğun olaraq gücləndirilməsi məqsədilə "Banklar haqqında" Azərbaycan Respublikası Qanununun 38.3-cü maddəsinə və "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 22.0.17-ci maddəsinə əsasən Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyəti

Q Ə R A R A A L I R:

1. "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası" təsdiq edilsin (əlavə olunur).

2. Bu Qərarın 1-ci hissəsi ilə təsdiq edilmiş "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası" 2022-ci il 1 aprel tarixindən qüvvəyə minir və həmin tarixdən Azərbaycan Respublikası Mərkəzi Bankı İdarə Heyətinin "Banklarda informasiya sistemlərinin təhlükəsizliyinə dair Qaydalar"ın təsdiq edilməsi barədə" 2014-cü il 10 dekabr tarixli 26/4 nömrəli Qərarının 1-ci hissəsi ləğv edilir.

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 edilməsini təmin etsin.

Mərkəzi Bankın sədri **Elman Rüstəmov**

"Təsdiq edilmişdir"
Azərbaycan Respublikasının
Mərkəzi Bankı
Qərar 20/1
14 iyul 2021-ci il

Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası

1. Ümumi müddəalar

1.1. Bu Qayda "Banklar haqqında" Azərbaycan Respublikası Qanununun 38.3-cü maddəsinə uyğun olaraq hazırlanmış və Beynəlxalq Standartlaşdırma Təşkilatının ISO/IEC 2700X standartlarının tələbləri nəzərə alınmaqla Azərbaycan Respublikasında fəaliyyət göstərən banklarda və xarici bankların yerli filiallarında (bundan sonra – banklar) informasiya təhlükəsizliyinə dair minimum tələbləri müəyyən edir.

1.2. Bu Qayda ilə müəyyən edilən tələblər bankların bütün biznes proseslərinə və informasiya sistemlərinə yönəlir, habelə həmin biznes proseslərin və informasiya sistemlərinin idarə edilməsinə məsul olan bütün struktur bölmələrin fəaliyyətini əhatə edir.

1.3. Banklarda fərdi məlumatların mühafizəsinə dair tələblər bu Qayda ilə yanaşı "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu ilə tənzimlənir.

2. Anlayışlar

2.1. Bu Qaydanın məqsədləri üçün istifadə edilmiş anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. aktiv – banklar üçün dəyəri olan əsas (biznes proseslər və informasiya) və dəstəkləyici (şəbəkə və texniki infrastruktur, proqram təminatları, personal, bina, təşkilati struktur) aktivlər;

2.1.2. aktiv sahibi – aktivin bütün fəaliyyət dövrü ərzində effektiv idarə edilməsinə və mühafizəsinə məsul olan bank işçisi;

2.1.3. audit – audit sübutlarının əldə edilməsi və onların audit meyarlarının yerinə yetirmə səviyyəsini müəyyənləşdirmək məqsədilə obyektiv olaraq qiymətləndirilməsi üçün həyata keçirilən sistematik, müstəqil və sənədləşdirilmiş proses;

2.1.4. autentifikasiya – xidmət istifadəçisinin kimliyini və fərdiləşdirilmiş təhlükəsizlik məlumatlarının istifadəsinin etibarlığını yoxlamağa imkan verən prosedur;

2.1.5. "brute-force" hücum – ədədi və ya simvol-rəqəm parolların çoxsaylı kombinasiyalarını sınamaqla giriş əldə etmək metodu;

2.1.6. əməliyyat inzibatçısı – informasiya sisteminin idarə edilməsi üzrə biznes prosesləri və onların sistemdə təzahürünü aydın bilən bank işçisi;

2.1.7. əməliyyat mühiti – informasiya sisteminin istifadəçiyə açıq real istismar mühiti;

2.1.8. fərdi məlumat – şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat;

2.1.9. informasiya – yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar;

2.1.10. informasiya aktivi – fiziki (kağız, CD və ya digər daşıyıcılarda olan) və ya elektron formada (məlumat bazaları, fayllar, fərdi kompüterlərdə saxlanılan) mövcud olan banklar üçün qiymətli olan, habelə bankların ixtiyarında olan informasiya;

2.1.11. informasiyanın əlçatanlığı – tələb olunduğu halda informasiyanın əldə edilə və istifadə oluna bilməsi xüsusiyyəti;

2.1.12. informasiyanın konfidensiallığı – informasiyanın səlahiyyətli olmayan girişlər üçün əlçatan və açıq olmama xüsusiyyəti;

2.1.13. informasiya prosesi – informasiyanın yaradılması, yığılması, işlənməsi, saxlanması, axtarışı, yayılması;

2.1.14. informasiya sistemi – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklə, nizamlanmış məcmusu;

2.1.15. informasiyanın tamlığı – informasiyanın dəqiqlik və bütünlük xüsusiyyəti;

2.1.16. informasiya təhlükəsizliyi – informasiyanın konfidensiallığının, tamlığının və əlçatanlığının mühafizə olunması;

2.1.17. informasiya təhlükəsizliyinin idarə edilməsi sistemi (bundan sonra - İTİS) – fəaliyyət məqsədlərinə nail olmaq üçün bankın informasiya təhlükəsizliyinin yaradılması, tətbiq edilməsi, dəstəklənməsi və davamlı inkişaf etdirilməsinə istiqamətlənən fəaliyyət və prosedurlar toplusu;

2.1.18. informasiya texnologiyaları – informasiya prosesləri zamanı, o cümlədən hesablama və rabitə texnikasının tətbiqi ilə istifadə edilən üsul və vasitələr sistemi;

2.1.19. informasiya təhlükəsizliyi hadisəsi – informasiya təhlükəsizliyi siyasətinin mümkün pozuntusu və ya idarəetmənin uğursuzluğunu göstərən bir sistem, xidmət və ya şəbəkə vəziyyətinin meydana gəlməsi və ya təhlükəsizliklə əlaqəli ola biləcək əvvəllər bilinməyən bir vəziyyət;

2.1.20. informasiya təhlükəsizliyi insidenti – biznes proseslərin pozulması və informasiya təhlükəsizliyi təhdidi yaratma ehtimalı əhəmiyyətli olan bir və ya bir neçə arzuolunmaz və ya gözlənilməz informasiya təhlükəsizliyi hadisəsi;

2.1.21. inkişaf mühiti – informasiya sisteminin proqram təminatlarının işlənib hazırlanma mühiti;

2.1.22. istifadəçi – informasiya sistemində işləmək icazəsi olan bankın işç iləri, kontragentləri və müştəriləri;

2.1.23. kriptoqrafik vasitələr – informasiyanın kriptoqrafik çevrilməsindən istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi üçün tətbiq olunan üsullar (avadanlıqlar, tətbiqi proqram təminatları və sair);

2.1.24. kritik informasiya sistemi – banklarda risklərin idarə olunması qaydalarına müvafiq olaraq risklərin qiymətləndirilməsinə əsasən yüksək təsir səviyyəsinə malik olan və bank fəaliyyətinin həyata keçirilməsi zamanı istifadə olunan informasiya sistemləri, o cümlədən əməliyyat, uçot və avtomatlaşdırılmış idarəetmə sistemləri və informasiya-telekommunikasiya şəbəkələri;

2.1.25. mobil cihaz – fərdi istifadə üçün nəzərdə tutulmuş portativ elektron cihaz (noutbuk, planşet, smartfonlar və sair);

2.1.26. sınaq mühiti – informasiya sisteminin real istismara verməzdən öncə test edilmə mühiti;

2.1.27. sistem inzibatçısı – informasiya sistemində dəyişiklikləri tətbiq edən, onun ehtiyat nüsxələrinin yaradılması, fəaliyyətinin monitorinqini və fasiləsiz fəaliyyətini təmin edən, habelə səlahiyyət bölgüsünə əsasən sistem üzrə digər funksiyaları həyata keçirən bank əməkdaşı.

3. İnformasiya təhlükəsizliyinin idarə edilməsi sistemi

3.1. İTİS banklarda risklərin idarə olunması qaydalarını tənzimləyən normativ xarakterli aktlara, bu Qaydaya və bankın Müşahidə Şurası tərəfindən təsdiq edilmiş risklərin idarə edilməsi strategiyası və siyasətinə uyğun olaraq formalaşdırılır.

3.2. İTİS informasiya aktivlərini qorumaq məqsədilə bank tərəfindən birgə idarə olunan siyasətlər, prosedurlar, müvafiq resurslar və fəaliyyətlərdən ibarətdir.

3.3. Müşahidə Şurası risklərin idarə edilməsi strategiyası və siyasəti çərçivəsində bankın məqsədlərinə və bu məqsədlərə nail olmaq üçün görülən tədbirlərə uyğun olaraq hazırlanmış informasiya təhlükəsizliyi siyasətini təsdiq edir.

3.4. İnformasiya təhlükəsizliyi siyasəti müvafiq informasiya risklərini və nəzarət sahələrini kompleks və əsaslı şəkildə əhatə edir, aydın və anlaşılan formada hazırlanır və təsdiq edilmiş redaksiyada aidiyyəti işçilər məlumatlandırılır.

3.5. İnformasiya təhlükəsizliyi siyasəti ən azı bu Qaydanın 4-15-ci hissələri ilə müəyyən edilən nəzarət məqsədlərini və mexanizmlərini əhatə edir və bank üçün İTİS-in davamlı surətdə təkmilləşdirilməsi öhdəliyini müəyyən edir.

3.6. İnformasiya təhlükəsizliyi siyasətinə ən azı ildə bir dəfə ayrıca, habelə bankda risklərin idarə edilməsi strategiyası və siyasətinə baxılarkən yenidən baxılır və tələb olunduqda müvafiq dəyişikliklər edilir. İTİS-in davamlılığı, adekvatlığı və effektivliyinin təmin edilməsi üçün dəyişikliklər edildikdə informasiya təhlükəsizliyi siyasətinə növbədənkənar qaydada yenidən baxılır.

4. İnformasiya təhlükəsizliyinin təşkili

4.1. Bankda İTİS-lə bağlı ümumi rəhbərlik Müşahidə Şurası tərəfindən həyata keçirilir və informasiya təhlükəsizliyinin təşkili məqsədilə aşağıdakılar təmin olunur:

4.1.1. informasiya təhlükəsizliyi ilə bağlı vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlərin müəyyən edilməsi və əlaqələndirilməsi;

4.1.2. bankın aktivlərinin sanksiya edilməmiş və ya qeyri-ixtiyari dəyişdirilməsi və ya sui-istifadəsi hallarının məhdudlaşdırılması üçün bir-biri ilə toqquşan vəzifələrin və öhdəlik sahələrinin bir-birindən ayrılması;

4.1.3. informasiya təhlükəsizliyinin təmin olunması məqsədi ilə səlahiyyətli dövlət orqanları ilə qarşılıqlı əlaqələrin yaradılması və qarşılıqlı fəaliyyət üzrə informasiyanın ötürülməsi, qəbulu və təqdim edilməsi, habelə müəyyən edilmiş informasiya təhlükəsizliyi insidentləri barədə məlumatların mübadiləsi ilə bağlı müvafiq prosedurların formalaşdırılması;

4.1.4. bankların qeyri-kommersiya birliklərində üzvlüyü ilə əlaqədar, habelə kart təşkilatları ilə müvafiq əlaqələrin yaradılması zamanı informasiya təhlükəsizliyinin təmin edilməsi məqsədilə konfidensial məlumatların mühafizəsi ilə bağlı tələbləri özündə əks etdirən məlumat mübadiləsi müqaviləsinin bağlanması;

4.1.5. layihələrin növündən asılı olmayaraq layihə idarəetməsi üzrə informasiya təhlükəsizliyinin təmin edilməsi və monitorinqi ilə bağlı tələblərin bütün layihələr üzrə nəzərə alınması.

4.2. Məsafədən iş və mobil cihazlardan istifadə zamanı təhlükəsizliyin təmin edilməsi üçün aşağıdakı tədbirlər görülür:

4.2.1. mobil cihazların istifadəsi zamanı yarana biləcək risklərin və informasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə siyasət hazırlanmalı və tətbiqi təmin edilməlidir;

4.2.2. mobil cihaz siyasəti müdafiə olunmayan mühitdə mobil cihazların istifadəsi ilə bağlı riskləri diqqətdə saxlamalı və aşağıda göstərilənləri nəzərə almalıdır:

4.2.2.1. mobil cihazların qeydiyyatı;

4.2.2.2. mobil cihazların fiziki təhlükəsizliyi üzrə tələbləri;

4.2.2.3. proqram təminatının yüklənməsi ilə bağlı məhdudiyyətləri;

4.2.2.4. mobil cihazların proqram təminatının versiyaları, o cümlədən tətbiq əlavələri (patch) üzrə tələbləri;

4.2.2.5. informasiya xidmətlərinə qoşulma ilə bağlı məhdudiyyətləri;

4.2.2.6. girişlərə nəzarət;

4.2.2.7. kriptoqrafik vasitələri;

4.2.2.8. zərərverici proqram təminatlarından müdafiə;

4.2.2.9. ehtiyat nüsxələr;

4.2.2.10. məsafədən söndürmə, silmə və ya bloklama;

4.2.2.11. veb xidmətlərin və veb proqram təminatlarının istifadəsi;

4.2.3. məsafədən iş fəaliyyətinə icazə verildiyi halda məlumatlarla təhlükəsiz formada işləməni təmin etmək üçün siyasət və dəstəkləyici təhlükəsizlik tədbirləri tətbiq edilməli və bu məqsədlə aşağıdakılar müəyyən olunmalıdır:

4.2.3.1. fiziki təhlükəsizlik tələbləri;

4.2.3.2. ev şəbəkəsi və simsiz şəbəkələr üzrə təhlükəsizlik tələbləri;

4.2.3.3. əqli mülkiyyət hüquqları ilə bağlı mübahisələrin qarşısını almaq məqsədilə şəxsi mobil cihazlarda yaradılan tətbiqlər üzrə siyasət və prosedurlar;

4.2.3.4. zərərverici proqram təminatlarından müdafiə üzrə tələblər.

5. İnsan resurslarının təhlükəsizliyi

5.1. Bank işçilərin və kontragentlərin fəaliyyətə başlamazdan əvvəl informasiya təhlükəsizliyi sahəsində onlar üçün nəzərdə tutulmuş vəzifələrə uyğun olmalarını təmin etmək məqsədilə aşağıdakı tədbirləri həyata keçirir:

5.1.1. biznes tələblərinə, giriş əldə edilən informasiyanın təsnifatına və proqnozlaşdırılan risklərə adekvat olaraq işə qəbul üçün müraciət etmiş namizədlərin uyğunluğu müəyyən olunmalıdır;

5.1.2. işçilər və kontragentlərlə bağlanmış müqavilələrdə onların və bankın informasiya təhlükəsizliyi üzrə öhdəlikləri müəyyənləşdirilməlidir.

5.2. Bank işçilərin, kontragentlərin, habelə müştərilərin informasiya təhlükəsizliyi ilə bağlı öz öhdəliklərini bilməsini və yerinə yetirməsini təmin etmək məqsədilə aşağıdakı tədbirləri həyata keçirir:

5.2.1. bütün işçilərin və kontragentlərin bankın müəyyən etdiyi siyasətlər və prosedurlara uyğun olaraq informasiya təhlükəsizliyini tətbiq etməsini tələb etməlidir;

5.2.2. bütün işçiləri və müvafiq hallarda kontragentləri onların funksiyaları ilə əlaqədar bankın siyasətləri və prosedurları, onlarda baş vermiş yeniliklərlə əlaqədar müvafiq məlumatlandırma təlimlərinə cəlb etməli, onların müvafiq təlim proqramını tam bitirməsi və proqrama yiyələnməsinin təsdiq olunması kimi tələblər müəyyən etməlidir;

5.2.3. bütün işçilər və kontragentlər, habelə müştərilər informasiya təhlükəsizliyi tələbləri ilə əlaqədar ən azı ildə iki dəfə maarifləndirilməlidir;

5.2.4. bankın təşkilati strukturu (İdarə Heyəti daxil olmaqla) üzrə informasiya təhlükəsizliyinə dair təlim proqramları bankın Müşahidə Şurası tərəfindən təsdiq edilməli və icrasına nəzarət edilməlidir;

5.2.5. informasiya təhlükəsizliyinin pozulmasına yol vermiş işçilərlə bağlı qanunvericiliklə müəyyən edilmiş tədbirlərin görülməsi üçün bankdaxili intizam qaydaları mövcud olmalıdır.

5.3. Əmək və kontragent münasibətlərinə xitam verilməsi və ya dəyişdirilməsi halında bankın maraqlarının qorunması məqsədilə işçilərlə əmək, kontragentlərlə müqavilə münasibətlərinə xitam verilməsi və ya dəyişdirilməsindən sonra informasiya təhlükəsizliyi üzrə öhdəliklər və vəzifələr müəyyənləşdirilməli və onlara bildirilməlidir.

6. Aktivlərin idarə olunması

6.1. Banklarda aktivlərin və onların mühafizəsi ilə bağlı müvafiq öhdəliklərin müəyyənləşdirilməsi üçün aşağıdakı tədbirlər həyata keçirilir:

6.1.1. informasiya, habelə informasiyanın işlənməsi vasitələri ilə bağlı aktivlər müəyyənləşdirilməli, bu aktivlərin inventarizasiyası aparılmalı və aktuallığı təmin edilməlidir;

6.1.2. inventarizasiya edilmiş aktivlər üzrə onların bütün istifadə dövründə düzgün idarə edilməsinə məsul olan aktiv sahibləri müəyyən edilməlidir;

6.1.3. informasiya, habelə informasiya ilə bağlı digər aktivlərdən və informasiyanın işlənməsi vasitələrindən məqbul istifadə qaydaları müəyyən edilməli, sənədləşdirilməli və tətbiq edilməlidir;

6.1.4. əmək və xidmət müqavilələrinin müddətləri bitdiyi zaman işçilər və kontragentlər istifadələrində olan bütün

aktivləri banka geri qaytarmalıdırlar.

6.2. İnformasiyanın bank üçün əhəmiyyətlilik dərəcəsinə uyğun olaraq lazımi səviyyədə mühafizə ilə təmin olunması məqsədilə aşağıdakı tədbirlər görülür:

6.2.1. informasiyanın qanunvericiliyin tələbləri, dəyəri, əhəmiyyətliliyi və icazəsiz açıqlanma və ya dəyişikliyə qarşı həssaslığı baxımından ən azı aşağıdakı siniflər üzrə təsnifatı həyata keçirilməlidir:

6.2.1.1. açıq - ictimaiyyətə açıqlanması mümkün olan informasiya;

6.2.1.2. məxfi - dövlət sirri təşkil edən məlumatlar;

6.2.1.3. konfidensial - kommersiya, bank sirləri, konfidensial fərdi məlumatlar və Azərbaycan Respublikasının qanunvericiliyinə əsasən konfidensial hesab olunan digər informasiya;

6.2.2. bank tərəfindən qəbul edilmiş informasiyanın təsnifatına uyğun olaraq informasiyanın işarələnməsi ilə bağlı müvafiq prosedurlar hazırlanmalı və tətbiq edilməlidir;

6.2.3. informasiya daşıyıcılarının işarələnməsi informasiyanın sinif mənsubiyyətindən asılı olaraq onlara "Məxfi informasiya", "Konfidensial informasiya" və digər qriflərin müəyyən edilməsi ilə həyata keçirilməlidir;

6.2.4. informasiya daşıyıcılarının qriflə işarələnməsi zamanı tələblər aşağıdakılardan ibarətdir:

6.2.4.1. qrif aydın görünməli və fərqlənməlidir;

6.2.4.2. qrifin pozulmasına yol verməmək üçün o, asan silinən (ləğv olan, qopan) olmamalıdır;

6.2.4.3. əgər format işarələnməyə imkan verirsə, faylların işarələnməsi faylı açarkən aydın görünən və fərqlənən işarə daxil edilməklə həyata keçirilməlidir;

6.2.5. bank tərəfindən qəbul edilmiş informasiyanın təsnifatına uyğun olaraq aktivlərin idarə edilməsi ilə bağlı prosedurlar hazırlanmalı və tətbiq edilməlidir.

6.3. İnformasiya daşıyıcılarında saxlanılan informasiyaların icazəsiz açıqlanmasının, dəyişdirilməsinin, ləğv edilməsinin və ya zədələnməsinin qarşısının alınması məqsədilə aşağıdakı tədbirlər həyata keçirilir:

6.3.1. bank tərəfindən qəbul edilmiş informasiyanın təsnifatına uyğun olaraq çıxarıla bilən informasiya daşıyıcıları ilə bağlı prosedurlar müəyyən edilməli və tətbiq edilməlidir;

6.3.2. istifadəsinə zərurət olmadıqda informasiya daşıyıcıları bank tərəfindən müəyyən edilmiş prosedur qaydalara uyğun olaraq məhv edilməlidir;

6.3.3. informasiya daşıyıcılarının daşınması zamanı sanksiya edilməmiş müdaxilə hallarının qarşısının alınması ilə bağlı müvafiq tədbirlər həyata keçirilməlidir.

7. Girişlərə nəzarət

7.1. İnformasiya və informasiyanın işlənməsi vasitələrinə girişlərin məhdudlaşdırılması məqsədilə aşağıdakı tədbirlər həyata keçirilir:

7.1.1. girişlərə nəzarət siyasəti biznes və informasiya təhlükəsizliyi tələbləri nəzərə alınmaqla formalaşdırılmalı, sənədləşdirilməli və aktuallığı təmin olunmalıdır;

7.1.2. istifadəçilər yalnız xüsusi olaraq istifadə etmək səlahiyyətinə malik olduqları şəbəkə və şəbəkə xidmətlərinə girişlə təmin edilməlidir.

7.2. İnformasiya sistemlərinə sanksiya edilmiş istifadəçinin girişini təmin etmək məqsədilə aşağıdakı tədbirlər həyata keçirilir:

7.2.1. giriş hüquqlarının təyin edilməsini təmin etmək üçün istifadəçi qeydiyyatı və qeydiyyatdan çıxarma prosesi rəsmiləşdirilməli və tətbiq edilməlidir;

7.2.2. istifadəçi səlahiyyətlərinə müvafiq olaraq bütün sistem və xidmətlərə giriş hüquqlarının təyin edilməsi və ya ləğv edilməsi üzrə proseslər müəyyən edilməli, rəsmiləşdirilməli və tətbiq edilməlidir;

7.2.3. imtiyazlı giriş hüquqlarının bölüşdürülməsi və istifadəsi məhdudlaşdırılmalı və idarə olunmalıdır;

7.2.4. məxfi autentifikasiya məlumatlarının (parol, bir neçə faktorlu eyniləşdirmə məlumatı, elektron imza, biometrik məlumat və sair) ötürülməsi prosesi müəyyən edilməli, rəsmiləşdirilməli və tətbiq edilməlidir.

7.2.5. aktiv sahibləri istifadəçilərin giriş hüquqlarını davamlı olaraq nəzərdən keçirməlidir;

7.2.6. işçilərlə əmək, kontragentlərlə müqavilə münasibətlərinə xitam verildikdə və ya dəyişdirildikdə onların informasiya və informasiyanın işlənməsi vasitələrinə giriş hüquqları dərhal ləğv edilməli və ya düzəlişə uyğunlaşdırılmalıdır.

7.3. İstifadəçiləri özlərinin məxfi autentifikasiya məlumatlarını qorumağa cavabdeh etmək məqsədilə bank tərəfindən müəyyən edilən qaydalara riayət etmələri tələb olunmalı və nəzarəti təmin edilməlidir.

7.4. İnformasiya sistemi və tətbiqi-proqram təminatlarına icazəsiz girişlərin qarşısını almaq məqsədilə aşağıdakı tədbirlər həyata keçirilir:

7.4.1. girişlərə nəzarət siyasətinə uyğun olaraq informasiya sistemi və tətbiqi-proqram təminatlarına girişlər məhdudlaşdırılmalıdır;

7.4.2. girişlərə nəzarət siyasətinə müvafiq olaraq informasiya sistemi və tətbiqi-proqram təminatlarına giriş ən azı aşağıdakı təhlükəsiz daxil olma proseduru ilə idarə edilməlidir:

7.4.2.1. "brute-force" hücumdan qorunma metodları tətbiq edilməlidir;

7.4.2.2. uğursuz və uğurlu cəhdlərin loqlanması aparılmalıdır;

7.4.2.3. uğurlu giriş tamamlandıqdan sonra aşağıdakı məlumatların göstərilməsi təmin olunmalıdır:

7.4.2.3.1. əvvəlki uğurlu girişin tarixi və saatı;

7.4.2.3.2. son uğurlu girişdən sonra baş verən uğursuz giriş cəhdlərinin təfərrüatları.

7.4.2.4. daxil edilən parol göstərilməməlidir;

7.4.2.5. parollar şəbəkə üzərindən açıq mətn formasında ötürülməməlidir;

7.4.2.6. müəyyən edilmiş müddət ərzində heç bir fəaliyyət olmadığı təqdirdə sistemlə qurulmuş əlaqələrin başa çatdırılması təmin edilməlidir;

7.4.3. Parolların idarə edilməsi sistemində parolların mürəkkəbliyi aşağıdakı şəkildə təmin edilməlidir:

7.4.3.1. istifadəçilər üçün parol uzunluğu minimum 8 (səkkiz) simvol olmalıdır;

7.4.3.2. imtiyazlı giriş hüquqlu istifadəçilər üçün parol uzunluğu minimum 12 (on iki) simvol olmalıdır;
7.4.3.3. parol aşağıdakılardan ən azı üçünün birləşməsindən ibarət olmalıdır:
7.4.3.3.1. ən azı bir kiçik hərf (a-z);
7.4.3.3.2. ən azı bir böyük hərf (A-Z);
7.4.3.3.3. ən azı bir rəqəm (0-9);
7.4.3.3.4. ən azı bir xüsusi simvol (məsələn, @ # $% ^ & * () _ + | ~ - = \ `{} []:"; '<> /).
7.4.3.4. parollarda istifadəçi identifikatorlarından istifadə olunmamalıdır;
7.4.3.5. parollarda ardıcıl olaraq ikidən çox eyni simvoldan istifadə oluna bilməz;
7.4.3.6. sistemə ilk giriş zamanı və ya parolun sistem inzibatçısı tərəfindən yenilənməsindən sonra informasiya sistemi istifadəçidən parolun yenilənməsini tələb etməli və tələbin inkar edilməsinə imkan verməməlidir;
7.4.3.7. parolun ən çoxu 6 (altı) dəfə səhv yığılması cəhdlərindən sonra sistemə giriş məhdudlaşdırılmalıdır;
7.4.3.8. parolların qüvvədə olma müddəti ən çoxu 90 (doxsan) gün olmalıdır. Parolun qüvvədə olması müddətinin bitməsi ilə bağlı istifadəçiyə müvafiq məlumatlandırma göndərilməlidir;
7.4.3.9. sistemdə istifadə olunmuş son 12 (on iki) parolun təkrar istifadəsinin qarşısı alınmalıdır;
7.4.3.10. standart (susmaya görə) istifadəçi hesablarının parolları ildə bir dəfədən az olmayaraq dəyişdirilməlidir;
7.4.3.11. istifadəçi parolları sistem inzibatçılarına açıq olmamalıdır;
7.4.3.12. 90 (doxsan) gündən artıq istifadə edilməyən bütün istifadəçi hesabları blok edilməlidir;
7.4.4. sistem və tətbiqi-proqram təminatının mənbə kodlarına giriş hüquqları məhdudlaşdırılmalıdır.

8. Kriptoqrafiya

8.1. İnformasiyanın konfidensiallığının, həqiqiliyi və/və ya tamlığının qorunması üçün kriptoqrafiyanın düzgün seçilməsi və effektiv istifadəsinin təmin olunması məqsədilə aşağıdakı tədbirlər həyata keçirilir:
8.1.1. informasiyanın mühafizəsi məqsədilə kriptoqrafik vasitələrdən istifadə üzrə siyasət formalaşdırılmalı və tətbiq edilməlidir. Siyasət ən azı aşağıdakı tələbləri əhatə etməlidir:
8.1.1.1. kriptoqrafik vasitələrlə təhlükəsizliyi təmin olunmalı informasiya müəyyən olunmalıdır;
8.1.1.2. risklərin qiymətləndirilməsinə əsasən informasiyanın kriptoqrafik vasitələrin şifrələnmə alqoritminin mürəkkəblik səviyyəsi müəyyən edilməlidir;
8.1.1.3. kriptoqrafik vasitələrdən istifadə üzrə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlər müəyyən edilməlidir;
8.1.2. kriptoqrafik açarların idarə edilməsi üzrə siyasət formalaşdırılmalı və açarların bütün istifadə dövrü ərzində tətbiq edilməlidir. Siyasət ən azı aşağıdakı tələbləri əhatə etməlidir:
8.1.2.1. kriptoqrafik açarların yaradılması;
8.1.2.2. kriptoqrafik açarların paylanılması;
8.1.2.3. kriptoqrafik açarların dəyişdirilməsi;
8.1.2.4. kriptoqrafik açarların geri çağırılması;
8.1.2.5. kriptoqrafik açarların qüvvəsinin dayandırılması və bərpa edilməsi;
8.1.2.6. kriptoqrafik açarların ehtiyat nüsxəsinin yaradılması və saxlanılması;
8.1.2.7. kriptoqrafik açarların məhv edilməsi;
8.1.2.8. kriptoqrafik açarların idarə edilməsi üzrə loqların qeydiyyatının aparılması.

9. Fiziki və perimetr üzrə təhlükəsizlik

9.1. İnformasiya və informasiyanın işlənməsi vasitələrinə sanksiya edilməmiş fiziki giriş, zədə və təsirin qarşısının alınması məqsədilə aşağıdakı tədbirlər həyata keçirilir:
9.1.1. bankda informasiya və informasiyanın işlənməsi vasitələrinin saxlanıldığı məkanların mühafizəsinin təmin edilməsi məqsədilə təhlükəsizlik perimetrləri müəyyən edilməli və istifadə edilməlidir;
9.1.2. təhlükəsizlik perimetrlərində işləmə üzrə müvafiq prosedurlar formalaşdırılmalı və tətbiq edilməlidir;
9.1.3. təhlükəsizlik perimetrləri yalnız səlahiyyətli şəxslərin girişinin təmin edilməsi üçün müvafiq giriş nəzarət mexanizmi (kart oxuyucu, biometrik məlumat oxuyucu və (və ya) PİN pad) ilə mühafizə olunmalıdır;
9.1.4. təhlükəsizlik perimetrlərinə giriş icazəsi olan səlahiyyətli şəxslərin siyahısı tərtib edilməli və aktuallığı təmin edilməlidir;
9.1.5. təhlükəsizlik perimetrləri hərəkət detektorları ilə təchiz edilməlidir;
9.1.6. icazəsiz şəxslərin daxil ola biləcəyi giriş nöqtələri (yükləmə və boşaltma sahələri) və digər oxşar nöqtələrə nəzarət edilməli və sanksiya edilməmiş giriş hallarının qarşısının alınması üçün həmin sahələrin informasiyanın işlənməsi vasitələrindən təcrid edilməsi təmin olunmalıdır.
9.2. Aktivlərin itirilməsi, zədələnməsi, qanunsuz olaraq ələ keçirilməsi və ya vəziyyətinin pisləşməsi və bankın fəaliyyətinin pozulmasının qarşısının alınması məqsədilə aşağıdakı tədbirlər həyata keçirilir:
9.2.1. sanksiya edilməmiş giriş imkanlarının, ətraf mühit təhdidlərinin və fəlakətlərin yaratdığı risklərin azaldılması məqsədilə avadanlıqların xüsusi ayrılmış yerlərdə yerləşdirilməsi və qorunması təmin edilməlidir;
9.2.2. təbii fəlakət, səlahiyyətsiz müdaxilə və qəza hallarının qarşısının alınması üçün iş yerlərinin, otaqların və avadanlıqların yerləşdiyi məkanların fiziki mühafizəsi təmin edilməlidir;
9.2.3. İnformasiyanın işlənməsi mərkəzi (server otağı) əlavə olaraq aşağıdakı tələblərə də cavab verməlidir:
9.2.3.1. 7/24 rejimində video-müşahidə həyata keçirilməli və video-müşahidə görüntülərinin ən azı 6 (altı) ay müddətində saxlanması təmin edilməlidir;
9.2.3.2. havalandırma (kondisioner) avadanlıqları və temperaturun tənzimlənməsi üçün termometrlə təchiz olunmalıdır;
9.2.3.3. mühafizə və yanğın-siqnalizasiya sistemləri ilə təchiz edilməlidir;
9.2.3.4. avtomatlaşdırılmış yanğınsöndürmə sistemləri ilə təchiz edilməlidir;

9.2.3.5. rütubətlilik göstəricilərini ölçən cihaz və tənzimləyən avadanlıqlar ilə təchiz edilməlidir;
9.2.3.6. döşəmə antistatik örtüklə təmin edilməlidir;
9.2.3.7. fasiləsiz elektrik enerjisi ilə təmin edən qida mənbəyi və generator ilə təchiz edilməlidir;
9.2.3.8. elektrik və telekommunikasiya xətlərinin kəsilməzliyi təmin edilməli, habelə kənar müdaxilələrdən və zədələnmələrdən qorunması məqsədilə aşağıdakılar nəzərə alınmalıdır:
9.2.3.8.1. elektrik və telekommunikasiya xətləri fərqli kanallarla aparılmalıdır;
9.2.3.8.2. elektrik və telekommunikasiya xətlərinin qovşaqları mühafizə edilməli və yerləşən otaqlara girişə nəzarət olunmalıdır.
9.2.4. avadanlıqlar elektrik enerjisinin kəsilməsi və dəstəkləyici vasitələrdə (fasiləsiz qida mənbələri, elektrik enerjisi, havalandırma və sair) baş verə biləcək nasazlıqlar nəticəsində yaranan fasilələrdən qorunmalıdır;
9.2.5. avadanlıqların etibarlı və davamlı fəaliyyətinin təmin edilməsi məqsədilə onlara adekvat dəstəkləmə xidməti göstərilməlidir;
9.2.6. avadanlıqlar, informasiya və ya tətbiqi-proqram təminatları razılaşdırılmadan bankın ərazisindən kənara çıxarılmamalıdır;
9.2.7. aktivlərin kənarda istifadəsi ilə bağlı yarana biləcək risklər nəzərə alınmalı və müvafiq təhlükəsizlik tədbirləri tətbiq edilməlidir;
9.2.8. informasiya daşıyıcıları olan avadanlıqlar məhv edilməzdən və ya yenidən istifadəyə verilməzdən öncə saxlanılan konfidensial informasiya və lisenziyalı proqram təminatları bərpanın mümkün olmaması təmin edilməklə silinməlidir. Avadanlıqların fiziki məhv edilməsi prosedurlaşdırılmalı, habelə xüsusi alət və texnologiyalardan istifadə etməklə aparılaraq sənədləşdirilməlidir;
9.2.9. istifadəçilər istifadələrində olan avadanlıqları nəzarətsiz saxladıqları müddətdə onların adekvat təhlükəsizliyinin təmin edildiyinə əmin olmalıdırlar. Bütün istifadəçilər nəzarətsiz qalmış avadanlıqların təhlükəsizliyinin təmin edilməsi ilə bağlı tələblər və prosedurlar, habelə öhdəlikləri barədə məlumatlandırılmalı, o cümlədən bank tərəfindən bu barədə ildə iki dəfədən az olmayaraq maarifləndirmə tədbirləri aparılmalıdır. İstifadəçilərə aşağıdakılar kommunikasiya olunmalıdır:
9.2.9.1. fəaliyyət bitdikdə bütün aktiv sessiyalar dayandırılmalıdır;
9.2.9.2. parol ilə girişin bloklanması və ya avtomatik ekran qoruyucusu funksiyası aktivləşdirilməlidir;
9.2.9.3. ehtiyac olmadıqda tətbiqi-proqram təminatları və ya şəbəkə xidmətləri bağlanılmalıdır;
9.2.10. kağız sənədlər və informasiya daşıyıcıları üçün təmiz masa siyasəti, o cümlədən informasiyanın işlənməsi vasitələri üçün təmiz ekran siyasəti qəbul edilməli və ən azı aşağıdakılar nəzərə alınmalıdır:
9.2.10.1. kritik informasiya və informasiyanın işlənməsi vasitələri mühafizə olunan sahədə saxlanılmalıdır;
9.2.10.2. kompüter avadanlıqlarından istifadə başa çatdırıldıqda müvafiq parol, token və digər istifadəçi autentifikasiya mexanizmi ilə giriş bağlanmalıdır;
9.2.10.3. printer, surətçıxarma və bu kimi digər avadanlıqlardan kritik informasiya dərhal təmizlənməli və mühafizəsi təmin olunmalıdır.

10. Fəaliyyətin təhlükəsizliyi

10.1. İnformasiyanın işlənməsi vasitələrinin düzgün və təhlükəsiz fəaliyyətini təmin etmək məqsədilə aşağıdakı tədbirlər həyata keçirilir:
10.1.1. əməliyyat prosedurları sənədləşdirilməli və müvafiq işçilər üçün əlçatan olmalıdır. Əməliyyat prosedurları ən azı aşağıdakı prosedurlardan ibarət olmalıdır:
10.1.1.1. tətbiqi-proqram təminatlarının yüklənməsi və quraşdırılması;
10.1.1.2. ehtiyat nüsxələrin yaradılması;
10.1.1.3. digər tətbiqi-proqram təminatları ilə qarşılıqlı inteqrasiya əlaqələri;
10.1.1.4. səhvlərin idarə edilməsi;
10.1.1.5. tətbiqi-proqram təminatlarının dəstəklənməsi üzrə əlaqələndirici şəxslərlə kommunikasiya planları;
10.1.1.6. fövqəladə hallar zamanı tətbiqi-proqram təminatlarının bərpası;
10.1.1.7. audit izi və loqların qeydiyyatının həyata keçirilməsi;
10.1.1.8. monitorinq prosedurları;
10.1.2. dəyişikliklərin idarə edilməsi prosesini tənzimləyən prosedurlar hazırlanmalı və tətbiqi təmin edilməlidir. Dəyişikliklərin idarə edilməsi prosesində bütün müvafiq məlumatları ehtiva edən yazılar saxlanılmalıdır. Bankda, biznes proseslərdə, informasiyanın işlənməsi vasitələrində və tətbiqi-proqram təminatlarında informasiya təhlükəsizliyinə təsir edən bütün dəyişikliklər idarə olunmalı və ən azı aşağıdakılar nəzərə alınmalıdır:
10.1.2.1. əhəmiyyətli dəyişikliklərin müəyyən olunması və qeydiyyata alınması;
10.1.2.2. dəyişikliklərin planlaşdırılması və testləşdirilməsi;
10.1.2.3. informasiya təhlükəsizliyinə təsirlər də daxil olmaqla, dəyişikliklərin potensial təsirlərinin risk əsaslı qiymətləndirilməsinin aparılması;
10.1.2.4. informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsinin yoxlanılması;
10.1.2.5. dəyişikliklərin təfərrüatlarının bütün əlaqəli şəxslərə çatdırılması;
10.1.2.6. dəyişikliklərin tətbiqi zamanı uğursuz dəyişikliklər və ya gözlənilməz halların ləğvi və ya geri qayıtma prosedurları və məsuliyyətlərinin müəyyən olunması;
10.1.2.7. insidentlərin həll edilməsi üçün zəruri olan təxirəsalınmaz dəyişikliklər üzrə proseslərin müəyyən olunması;
10.1.3. resursların istifadəsi monitorinq edilməli, tənzimlənməli və fəaliyyət üzrə potensial ehtiyaclar nəzərə alınmaqla proqnozlaşdırılmalıdır. Resursların idarəedilməsi prosesi ən azı aşağıdakıları əhatə etməlidir:
10.1.3.1. köhnəlmiş məlumatların silinməsi təmin edilməlidir;
10.1.3.2. yararsız tətbiqi-proqram təminatlarının və verilənlər bazasının idarəetmə sistemlərinin istismardan çıxarılması təmin edilməlidir;

10.1.3.3. tətbiqi-proqram təminatlarının məntiqinin və verilənlər bazasının idarəetmə sistemlərinə edilən sorğuların optimizasiyası təmin edilməlidir;

10.1.4. əməliyyat mühitinə sanksiya edilməmiş girişlər və dəyişikliklərlə bağlı risklərin minimallaşdırılması məqsədilə inkişaf, sınaq və əməliyyat mühitlərinin ayrıIması təmin edilməlidir.

10.2. İnformasiya və informasiyanın işlənməsi vasitələrinin zərərverici proqramlardan qorunmasını təmin etmək məqsədilə aşağıdakı tədbirlər həyata keçirilir:

10.2.1. zərərverici proqram təminatlarından müdafiə məqsədilə aşkarlama, qarşısını alma və bərpa istiqamətində nəzarət tədbirləri müvafiq istifadəçi məlumatlandırılması ilə birgə həyata keçirilməlidir;

10.2.2. bankda yalnız lisenziyalı zərərverici proqram təminatından mühafizə vasitələrinin tətbiqi təmin edilməlidir;

10.2.3. zərərverici proqram təminatından mühafizə vasitələri bütün informasiyanın işlənməsi vasitələrinə tətbiq edilməlidir;

10.2.4. zərərverici proqram təminatından mühafizə vasitələrinin mərkəzləşdirilmiş qaydada idarə edilməsi təmin edilməlidir;

10.2.5. zərərverici proqram təminatından mühafizə vasitələrinin quraşdırılması, sazlanılması, yoxlanılması, dəstəklənməsi və monitorinqi səlahiyyətli şəxslər tərəfindən həyata keçirilməlidir;

10.2.6. zərərverici proqram təminatından mühafizə vasitələrinin bazaları avtomatik olaraq ən son yenilənmələrlə təmin edilməlidir;

10.2.7. zərərverici proqram təminatından mühafizə vasitələri aşkar edilmiş bütün zərərverici proqram təminatlarının avtomatik olaraq silinməsi üçün sazlanmalıdır;

10.2.8. zərərverici proqram təminatlarının silinməsi mümkün olmadıqda informasiyanın işlənməsi vasitəsinin şəbəkədən ayrılması təmin edilməlidir;

10.2.9. zərərverici proqram təminatından mühafizə vasitələri tərəfindən ən azı aşağıdakı yoxlamalar həyata keçirilməlidir:

10.2.9.1. şəbəkə və ya istənilən yaddaş qurğuları vasitəsilə qəbul edilən informasiyanın istifadədən öncə yoxlanılması;

10.2.9.2. elektron məktublara qoşmaların istifadədən öncə yoxlanılması;

10.2.9.3. internet səhifələrin yoxlanılması;

10.2.10. bütün zərərverici proqram təminatlarına yoluxma faktları qeydə alınmalı, habelə onların tiplərini və yoluxma mənbələri göstərilməklə hesabatlığı aparılmalıdır.

10.3. Banklarda istifadəsinə icazə verilən tətbiqi-proqram təminatlarının siyahısı formalaşdırılmalı və quraşdırılması yalnız səlahiyyətli şəxslər tərəfindən həyata keçirilməlidir.

10.4. Banklarda bütün xarici yaddaş qurğularının istifadəsi qadağan edilməli, istifadəsinə zərurət yarandığı halda siyahısı formalaşdırılmalı və fəaliyyət səlahiyyətli şəxslər tərəfindən idarə edilməlidir. Xarici yaddaş qurğularında konfidensial informasiyanın yalnız şifrələnmiş şəkildə saxlanılması təmin edilməlidir.

10.5. İnformasiya itkisinin qarşısının alınması məqsədi ilə kritik informasiya sisteminin ehtiyat nüsxələrinin yaradılması, həmçinin bərpa prosesinin testləşdirilməsi üzrə ən azı aşağıdakı tələbləri əhatə edən prosedurlar hazırlanır və tətbiqi təmin edilir:

10.5.1. ehtiyat nüsxələrin yaradılması və bərpası məqsədilə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlər müəyyən edilməlidir;

10.5.2. ehtiyat nüsxələrin yaradılması vasitələrinin mərkəzləşdirilmiş qaydada idarə edilməsi təmin edilməlidir;

10.5.3. konfidensial informasiyanın ehtiyat nüsxələrinin şifrələnmiş şəkildə saxlanılması təmin edilməlidir;

10.5.4. gündəlik, həftəlik, aylıq və illik ehtiyat nüsxələrinin yaradılması təmin edilməlidir;

10.5.5. ehtiyat nüsxələrin ildə ən azı bir dəfə olmaqla sınaq bərpası həyata keçirilməli və nəticələri rəsmiləşdirilməlidir;

10.5.6. ehtiyat nüsxələrin yaradılması üzrə loqların qeydiyyatı aparılmalı, saxlanılmalı və davamlı olaraq gözdən keçirilməlidir;

10.5.7. təbii fəlakət, bədniyətli müdaxilə və qəza hallarından müdafiə məqsədilə ehtiyat nüsxələrin bankın olduğu yerdən kənarda ehtiyat mərkəzində saxlanılması təmin edilməlidir.

10.6. Kritik informasiya sistemində hadisələrin qeydiyyatını aparmaq və dəlil formalaşdırmaq üçün aşağıdakı tədbirlər görülür:

10.6.1. informasiya təhlükəsizliyi hadisələri, xətalar, habelə istifadəçilərin fəaliyyəti barədə məlumatları qeydə alan hadisə loqlarının qeydiyyatı aparılmalı, saxlanılmalı və mütəmadi olaraq gözdən keçirilməlidir. Hadisə loqları bir il müddətinə saxlanılmalıdır. Qeydiyyatı aparılan loqlara aşağıdakılar daxil edilməlidir:

10.6.1.1. informasiya xarakterli loqlar:

10.6.1.1.1. "debug" loqları (debug) – informasiya sistemləri və avadanlıqlar (şəbəkə və təhlükəsizlik) tərəfindən bütün proseslər üzrə araşdırma aparılması üçün aktivləşdirilən loqlar;

10.6.1.1.2. informativ loqlar (info) – informasiya sistemləri və avadanlıqlar (şəbəkə və təhlükəsizlik) tərəfindən servislərin normal işləməsi barədə məlumatları əks etdirən loqlar.

10.6.1.2. kritik xarakterli loqlar:

10.6.1.2.1. xəbərdarlıq loqları (warn) – informasiya sistemləri və avadanlıqlar (şəbəkə və təhlükəsizlik) tərəfindən servislərin anomal fəaliyyəti və baş verə biləcək nasazlıqları özündə əks etdirən loqlar;

10.6.1.2.2. səhvlər üzrə loqlar (error) – informasiya sistemləri və avadanlıqlar (şəbəkə və təhlükəsizlik) tərəfindən servislərin vacib elementləri üzrə dayanmaları və ya sıradan çıxmaları əks etdirən loqlar;

10.6.1.2.3. kritik loqlar (critical) – informasiya sistemləri və avadanlıqlar (şəbəkə və təhlükəsizlik) üzrə baş vermiş kritik hadisələri özündə əks etdirən loqlar.

10.6.2. hər bir hadisə loqu özündə ən azı aşağıdakı məlumatları saxlamalıdır:

10.6.2.1. istifadəçi identifikatoru;

10.6.2.2. əsas hadisələrin baş vermə tarixi, vaxtı və təfərrüatları (giriş, çıxış və sair);

10.6.2.3. hadisənin statusu, və (və ya) xətanın kodu;
10.6.2.4. uğurlu və uğursuz giriş cəhdləri;
10.6.2.5. sistem konfiqurasiyasına dəyişikliklər;
10.6.2.6. giriş edilmiş fayllar və giriş növü;
10.6.2.7. şəbəkə ünvanları və protokolları;
10.6.2.8. mühafizə sistemlərinin aktivləşdirilməsi və deaktivləşdirilməsi;
10.6.2.9. tətbiqi-proqram təminatında həyata keçirilən əməliyyatlar;
10.6.3. loqların qeydiyyatı vasitələri və loq məlumatları dəyişdirilməyə və sanksiya olunmamış girişə qarşı müdafiə edilməlidir;
10.6.4. qeydiyyat jurnallarında sistem inzibatçılarının və əməliyyat inzibatçılarının fəaliyyətləri üzrə loqlar qeydə alınmalı, qorunmalı və mütəmadi olaraq gözdən keçirilməlidir;
10.6.5. loqların mühüm əhəmiyyət kəsb etdiyini nəzərə alaraq, informasiya sistemlərinin və informasiyanın işlənməsi vasitələrinin vahid zaman mənbəyi ilə sinxronlaşdırılması təmin edilməlidir.
10.7. Kritik informasiya sistemində texniki zəifliklərin müəyyən edilməsi və onlardan sui-istifadəsinin qarşısını almaq məqsədilə aşağıdakı tədbirlər həyata keçirilir:
10.7.1. texniki zəifliklərin monitorinqi, zəifliklər üzrə risklərin qiymətləndirilməsi və tətbiq əlavələrinin (patch management) idarə edilməsi məqsədilə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlər müəyyən edilməlidir;
10.7.2. hər bir kritik informasiya sistemi üzrə texniki zəifliklərin analizi və aradan qaldırılması məqsədilə ildə ən azı bir dəfə müdaxilə sınaqlarının keçirilməsi təmin edilməli və nəticələri rəsmiləşdirilməlidir;
10.7.3. kritik informasiya sisteminin əməliyyat mühitinə keçirilməsi texniki zəifliklərin analizi və aradan qaldırılması məqsədilə müdaxilə sınaqları keçirildikdən sonra təmin edilməlidir;
10.7.4. texniki zəiflik aşkar edildikdən sonra əlaqəli risklər və görüləcək tədbirlər müəyyənləşdirilməlidir.
10.8. İnformasiya sistemlərini əhatə edən audit zamanı bankın biznes proseslərinə mənfi təsirləri minimallaşdırmaq məqsədilə audit tələbləri və fəaliyyəti dəqiqliklə planlaşdırılır və aktiv sahibi ilə razılaşdırılır.

11. İnformasiya mübadiləsinin təhlükəsizliyi

11.1. Şəbəkələrdə və onu dəstəkləyən informasiyanın işlənməsi vasitələrində informasiyanın qorunması məqsədilə şəbəkələr idarə edilir və fəaliyyətinə nəzarət edilir. Şəbəkələrdə və onu dəstəkləyən informasiyanın işlənməsi vasitələrində informasiyanın qorunması məqsədilə ən azı aşağıdakılar nəzərə alınır:
11.1.1. şəbəkə infrastrukturunun idarə edilməsi üzrə öhdəlikləri və prosedurları tənzimləyən qaydalar hazırlanmalı və tətbiqi təmin olunmalıdır;
11.1.2. tətbiqi-proqram təminatlarının çıxışı olan simsiz və qlobal şəbəkələrdə ötürülən informasiyanın konfidensiallığının və tamlığının qorunması məqsədilə adekvat nəzarət mexanizmləri tətbiq edilməlidir;
11.1.3. informasiya təhlükəsizliyinə təsir göstərə biləcək hərəkətlərin qeydiyyatı aparılmalı və aşkarlanmasını təmin etmək üçün müvafiq loqlama və monitorinq tətbiq olunmalıdır;
11.1.4. bütün şəbəkə xidmətləri üzrə təhlükəsizlik mexanizmləri, xidmət səviyyələri və idarəetmə tələbləri müəyyən edilməli və daxildə və ya kənardan təmin edilməsindən asılı olmayaraq şəbəkə xidmətlərinin göstərilməsi müqavilələrinə daxil edilməlidir;
11.1.5. şəbəkədə informasiya təhlükəsizliyinin təmin edilməsi məqsədilə ən azı istifadəçilərin və informasiya sistemlərinin seqmentlər üzrə ayrılması təmin edilməlidir.
11.2. Bank daxilində və kənara informasiyanın ötürülməsinin təhlükəsizliyini təmin etmək məqsədilə aşağıdakı tədbirlər həyata keçirilir:
11.2.1. informasiyanın istənilən növ kommunikasiya vasitələri ilə ötürülməsi zamanı təhlükəsizliyin təmin edilməsi məqsədi ilə mübadilə siyasəti, prosedurları və nəzarət mexanizmləri formalaşdırılmalı və tətbiq edilməlidir;
11.2.2. informasiyanın konfidensiallığının qorunması və kənara açıqlanmasının qarşısının alınması üzrə tələblər tərəflər arasında bağlanılan müqavilələrdə nəzərdə tutulmalıdır;
11.2.3. elektron yazışmada istifadə edilən məlumatların sanksiya edilməmiş müdaxilələrə qarşı müdafiəsi təmin edilməlidir.

12. İnformasiya sistemlərinin əldə edilməsi, tətbiqi və dəstəklənməsi

12.1. İnformasiya təhlükəsizliyinin kritik informasiya sisteminin bütün istifadə dövrü ərzində onun ayrılmaz tərkib hissəsi olmasının təmin edilməsi məqsədilə aşağıdakı tədbirlər həyata keçirilir:
12.1.1. yeni informasiya sistemlərinin tətbiqi və ya mövcud informasiya sistemlərinin təkmilləşdirilməsi zamanı informasiya təhlükəsizliyi tələbləri nəzərə alınmalıdır;
12.1.2. açıq şəbəkələr üzərindən tətbiqi proqramlaşdırma interfeysləri vasitəsilə ötürülən informasiyanın kənar müdaxilələrdən, icazəsiz açıqlanmadan və dəyişiklikdən qorunması təmin olunmalıdır;
12.1.3. tətbiqi proqramlaşdırma interfeysləri vasitəsilə mübadilə olunan informasiyanın natamam ötürülməsi, yanlış ünvanlandırılması, sanksiya olunmamış açıqlanması, dəyişdirilməsi, nüsxəsinin çıxarılması və çoxaldılması kimi halların qarşısının alınması məqsədilə informasiyanın mühafizəsi təmin olunmalıdır;
12.1.4. informasiya sistemlərində dəyişikliklərin idarə edilməsi məqsədilə müvafiq idarəetmə prosedurları hazırlanmalı və təsdiq edilməlidir;
12.1.5. informasiya sistemlərində edilən dəyişikliklər risk əsaslı qiymətləndirilməli, tətbiqi prioritetləşdirilməli, geriyə (əvvəlki versiyaya) dönüş strategiyası hazırlanmalı və istismara verilməzdən əvvəl sınaqdan keçirilməlidir;
12.1.6. mühafizə olunan informasiya sistemlərinin tətbiqi prinsipləri müəyyən edilməli, sənədləşdirilməli və informasiya sistemlərinin tətbiqi zamanı istifadə edilməlidir;
12.1.7. informasiya sistemlərinin yaradılması zamanı bütün mühitlərin (inkişaf, sınaq və əməliyyat) təhlükəsizliyi təmin olunmalıdır;

12.1.8. informasiya sistemlərinin tətbiqi üzrə xidmətlər kontragentdən əldə edildikdə təhlükəsizlik tələbləri tərəflər arasında bağlanmış müqavilə ilə təsbit olunmalıdır;

12.1.9. informasiya sistemlərinin tətbiqi zamanı sistemlərin informasiya təhlükəsizliyi mexanizmləri testləşdirilməli və təhlükəsiz fəaliyyəti təmin olunmalıdır;

12.1.10. yeni informasiya sistemlərinin, yeniləmələrin və yeni versiyaların tətbiqi zamanı informasiya təhlükəsizliyi tələblərinə uyğunluq üzrə qəbul sınaqları həyata keçirilməli, sənədləşdirilməli, razılaşdırılmalı və onlara əsasən sistemlərin qəbulu təmin edilməlidir;

12.1.11. sınaq yoxlamaları zamanı konfidensial informasiyadan istifadəyə yol verilməməli, sınaq mühitinin təhlükəsizliyi diqqətdə saxlanılmalı və aparılan əməliyyatların loqlanması təmin edilməlidir.

13. Kontragentlər ilə münasibət

13.1. Kontragentlər ilə münasibətdə informasiya təhlükəsizliyi təmin olunur və aşağıdakı tədbirlər həyata keçirilir:

13.1.1. bankın aktivlərinə giriş icazəsi olan kontragentlərlə münasibətdə risklərin minimallaşdırılması məqsədilə informasiya təhlükəsizliyi tələbləri nəzərə alınmalı, kontragentlərlə razılaşdırılmalı və sənədləşdirilməlidir;

13.1.2. bankın informasiyasına girişi olan, onu işlədən, saxlayan, ötürən və ya informasiya texnologiyaları infrastrukturu komponentlərini təmin edən hər bir kontragentlə bağlı bütün müvafiq informasiya təhlükəsizliyi tələbləri formalaşdırılmalı və onlarla razılaşdırılmalıdır;

13.1.3. kontragentlərlə bağlanmış müqavilələrə informasiya təhlükəsizliyi üzrə risklərin minimallaşdırılması məqsədilə müvafiq tələblər daxil edilməlidir.

13.2. Kontragentlərlə bağlanmış xidmət müqavilələri çərçivəsində informasiya təhlükəsizliyinin və adekvat xidmətlərin təqdim edilməsinin razılaşdırılmış səviyyədə təmin edilməsi məqsədilə aşağıdakılar nəzərə alınır:

13.2.1. kontragentlərin göstərdikləri xidmətlər bank tərəfindən mütəmadi monitorinq edilməli və auditi həyata keçirilməlidir;

13.2.2. kontragentlər tərəfindən göstərilən xidmətlərdə edilən dəyişikliklər informasiya, informasiya sistemləri və proseslərin kritikliyi nəzərə alınmaqla informasiya təhlükəsizliyi üzrə mövcud siyasətə, prosedur və nəzarət mexanizmlərinə uyğun olaraq aparılmalı və risk qiymətləndirilməsi həyata keçirilməlidir;

13.2.3. banklar informasiya təhlükəsizliyi ilə əlaqəli xidmətləri kənardan aldıqları zaman sahib olduqları informasiyanın konfidensiallığı, tamlığı və əlçatanlığını qorumaq, bank fəaliyyətinin fasiləsizliyinə təsirlərini minimallaşdırmaq məqsədilə belə xidmət göstərən kontragentlərin konfidensial və xidməti məlumatlara çıxışını məhdudlaşdırmaq üçün müvafiq tədbirlər görməlidir.

14. İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi

14.1. Təhlükəsizlik hadisələri və zəifliklərin kommunikasiyası daxil olmaqla informasiya təhlükəsizliyi insidentlərinin davamlı və effektiv idarə edilməsi məqsədilə aşağıdakı tədbirlər həyata keçirilir:

14.1.1. informasiya təhlükəsizliyinə təsir göstərə biləcək hərəkətlərin və sanksiya olunmamış müdaxilələrin aşkarlanması məqsədilə davamlı monitorinq aparılmalı, siyasət və prosedurlar tətbiq edilməlidir;

14.1.2. informasiya təhlükəsizliyi insidentlərinə adekvat reaksiyanın verilməsi məqsədilə aydın səlahiyyət bölgüsü və zəruri kommunikasiya kanalları müəyyən edilməlidir;

14.1.3. informasiya təhlükəsizliyi hadisələri barədə məlumatlandırma müvafiq idarəetmə kanalları vasitəsilə mümkün olduğu qədər tez bir vaxtda həyata keçirilməlidir;

14.1.4. informasiya sistemlərindən istifadə edən işçilər və kontragentlərdən müvafiq informasiya sistemlərində aşkar edilən və ya şübhələnilən zəifliklərin qeydiyyatının aparılması və onlar barədə məlumatın verilməsi tələb edilməlidir;

14.1.5. informasiya təhlükəsizliyi hadisələri qiymətləndirilməli və hadisənin informasiya təhlükəsizliyi insidenti olub-olmaması haqqında qərar qəbul edilməlidir;

14.1.6. informasiya təhlükəsizliyi insidentləri ilə bağlı tədbirlər müvafiq prosedur qaydalara əsasən həyata keçirilməlidir. Bu prosedur qaydalar tərtib olunarkən aşağıdakı tələblər nəzərə alınmalıdır:

14.1.6.1. insident baş verdiyi andan dəlillərin yığılması təmin olunmalıdır;

14.1.6.2. insidentin qeydiyyatı aparılmalı və kommunikasiyası təmin edilməlidir;

14.1.6.3. insidentin risk əsaslı qiymətləndirilməsi və prioritetləşdirilməsi həyata keçirilməlidir;

14.1.6.4. insidentlərin prioritetləşdirilməsi məqsədilə ən azı aşağıdakı kimi kateqoriyalaşdırılması aparılmalıdır:

14.1.6.4.1. aşağı - insident nəticəsində bank bir biznes proses üzrə fəaliyyəti qeyri-effektiv şəkildə həyata keçirməyə davam edir;

14.1.6.4.2. orta - insident nəticəsində bank bir neçə biznes proses üzrə fəaliyyəti həyata keçirə bilmir;

14.1.6.4.3. yüksək - insident nəticəsində bank heç bir biznes proses üzrə fəaliyyəti həyata keçirə bilmir.

14.1.6.5. insidentin aradan qaldırılması məqsədilə görüləcək tədbirlərin siyahısı formalaşdırılmalı və icrasına nəzarət həyata keçirilməlidir;

14.1.6.6. insident aradan qaldırıldıqdan sonra insident bağlanılmalı və hesabatlığı aparılmalıdır;

14.1.6.7. insidentlər barədə xəbərvermə vasitələri (elektron poçt, xüsusi təyinatlı informasiya sistemi, telefon zəngi və sair) təyin edilməli, qeydiyyata alınmalı və prosedurlaşdırılmalıdır.

14.2. İnformasiya təhlükəsizliyi üzrə baş vermiş yüksək kateqoriyalı insidentlər barədə məlumatlar bu Qaydaya Əlavə 1-də göstərilmiş formada 5 (beş) iş günü ərzində bankın İdarə Heyətinin sədri tərəfindən gücləndirilmiş elektron imza ilə təsdiqlənərək Mərkəzi Banka xüsusi təyinatlı informasiya mübadilə sistemi vasitəsilə təqdim edilməlidir.

14.3. İnsidentlərinin analizi və həll edilməsi nəticəsində formalaşmış təcrübə insidentlərin gələcəkdə baş vermə ehtimalının və təsirinin azaldırılması məqsədilə istifadə edilməlidir.

15. Fəaliyyətin fasiləsizliyinin idarə edilməsində informasiya təhlükəsizliyi

15.1. Hər bir bankda informasiya sistemlərinin və informasiya texnologiyalarının zədələndiyi, dağıldığı və ya təhlükəyə məruz qaldığı hallarda informasiya təhlükəsizliyinin davamlılığı təmin edilməlidir.

15.2. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyinin davamlılığını təmin etmək üçün bank tərəfindən aşağıdakı tədbirlər həyata keçirilir:

15.2.1. fövqəladə hallar zamanı informasiya təhlükəsizliyinin davamlılığının lazımi səviyyəsini təmin etmək məqsədilə proseslər, prosedurlar və idarəetmə üsulları təyin edilməli, sənədləşdirilməli, tətbiq edilməli və aktuallığı təmin edilməlidir;

15.2.2. informasiya sistemlərinin ehtiyat nüsxələrinin saxlanılması və fəaliyyətin bərpası üçün bankın olduğu yerdən kənarda ehtiyat mərkəzi olmalı və adekvat fəaliyyəti təmin edilməlidir;

15.2.3. fövqəladə hallarda fəaliyyətin davamlılığı planı və informasiya sistemləri üzrə bərpa planı hazırlanmalı və təsdiq olunmalıdır. Fəaliyyətin davamlılığı planında fövqəladə hallar zamanı kommunikasiya tədbirləri müəyyənləşdirilməli, biznes təsir analizi aparılmalı, bankda fəaliyyətin bərpası, ehtiyat mərkəzə keçid və sonrakı bərpa prosedurları müəyyən edilməlidir;

15.2.4. fövqəladə hallarda informasiya sistemlərinin etibarlı və davamlı fəaliyyətinin təmin edildiyini yoxlamaq məqsədilə ildə iki dəfədən az olmayaraq informasiya sistemlərinin fəaliyyəti ehtiyat mərkəzi üzərindən həyata keçirilməli və nəticələrinin rəsmiləşdirilməsi təmin edilməlidir;

15.2.5. fövqəladə hallarda informasiya təhlükəsizliyinin davamlılığını təmin etmək məqsədilə informasiya sistemlərində, informasiya texnologiyaları və kommunikasiya avadanlıqlarında qəza zamanı riayət olunmalı prosedurlarla bağlı bankda əlaqədar işçilər üçün ildə iki dəfədən az olmayaraq təlimlər həyata keçirilməli və nəticələri rəsmiləşdirilməlidir.

“Banklarda informasiya təhlükəsizliyinin
idarə edilməsi Qaydası”na
Əlavə 1

Yüksək kateqoriyalı insidentlər barədə məlumatlar

	İnformasiya təhlükəsizliyi insidentinin xüsusiyyətləri	**İnformasiya təhlükəsizliyi insidenti barədə məlumatlar**
	Ümumi məlumat	
1	İnsidentin adı	
2	İnsidentin təsviri	
3	İnsidentin baş verdiyi vaxt (gg.aa.iiii ss:dd:ss)	
4	İnsidentin aşkar edildiyi vaxt (gg.aa.iiii ss:dd:ss)	
5	İnsidentin müəyyən olunma yeri (bank, filial/şöbə, informasiya sistemi)	
6	İnsident haqqında məlumatın mənbəyi (istifadəçi və/ və ya əlaqədar inzibatçı)	
7	İnsidentin baş verməsində istifadə olunan metodlar (sosial mühəndislik, zərərverici proqram təminatının tətbiqi və sair)	
Məzmunu		
8	İnsident hadisəsi: - informasiya sistemində olan zəifliklərin istismarı; - informasiya sisteminə sanksiya olunmamış giriş; - xidmətdən imtina (DoS, DDoS); - zərərverici proqram təminatının yaradılması və yayılması; - maliyyə vəsaitinin sanksiya olunmamış köçürülməsi; - bankda fasiləsiz fəaliyyətə təhdid edən digər informasiya təhlükəsizliyi insidentləri.	
9	Təsirə məruz qalan aktivlər: - informasiya sisteminin texniki infrastrukturu (server, şəbəkə, təhlükəsizlik avadanlıqları və sair); - tətbiqi proqram təminatları, servislər və əməliyyat sistemləri; - bankın biznes prosesləri.	
10	Dəymiş ziyan (manatla)	
11	İnsident barədə informasiya mənbəyi	
Görülmüş tədbirlər		
12	Görülmüş tədbirlər (zəifliyin müəyyən edilməsi, bloklanması, bərpası və sair)	
13	Görülməsi planlaşdırılan tədbir(lər)	
14	Tədbir(lər)in başlama və bitmə vaxt(lar)ı (gg.aa.iiii ss:dd:ss)	
15	Tədbir(lər)ə məsul şəxs(lər) (soyadı, adı, atasının adı, vəzifəsi)	
16	Məlumatlandırılmış şəxs(lər) (soyadı, adı, atasının adı, vəzifəsi)	
17	Cəlb edilmiş mütəxəssis(lər) (soyadı, adı, atasının adı, vəzifəsi)	

İmza: _____

Tarix: _____