Azərbaycan Respublikası
Mərkəzi Bankı İdarə Heyətinin
“07” mart 2024-cü il tarixli qərarı
ilə təsdiq edilmişdir
Protokol № 11

# AZƏRBAYCAN RESPUBLİKASI MƏRKƏZİ BANKININ İNFORMASİYA VƏ KİBERTƏHLÜKƏSİZLİK DEPARTAMENTİ HAQQINDA

# Ə S A S N A M Ə

**BAKI - 2024**

## 1. ÜMUMİ MÜDDƏALAR

1.1. Azərbaycan Respublikası Mərkəzi Bankının İnformasiya və kibertəhlükəsizlik departamenti (bundan sonra – Departament) Azərbaycan Respublikası Mərkəzi Bankının (bundan sonra – Mərkəzi Bank) mərkəzi aparatının struktur bölməsidir.

1.2. Departament öz fəaliyyətində Azərbaycan Respublikasının Konstitusiyasını, "Azərbaycan Respublikasının Mərkəzi Bankı haqqında", "Dövlət sirri haqqında" Azərbaycan Respublikasının qanunlarını, Azərbaycan Respublikasının qüvvədə olan digər normativ hüquqi aktlarını, Mərkəzi Bankın normativ xarakterli aktlarını, İdarə Heyətinin qərarlarını, Mərkəzi Bank üzrə əmrləri, sərəncamları və bu Əsasnaməni rəhbər tutur.

1.3. Departament bu Əsasnamə ilə müəyyən olunmuş funksiyaların yerinə yetirilməsi prosesində Mərkəzi Bankın digər struktur bölmələri, ərazi idarələri və Azərbaycan Respublikasının müvafiq dövlət orqanları ilə fəaliyyətini əlaqələndirir.

## 2. DEPARTAMENTİN FƏALİYYƏTİNİN ƏSAS MƏQSƏDİ

Departamentin fəaliyyətinin əsas məqsədi Mərkəzi Bankda informasiya təhlükəsizliyi və kibertəhlükəsizliyin təmin edilməsi, maliyyə bazarları iştirakçılarının informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə nəzarət tədbirləri ilə əhatə edilməsi, onların kibertəhlükəsizlik sahəsində fəaliyyətlərinin əlaqələndirilməsi, informasiya təhlükəsizliyi üzrə davamlılığın təmin edilməsi, həmçinin informasiya təhlükəsizliyi üzrə risklərin vaxtında aşkarlanaraq qarşısının alınmasından ibarətdir.

## 3. DEPARTAMENTİN ƏSAS FUNKSİYALARI

Departamentin əsas funksiyaları aşağıdakılardır:

3.1. Mərkəzi Bankın informasiya və ödəniş sistemlərinin (bundan sonra – informasiya sistemlərinin) kənar müdaxilələrdən qorunması, informasiya təhlükəsizliyi tələblərinə riayət olunmasına nəzarətin həyata keçirilməsi;

3.2. informasiya sistemlərinə təsir edə biləcək kibertəhlükələrin qarşısının alınması məqsədilə zəruri kibertəhlükəsizlik infrastrukturunun yaradılması və dəstəklənməsi üzrə tədbirlərin görülməsi, daim artan və yenilənən hücum ssenarilərinin öyrənilərək mühafizə üsullarının araşdırılması;

3.3. Mərkəzi Bankda informasiya sistemlərinin yaradılması üzrə layihələrdə informasiya təhlükəsizliyi tələblərinə riayət edilməsinin nəzarətdə saxlanılması;

3.4. Mərkəzi Bankda informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin edilməsi üzrə 24/7 nəzarət sisteminin yaradılması, dəstəklənilməsi və müvafiq insidentlərin araşdırılması;

3.5. fövqəladə hallar zamanı Mərkəzi Bankda fəaliyyətin davamlılığının təmin edilməsi prosesində iştirak edilməsi;

3.6. Mərkəzi Bankda informasiya təhlükəsizliyi və kibertəhlükəsizilik tədbirlərinin təkmilləşdirilməsi üzrə beynəlxalq standartlara və qabaqcıl təcrübəyə uyğun normativ-metodoloji sənədlərin hazırlanmasında iştirak edilməsi;

3.7. Mərkəzi Bankda informasiya təhlükəsizliyi və kibertəhlükəsizlik tədbirlərinin təkmilləşdirilməsi və davamlı inkişafı işinin təşkil edilməsi;

3.8. Mərkəzi Bankda informasiya və digər əlaqəli aktivlərin inventarizasiya prosesinin effektiv aparılmasına nəzarətin həyata keçirilməsi;

3.9. Mərkəzi Bankda informasiya sistemlərinə giriş icazələrinin idarə olunması və nəzarətin həyata keçirilməsi;

3.10. Mərkəzi Bankın əməkdaşlarının informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində maarifləndirilməsi prosesinin təşkil edilməsi;

3.11. Mərkəzi Bankla təchizatçılar arasında olan münasibətlərdə informasiya təhlükəsizliyi tələblərinin müəyyən olunaraq tətbiq edilməsi və fəaliyyətə nəzarətin həyata keçirilməsi;

3.12. həssas informasiyanın kənara sızmasının qarşısının alınması üzrə kompleks tədbirlərin icra edilməsi;

3.13. informasiya təhlükəsizliyi boşluqlarının aşkarlanması məqsədi ilə mütəmadi müdaxilə sınaq testlərinin həyata keçirilməsi;

3.14. Mərkəzi Bankın nəzarət subyektlərində informasiya təhlükəsizliyinin təmin edilməsinə dair minimum tələblərin müəyyən edilməsi və onların müvafiq tələblərə uyğunluğunun yoxlanılması;

3.15. Departament üzrə büdcə layihəsinin hazırlanması və icrasının təmin edilməsi;

3.16. Departamentə aidiyyəti üzrə daxil olan müraciətlərə baxılması, məktub və sorğuların cavablandırılması;

3.17. rəhbərliyin tapşırığı ilə səlahiyyətinə aid məsələlər üzrə arayışların və materialların hazırlanması;

3.18. rəhbərliyin tapşırıqlarına uyğun olaraq Departamentin fəaliyyət istiqamətləri üzrə digər işlərin yerinə yetirilməsi.

## 4. DEPARTAMENTİN TƏŞKİLATİ STRUKTURU VƏ İDARƏ OLUNMASI

4.1. Departamentin təşkilati strukturu aşağıdakı şöbələrdən ibarətdir:

4.1.1. İnformasiya təhlükəsizliyi mühəndisliyi şöbəsi;

4.1.2. Kibertəhlükəsizlik şöbəsi;

4.1.3. Təhlükəsizlik əməliyyat mərkəzi şöbəsi;

4.1.4. İnformasiya və kibertəhlükəsizlik siyasəti və nəzarəti şöbəsi.

4.2. Departamentin fəaliyyətinə departament direktoru rəhbərlik edir. Departament direktoru işdə olmadıqda onun səlahiyyətlərini direktor müavini (olduqda) həyata keçirir, bu şərtlə ki, rəhbərlik tərəfindən direktor vəzifəsinin icrası şöbə rəislərindən birinə və ya digər şəxsə həvalə edilməsin.

4.3. Departamentin nomenklatur vəzifəli şəxsləri Mərkəzi Bankın İdarə Heyəti tərəfindən və ya İdarə Heyətinin müəyyən etdiyi qaydada vəzifəyə təyin edilir və vəzifədən azad olunurlar.

## 5. DEPARTAMENTİN İŞİNİN TƏŞKİLİ

### 5.1. İnformasiya təhlükəsizliyi mühəndisliyi şöbəsi:

5.1.1. Mərkəzi Bankda informasiya resurslarının qorunmasını, informasiyanın emalı proseslərinin mühafizəsini təşkil edir, həmçinin informasiya sistemlərinin təhlükəsizliyini təmin edir;

5.1.2. informasiya təhlükəsizliyinin effektivliyinin artırılması məqsədilə müasir texnoloji həllərin araşdırılması, yeni təhdid və hücumlara qarşı effektiv mübarizənin həyata keçirilməsi məqsədilə beynəlxalq təcrübəni öyrənir, müvafiq hesabat və təkliflər hazırlayır;

5.1.3. informasiya sistemləri üzrə texniki infrastrukturun kiberhücumlardan, kibertəhdidlərdən və hücum ssenarilərindən (daxili və xarici) qorunması məqsədilə mühafizə üsullarının tətbiqi və yenilənməsi üzrə fəaliyyətə rəhbərlik edir;

5.1.4. Mərkəzi Bankın nəzarət subyektlərində yoxlama proseslərində iştirak edir, informasiya təhlükəsizliyi və kibertəhlükəsizlik məsələlərinin texniki effektivliyinin yoxlanılması üzrə fəaliyyəti icra edir;

5.1.5. informasiya sistemlərinin dayanıqlığının yoxlanılması məqsədilə müdaxilə sınaq testləşdirilməsi prosesində iştirak edir;

5.1.6. informasiya sistemlərində, həmçinin təhlükəsizlik və mühafizə vasitələrində mövcud olan təhlükəsizlik boşluqlarının vaxtında aşkarlanması və aradan qadırılması prosesində iştirak edir;

5.1.7. informasiya təhlükəsizliyi tələblərinin pozulması hallarının və risklərinin aşkarlanması və qiymətləndirilməsi prosesini həyata keçirir;

5.1.8. informasiya təhlükəsizliyi sahəsində yaranmış insidentlərlə bağlı tədbirlər görür;

5.1.9. informasiya təhlükəsizliyi prosesinin beynəlxalq standartlara uyğunluğunun yoxlanılması üzrə aparılan audit yoxlamaları zamanı zəruri tədbirlər həyata keçirir;

5.1.10. fövqəladə hallar zamanı Mərkəzi Bankda fəaliyyətin davamlılığının təmin edilməsi üzrə zəruri tədbirlərin görülməsi prosesində iştirak edir;

5.1.11. informasiya təhlükəsizliyi tədbirlərinin effektivliyinin yoxlanılması prosesində iştirak edir;

5.1.12. Mərkəzi Bankda təsnifləşdirilmiş informasiyanın qorunmasına dair təhlükəsizlik tədbirlərini icra edir;

5.1.13. rəhbərliyin tapşırıqlarına uyğun olaraq fəaliyyət istiqamətləri üzrə digər işləri yerinə yetirir.

**5.2. Kibertəhlükəsizlik şöbəsi:**

5.2.1. informasiya sistemləri üzrə müdafiə vasitələrinin və tədbirlərinin dayanıqlığının vaxtaşırı yoxlanılması və monitorinqi prosesinin təşkilini həyata keçirir;

5.2.2. informasiya sistemləri üzrə müdaxilə sınaq yoxlamalarının aparılması məqsədilə yoxlama qrafikini resurs sahibləri ilə razılaşdıraraq hazırlayır;

5.2.3. informasiya sistemlərinin təhlükəsizliyinə dair vahid və avtomatlaşdırılmış yanaşmanı təmin etmək üçün müvafiq texnoloji proseslərin bütün həyat dövrü ərzində təhlükəsizlik tədbirləri ilə əhatə olunmasını həyata keçirir və müvafiq tədbirləri tətbiq edir;

5.2.4. informasiya sistemlərində, həmçinin təhlükəsizlik və mühafizə vasitələrində mövcud olan təhlükəsizlik boşluqlarının vaxtında aşkarlanması və aradan qadırılması prosesində iştirak edir;

5.2.5. informasiya təhlükəsizliyi tələblərinin pozulması hallarının və risklərinin aşkarlanması və qiymətləndirilməsi prosesində iştirak edir;

5.2.6. informasiya sistemlərinin istismara verilməsindən öncə sistemlərin müdaxilə sınaq yoxlamasını həyata keçirir;

5.2.7. müdaxilə sınaq yoxlamalarının aparılması üzrə fəaliyyətin koordinasiyasını həyata keçirir;

5.2.8. müdaxilə sınaq yoxlamaları çərçivəsində prosesin qeydiyyatını və vaxtında reaksiya verilmə fəaliyyətini yoxlayır;

5.2.9. müdaxilə sınaq yoxlamaları nəticələrinin aradan qaldırılmasına nəzarəti həyata keçirir;

5.2.10. informasiya sistemlərinin tətbiqi layihələrində iştirak edir və layihələrdə kibertəhlükəsizlik üzrə texniki tələbləri formalaşdırır;

5.2.11. müasir kibertəhdidlər barədə məlumatların mütəmadi olaraq əldə olunması, trendlərin izlənilməsi və “sıfır gün” hücumlarına (sistem və proqram təminatlarındakı boşluqlardan sui-istifadə) qarşı tədbirlərin kommunikasiya edilməsi prosesini icra edir;

5.2.12. informasiya təhlükəsizliyi istiqamətində intellektual, resurs və texnoloji baxımdan qabaqlayıcı rejimdə fəaliyyətin aparılmasını təmin edir;

5.2.13. informasiya sistemləri üzrə baş vermiş insidentlərin araşdırılması üzrə müvafiq tədbirlərin icrasını planlaşdırır və təmin edir;

5.2.14. rəhbərliyin tapşırıqlarına uyğun olaraq fəaliyyət istiqamətləri üzrə digər işləri yerinə yetirir.

**5.3. Təhlükəsizlik əməliyyat mərkəzi şöbəsi:**

5.3.1. informasiya sistemlərində, o cümlədən onların texniki infrastrukturunda insidentlərin identifikasiyası, aşkarlanması və cavab strategiyalarının hazırlanması fəaliyyətini icra edir;

5.3.2. insidentlərin idarə edilməsi fəaliyyətinin qabaqcıl təcrübəyə və beynəlxalq standartların tələblərinə uyğunluğunu təmin edir;

5.3.3. insidentlərin idarə edilməsi fəaliyyətinin təmin edilməsi üçün müvafiq normativ-metodoloji sənədlərin hazırlanmasında iştirak edir;

5.3.4. insidentlərin idarə edilməsi üzrə texniki informasiya sistemlərinin, alətlərin idarə edilməsi və dəstəklənməsi prosesini təşkil edir;

5.3.5. insidentlərin idarə edilməsi fəaliyyətinin təkmilləşdirilməsi məqsədilə müasir texnoloji həlləri qiymənləndirir və müvafiq həllərin tətbiqini təşkil edir;

5.3.6. insidentlərin idarə edilməsi fəaliyyətinin davamlılığını təşkil edir, o cümlədən 24/7 monitorinq fəaliyyətini təmin edir və nəzarəti həyata keçirir;

5.3.7. qeydə alınmış informasiya təhlükəsizliyi hadisələri və şübhə doğuran məsələlərin analizinin aparılması və informasiya təhlükəsizliyi insidentlərinin aşkarlanması fəaliyyətini idarə edir;

5.3.8. informasiya təhlükəsizliyi insidentlərinə cavab strategiyasını və cavab tədbirlərinin icra ssenarilərini formalaşdırır və işləkliyini təmin edir;

5.3.9. insidentlər üzrə “doğru bilinən yanlışlar”ın analizini həyata keçirir və insidentlərin kateqoriyalarının təyini prosesini icra edir;

5.3.10. baş vermiş insidentlər barədə rəhbərliyin, həmçinin əlaqədar tərəflərin məlumatlandırılması, müvafiq hesabatların hazırlanması, təqdim edilməsi və insidentlərin qarşısının alınması üzrə fəaliyyətin koordinasiyasını təmin edir;

5.3.11. informasiya təhlükəsizliyi hadisələrinin idarə edilməsi prosesinin təşkil olunması üzrə loq mənbələrinin təhlükəsizlik məlumatı və hadisələrin idarə edilməsi sisteminə (SİEM) qoşulması işini təşkil edir, loqların qəbul edilməsi prosesinin mövcud normativ sənədlərin tələblərinə uyğunlaşdırılmasını təmin edir;

5.3.12. insident nəticələrinin aradan qaldırılması və bərpası prosesində iştirak edir, insidentlərin baş verdiyi andan bərpası dövrünədək öyrənilmiş təcrübəni özündə ehtiva edən bilik bazasının formalaşdırılmasını təmin edir;

5.3.13. ölkədə fəaliyyət göstərən kompüter insidentlərinə qarşı mübarizə mərkəzləri (CERT) ilə əməkdaşlıq edir və ölkə üzrə mövcud aktiv kiberhücumlar barədə informasiyanın əldə edilməsini təmin edir;

5.3.14. informasiya sistemlərinin tətbiqi layihələrində iştirak edir, o cümlədən loqların idarə edilməsi və monitorinqi üzrə texniki tələbləri formalaşdırır;

5.3.15. yeni insidentlər barədə daimi məlumatların əldə olunması, trendlərin izlənilməsi və mövcud təhlükəsizlik boşluqları barədə məlumatlandırma prosesini icra edir;

5.3.16. insident idarəetməsi üzrə qabaqcıl təcrübəni öyrənir və təklif verir;

5.3.17. kənar təchizatçılarla fəaliyyət zamanı insidentlərin idarə edilməsi üzrə nəzarəti və monitorinqi həyata keçirir;

5.3.18. Mərkəzi Bankın əməkdaşlarının insidentlərin idarə edilməsi sahəsində maarifləndirilməsini təşkil edir;

5.3.19. Təhlükəsizlik Əməliyyat Mərkəzinin fəaliyyəti və aşkar edilmiş insidentlər barədə rəhbərliyin mütəmadi olaraq məlumatlandırılmasını təmin edir;

5.3.20. müdaxilə sınaq yoxlamları zamanı fəaliyyətin qeydiyyatını aparır və proses üzrə vaxtında reaksiya verilməni həyata keçirir;

5.3.21. rəhbərliyin tapşırıqlarına uyğun olaraq fəaliyyət istiqamətləri üzrə digər işləri yerinə yetirir.

### 5.4. İnformasiya və kibertəhlükəsizlik siyasəti və nəzarəti şöbəsi:

5.4.1. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsi üzrə baş verən yenilikləri daim izləyir, bu yeniliklərin Mərkəzi Bankda tətbiqi imkanlarını müəyyən edir və müvafiq təklifləri formalaşdırır;

5.4.2. informasiya təhlükəsizliyi və kibertəhlükəsizliyin inkişafı strategiyasını hazırlayır və icrasını təşkil edir;

5.4.3. Mərkəzi Bankda informasiya təhlükəsizliyi tədbirlərinin qabaqcıl təcrübəyə və beynəlxalq standartlara uyğunlaşdırılması üzrə daxili reqlament sənədlərinin hazırlanması və təkmilləşdirilməsi işini təşkil edir;

5.4.4. informasiya təhlükəsizliyi idarəetmə sistemi (İTİS) üzrə nəzarəti həyata keçirir və sistemin beynəlxalq standartların tələblərinə uyğun təkmilləşdirilməsini təmin edir;

5.4.5. informasiya sistemlərində həyata keçirilən dəyişikliklərin informasiya təhlükəsizliyi tələblərinə uyğunluğunun qiymətləndirilməsini və icrasına müvafiq nəzarəti həyata keçirir;

5.4.6. Mərkəzi Bankın nəzarət subyektlərində informasiya təhlükəsizliyinin təmin edilməsinə dair minimum tələbləri müvafiq struktur bölmələrlə birgə formalaşdırır;

5.4.7. Mərkəzi Bankın nəzarət subyektlərində həyata keçirilən yoxlama prosesində iştirak edir, informasiya təhlükəsizliyi və kibertəhlükəsizlik məsələlərinin hüquqi aktların tələbləri çərçivəsində idarə edilməsinin effektivliyinin yoxlanılması üzrə fəaliyyəti icra edir;

5.4.8. əməliyyat risklərinin qiymətləndirilməsi prosesi çərçivəsində informasiya təhlükəsizliyi risklərini qiymətləndirir və cavab tədbirlərini formalaşdırır;

5.4.9. informasiya sistemlərinin illik yoxlama planlarını resurs sahibləri ilə razılaşdıraraq hazırlayır və məsul şəxsləri təyin edir;

5.4.10. biznes proseslərin fəaliyyətinə mənfi təsir edəcək insident ssenarilərinin formalaşdırılması məqsədi ilə aidiyyəti struktur bölmələrlə müzakirələr aparır;

5.4.11. Mərkəzi Bankda informasiya və digər əlaqəli aktivlərin inventarizasiya prosesinin effektiv aparılmasına nəzarəti həyata keçirir;

5.4.12. Mərkəzi Bankda informasiya sistemlərinə giriş icazələrinin idarə olunması və nəzarətin həyata keçirilməsi fəaliyyətini təmin edir;

5.4.13. həssas informasiyanın icazəsiz kənara sızmasının qarşısının alınması üzrə kompleks tədbirlərin icrasında iştirak edir;

5.4.14. struktur bölmələrin mövcud biznes proseslərinin müasir texnoloji inkişaf nəzərə alınmaqla təkmilləşdirilməsi yollarını araşdırır;

5.4.15. beynəlxalq standartlara uyğun olaraq informasiya təhlükəsizliyi vasitələrinin yenilənməsini və inkişaf etdirilməsini təşkil edir;

5.4.16. informasiya təhlükəsizliyi üzrə sistem və alətlərin əldə edilməsi ilə bağlı aidiyyəti struktur bölmələrlə birlikdə texniki şərtlərin hazırlanması işini təmin edir;

5.4.17. informasiya təhlükəsizliyi sistemlərinin tətbiqi proseslərini planlaşdırır və layihələri Mərkəzi Bankın korporativ layihə idarəetmə konsepsiyasına uyğun olaraq həyata keçirir;

5.4.18. informasiya təhlükəsizliyi prosesinin beynəlxalq standartlara uyğunluğunun yoxlanılması üzrə aparılan audit yoxlamaları (daxili və kənar) zamanı zəruri tədbirlər həyata keçirir;

5.4.19. Mərkəzi Bank əməkdaşlarının informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsi üzrə bilik və bacarıqlarının artırılması məqsədilə İnsan resursları departamenti ilə birlikdə bankdaxili təlimlərin keçirilməsini təmin edir;

5.4.20. avtomatlaşdırılmış idarəetmə sistemlərinin yaradılması üzrə layihələrin bütün həyat tsikli üzrə informasiya təhlükəsizliyi tədbirlərinin nəzərə alınmasına və informasiya təhlükəsizliyi tələblərinə riayət olunmasına nəzarət edir;

5.4.21. kənar təchizatçılarla fəaliyyət zamanı informasiya təhlükəsizliyi və kibertəhlükəsizlik məsələlərinə nəzarəti həyata keçirir;

5.4.22. Mərkəzi Bankda informasiya və kibertəhlükəsizliyinin təmin olunması sahəsində bankdaxili hazırlıq və maarifləndirmə prosesində iştirak edir;

5.4.23. informasiya təhlükəsizliyi tələblərinin pozulması hallarının və risklərinin aşkarlanması və qiymətləndirilməsi prosesində iştirak edir;

5.4.24. Departament tərəfindən göstərilən xidmətlər üzrə məmnunluq səviyyəsinin ölçülməsi ilə bağlı soruğuların keçirilməsini təşkil edir;

5.4.25. rəhbərliyin tapşırıqlarına uyğun olaraq fəaliyyət istiqamətləri üzrə digər işləri yerinə yetirir.

## 6. Yekun müddəalar

6.1. Bu Əsasnamə təsdiq olunduğu gündən qüvvəyə minir.

6.2. Bu Əsasnamə qüvvəyə mindiyi gündən Mərkəzi Bankın İdarə Heyətinin 07 sentyabr 2022-ci il tarixli qərarı (protokol № 38) ilə təsdiq edilmiş “Azərbaycan Respublikası Mərkəzi Bankının İnformasiya və kibertəhlükəsizlik şöbəsi haqqında Əsasnamə” ləğv edilir.

**Mərkəzi Bankın sədri** **Taleh Kazımov**