AZƏRBAYCAN RESPUBLİKASININ
MƏRKƏZİ BANKI

Maliyyə bazarları üzrə kibertəhlükəsizlik strategiyası

2023 - 2026

Mündəricat

1. Qısa xülasə

Müasir dövrün çağırışları hesab olunan innovativ həllərə əsaslanan rəqəmsal maliyyə xidmətləri fəaliyyətin effektivliyini və səmərəliliyini artırmaqla yanaşı maliyyə ekosistemini kiberhücumlara qarşı daha həssas etməkdədir. Bununla qlobal maliyyə sistemləri kibercinayətkarların başlıca hədəflərinə çevrilmiş, nəticədə kiberhücumların tezliyi artmış və hücum ssenariləri mürəkkəbləşmişdir. Bu istiqamətdə baş verən kiber trendlər öz növbəsində, kiber risklərin düzgün idarə edilməsini və adekvat tənzimləmə çərçivəsinin tətbiq edilməsini zəruri edir. Bu səbəbdən, maliyyə bazarlarına nəzarət orqanları maliyyə sistemində kiberdayanıqlığı davamlı olaraq təkmilləşdirir və onunla bağlı tədbirləri hər bir təşəbbüsün tərkib hissəsinə çevirir.

2023-2026-cı illər üçün “Maliyyə bazarları üzrə kibertəhlükəsizlik Strategiyası”nın (Strategiya) başlıca məqsədi Azərbaycan Respublikasının Mərkəzi Bankı (AMB) və ölkədə fəaliyyət göstərən maliyyə institutlarında informasiya təhlükəsizliyinin və kibertəhlükəsizliyin gücləndirilməsi, o cümlədən müasir dövrün kibertəhlükəsizlik təhdidlərinin və kiberhücumların qarşısının daha effektiv alınması üzrə əsas fəaliyyət istiqamətlərinin müəyyən edilməsidir. Strategiyaya daxil edilmiş təşəbbüslər və icrası nəzərdə tutulmuş tədbirlər AMB-nin və ümumilikdə maliyyə bazarlarının mümkün kibertəhlükəsizlik insidentlərinə və fövqəladə hallara hazırlıq səviyyəsinin yüksəldilməsinə, həmçinin maraqlı tərəfləri vaxtında məlumatlandıraraq kibertəhlükəsizlik təşəbbüsləri ilə bağlı qərarların qəbul edilməsi proseslərinin daha effektiv təşkil edilməsinə yönəlmişdir.

Strategiyanın vizyonu **“maliyyə sabitliyinin təmin edilməsi üçün artan kibertəhdidlər fonunda ölkənin maliyyə bazarlarında kiber dayanıqlığın gücləndirilməsidir”**. Bu Strategiya ölkədə informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə dövlət siyasətinin tərkib hissəsi olaraq, bu sahədə fəaliyyətin əsas məqsədlərini, prinsiplərini, istiqamətlərini və prioritet vəzifələrini müəyyən edir. Strategiyanın əsas missiyası **kibertəhlükəsizlik sahəsində etibarlı təhlükəsizlik infrastrukturu, təkmil bilik və bacarıqlara malik olan insan kapitalı, kibertəhdidlər barədə məlumatların qarşılıqlı kommunikasiyası həyata keçirilən effektiv əməkdaşlıq münasibətləri, habelə adekvat tənzimləmə çərçivəsi ilə əhatə olunmuş maliyyə sisteminin formalaşdırılması və onun kiber dayanıqlığının təmin edilməsidir.**

Strategiya formalaşdırılarkən maliyyə sektorunun cari kibertəhlükəsizlik vəziyyəti Beynəlxalq Maliyyə Korporasiyası ilə birgə əməkdaşlıq çərçivəsində Standartlar və Texnologiyalar Milli İnstitutunun (NIST) müvafiq standartları əsasında hazırlanmış özünüqiymətləndirmə çərçivəsinə uyğun olaraq qiymətləndirilmiş, habelə bençmark ölkələrdə tətbiq edilən kibertəhlükəsizlik strategiyaları və yanaşmaları təhlil edilmişdir.

Strategiyanın başlıca hədəfləri: **1)** ölkənin maliyyə bazarlarında kibertəhlükəsizlik ekosisteminin formalaşdırılması, o cümlədən kibertəhdidlərə adekvat reaksiyanın verilməsi və kibertəhlükəsizlik səviyyəsinin yüksəldilməsi; **2)** kibergigiyena tədbirlərinə, həmçinin qarşılıqlı tərəfdaşlıq çərçivəsində davamlı məlumat mübadiləsinə üstünlük verərək maliyyə sisteminin dayanıqlığının yüksəldilməsi; **3)** AMB-nin mandatı çərçivəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik ilə bağlı normativ-metodoloji bazanın formalaşdırılması, davamlı aktuallaşdırılması və bununla da ölkənin maliyyə bazarlarında maliyyə sabitliyinin təmin edilməsidir.

2. Ölkənin maliyyə sisteminin kibertəhlükəsizlik vəziyyəti

Son zamanlar ölkənin milli kibertəhlükəsizlik ekosisteminin gücləndirilməsi və beynəlxalq trendlər nəzərə alınmaqla inkişaf etdirilməsi istiqamətində aidiyyəti dövlət qurumları və assosiasiyaları tərəfindən həyata keçirilən kompleks tədbirlər nəticəsində ölkəmizin kibertəhlükəsizlik üzrə beynəlxalq reytinqlərdə mövqeyi yüksəlməkdədir. Belə ki, 2023-cü il üzrə Milli Kibertəhlükəsizlik İndeksinə əsasən Azərbaycan reytinqdə 33 pillə irəliləyərək Qazaxıstan, Belarus, Özbəkistan, Ermənistan kimi ölkələri qabaqlamış və reytinqdə 53-cü yerdə qərarlaşmışdır[1]. Bu inkişaf tempinin qorunub saxlanması, o cümlədən ölkəmizin milli kibertəhlükəsizilik ekosisteminin tərkib hissəsi olan maliyyə sisteminin kiber dayanıqlığının qorunub saxlanması mühüm prioritetlərdən birinə çevrilmişdir. Bu prioritetin icrası ölkənin maliyyə sisteminin kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsini zəruri edir.

Strategiyanın bu bölməsində tətbiq edilən özünüqiymətləndirmə metodologiyası, daha sonra isə müxtəlif maliyyə institutları arasında aparılan kibertəhlükəsizlik sorğusunun nəticələri şərh edilir.

[1] https://ncsi.ega.ee/ncsi-index/?order=rank

2.1. Maliyyə institutları üzrə qiymətləndirmə çərçivəsi

Maliyyə bazarlarında kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi məqsədilə maliyyə institutları üzrə sorğular keçirilmişdir. Aparılmış sorğularda 51 respondent olan maliyyə institutları, o cümlədən banklar, sığorta şirkətləri və maliyyə bazarlarının digər iştirakçıları iştirak etmişlər:

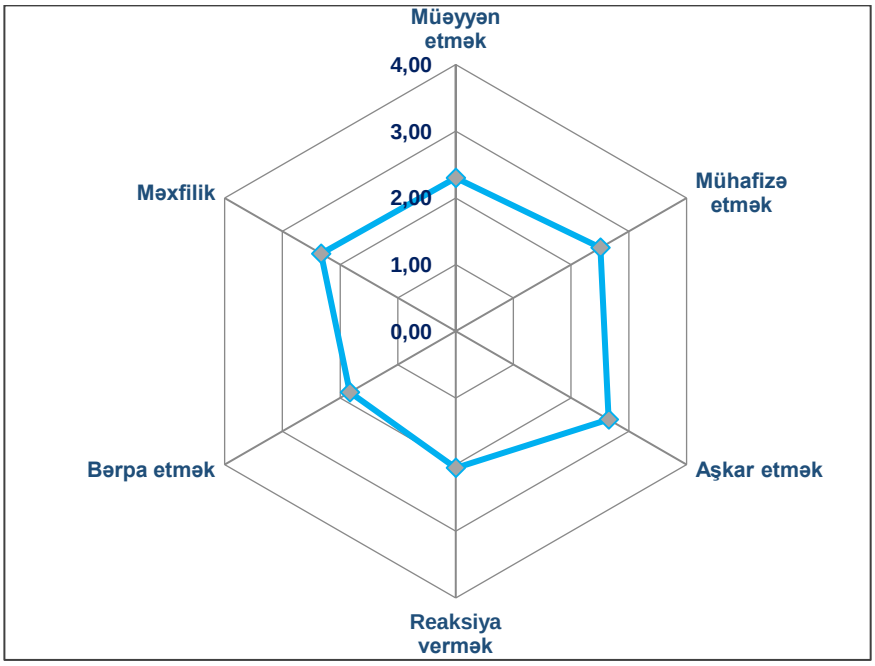
- Bankların sayı: 22
- BOKT-ların sayı: 15
- Sığorta şirkətlərinin sayı: 10
- Kart prosessinq mərkəzləri: 2
- Digər (Milli Depozit Mərkəzi, İcbari Sığorta Bürosu): 2

Keçirilmiş sorğular NIST standartının kiberəthlükəsizlik çərçivəsinə əsasən hazırlanmış, 6 kateqoriyaya və 52 suala bölünmüşdür. Sorğular zamanı maliyyə institutlarında informasiya aktivlərinin müəyyən edilməsi və mühafizəsi, təhlükəsizlik hadisələrinin aşkar edilməsi, onlara adekvat cavab reaksiyasının verilməsi və aradan qaldırılması, həmçinin məlumatların məxfiliyi üzrə məsələlər təhlil edilmişdir.

2.2. Maliyyə institutlarının kibertəhlükəsizlik səviyyəsi

Maliyyə institutları üzrə keçirilmiş sorğular nəticəsində müəyyən edilmişdir ki, “təhlükəsizlik hadisələrinə reaksiya verilməsi” və “fəaliyyətin bərpa edilməsi” üzrə göstəricilər ölkənin maliyyə sektorunun kibertəhlükəsizlik üzrə orta göstəricisindən aşağıdır (Cədvəl 1). Bu xüsusda, Strategiyanın əsas hədəflərindən biri də qabaqcıl təcrübələri mərhələli şəkildə tətbiq etməklə bu göstəricilərin yüksəldilməsidir.

Şəkil 1: Ölkənin maliyyə bazarlarında kibertəhlükəsizlik vəziyyəti



Mənbə: Kibertəhlükəsizlik üzrə sorğunun nəticələri

Cədvəl 1-də göründüyü kimi, bank sektoru və ödəniş bazarı iştirakçılarının kibertəhlükəsizlik üzrə vəziyyəti sorğuda iştirak edən sığorta şirkətləri ilə müqayisədə daha qənaətbəxşdir. "Təhlükəsizlik hadisələrinin aşkar edilməsi" indikatoruna əsasən bank sektoru və ödəniş bazarı iştirakçılarının kibertəhlükəsizlik üzrə yetkinlik səviyyəsi 2.4-dən yüksəkdir. Maliyyə sektorunun kibertəhlükəsizlik üzrə orta göstəricisi hər üç seqment üzrə 2.28 təşkil etdiyi halda, bank sektoru üzrə göstərici 2.14, sığorta təşkilatları üzrə 1.85, ödəniş bazarları üzrə isə 2.85 təşkil etmişdir. Odur ki, maliyə bazarlarının hər üç seqmenti üzrə iştirakçıları kibertəhlükəsizliyin gücləndirilməsi istiqamətində tədbirləri intensivləşdirməli və bu sahəni xüsusi diqqət mərkəzində saxlamalıdır.

Cədvəl 1: Maliyyə institutları üzrə kibertəhlükəsizlik vəziyyəti[2]

İndikatorlar	Bank sektoru	Sığorta sektoru	Ödəniş bazarı	Orta göstərici
İnformasiya aktivlərinin müəyyən edilməsi	2.15	1.9	2.85	**2.3**
İnformasiya aktivlərinin mühafizə edilməsi	2.2	2.1	3.25	**2.51**
Təhlükəsizlik hadisələrinin aşkar edilməsi	2.4	2.2	3.35	**2.65**

[2] *"Bank sektoru" üzrə banklar və BOKT-lər, "Sığorta sektoru" üzrə İSB və sığorta şirkətləri, "Ödəniş bazarı" üzrə kart prosessinq mərkəzləri qiymətləndirmədə iştirak etmişlər.*

Təhlükəsizlik hadisələrinə reaksiya verilməsi	1.8	1.2	3.15	**2.05**
Fəaliyyətin bərpa edilməsi	1.9	1.5	2.1	**1.83**
Məlumatların məxfiliyi	2.4	2.2	2.4	**2.33**
Orta göstərici	**2.14**	**1.85**	**2.85**	**2.28**

Mənbə: Kibertəhlükəsizlik üzrə sorğu nəticələri

2.3. Mərkəzi Bankda informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət

"Azərbyacan Respublikasının Mərkəzi Bankı haqqında" Qanunun 48-ci maddəsinə əsasən AMB maliyyə bazarları nəzarət subyektləri üzərində tənzimləmə və nəzarət funksiyasını həyata keçirməkdədir. Bu xüsusda, AMB tərəfindən nəzarət subyektlərində hərtərəfli və tematik yoxlamalar həyata keçirilir və bu zaman onlarda informasiya təhlükəsizliyinin, o cümlədən fərdi məlumatların qorunması üzrə məsələlərin qiymətləndirilməsi diqqət mərkəzində saxlanılır. Belə ki, Azərbaycan Respublikasının Nazirlər Kabinetinin 6 sentyabr 2010-cu il tarixli 161 nömrəli Qərarına əsasən maliyyə bazarları sahəsində fərdi məlumatların informasiya mühafizəsinə dair tələblərin icrasına nəzarət səlahiyyəti maliyyə bazarlarına nəzarət orqanına həvalə edilmişdir.

Maliyyə bazarlarında informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin edilməsi müvafiq hüquqi tənzimləmə çərçivəsinin, o cümlədən AMB-nin sözügedən sahə üzrə fəaliyyətin təşkili və maliyyə bazarları iştirakçıları üçün tənzimləyici tələblərin müəyyən edilməsi səlahiyyətlərinin formalaşdırılmasını tələb edir. Belə ki, mövcud qanunvericiliyə, o cümlədən "Banklar haqqında" Azərbaycan Respublikası Qanununun 38.3-cü maddəsinə əsasən AMB bankların istifadə etdikləri avtomatlaşdırılmış hesablaşma və pul köçürmələri sistemlərinin etibarlığının və təhlükəsizliyinin, bank informasiyasının mühafizəsinin onlar tərəfindən təmin edilməsinə aid minimum tələbləri müəyyən edir. Bu xüsusda, AMB müvafiq dövrlərdə informasiya təhlükəsizliyinə dair minimum tələbləri özündə ehtiva edən normativ-hüquqi bazanı formalaşdırmış və davamlı olaraq aktuallaşdırmışdır.

Belə ki, AMB-nin İdarə Heyətinin 14 iyul 2021-ci il tarixli, 20/1 nömrəli qərarına əsasən "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası" təsdiq edilmiş və 2022-ci il 1 aprel tarixindən qüvvəyə minmişdir[3]. Qayda ISO/IEC 2700X standartlarının tələblərinə

[3] https://e-qanun.az/framework/48025

uyğun olaraq banklarda “İnformasiya təhlükəsizliyinin idarə edilməsi sistemi”nin formalaşdırılması və təşkili, insan resurslarının təhlükəsizliyi, aktivlərin idarə olunması, girişlərə nəzarət, kriptoqrafiya, fiziki və perimetr üzrə təhlükəsizlik, informasiya mübadiləsinin təhlükəsizliyi, informasiya sistemlərinin əldə edilməsi, tətbiqi və dəstəklənməsi zamanı təhlükəsizliyin təmin olunması, kənar təchizatçılarla xidməti münasibətlərdə informasiya təhlükəsizliyinin qorunması, informasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə nəzarət mexanizmlərini və tələbləri ehtiva edir.

Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik səviyyəsinin gücləndirilməsi ilə yanaşı AMB qanunvericiliklə müəyyən olunan mandat və funksiyalarını dəstəkləyən ödəniş və informasiya sistemlərinin də təhlükəsiz, etibarlı və davamlı fəaliyyətinin təmin olunması istiqamətində kompleks tədbirlər həyata keçirir. Bu tədbirlər həm təşkilat daxilində “İnformasiya təhlükəsizliyinin idarə edilməsi sistemi”nin formalaşdırılması, həmçinin də zəruri texnoloji infrastrukturun qurulması və modernizasiyası üzrə fəaliyyətləri özündə ehtiva edir. Xüsusilə AMB-də:

- “İnformasiya təhlükəsizliyinin idarə edilməsi sistemi”nin davamlı aktuallaşan siyasətlərdən, prosedurlardan və fəaliyyətlərdən ibarət olması;
- İnformasiya təhlükəsizliyi siyasətinin müvafiq informasiya risklərini və nəzarət sahələrini əhatə etməsi;
- İnformasiya təhlükəsizliyi ilə bağlı aşağıda qeyd edilən məqsədlər üzrə öhdəliklərin və səlahiyyətlərin müəyyən edilməsi:
  - işçilər və qarşı tərəflərin (kontragentlər) fəaliyyətə başlamazdan əvvəl informasiya təhlükəsizliyi öhdəliklərini qəbul etməsi;
  - məsafədən iş və mobil cihazlardan istifadə zamanı informasiya təhlükəsizliyi tələblərinə riayət etməsi;
  - informasiya təhlükəsizliyi sahəsində maarifləndirmə prosesinin təşkili ilə bağlı öhdəliklərin müəyyən edilməsi.
- İnformasiya sistemlərində saxlanılan məlumatların icazəsiz açıqlanmasının, dəyişdirilməsinin, məhv edilməsinin və ya zədələnməsinin qarşısının alınması üçün tədbirlərin görülməsi;

- İnformasiya və məlumatlara çıxış imkanlarının məhdudlaşdırılması üzrə müvafiq tədbirlərin təmin edilməsi;
- İnformasiya sistemlərinə və proqram təminatlarına icazəsiz girişin məhdudlaşdırılması üzrə tədbirlərin təmin olunması;
- İnformasiyanın məxfiliyinin və tamlığının qorunması məqsədilə kriptoqrafik vasitələrin düzgün seçilməsi və istifadəsi üzrə tədbirlərin həyata keçirilməsi;
- Təşkilatdaxili və xarici perimetr üzrə fiziki təhlükəsizlik tədbirlərinin təmin edilməsi;
- İnformasiya emalı vasitələrinin düzgün və təhlükəsiz istismarı üçün tədbirlərin görülməsi, xüsusən:
  - dəyişikliklərin idarə edilməsi prosedurlarının tətbiq edilməsi;
  - zərərli proqramlardan və kodlardan mühafizənin təmin edilməsi;
  - xarici yaddaş qurğularına münasibətdə təhlükəsizlik tədbirlərinin görülməsi;
  - informasiya sistemlərinin ehtiyat nüsxələrinin yaradılması və bərpası;
  - informasiya sistemlərində hadisələrin və insidentlərin qeydiyyatının aparılması və prosesin idarə edilməsi;
  - informasiya sistemlərində zəifliklərin aşkarlanması, qarşısının alınması və sair.
- İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin qoruması məqsədilə şəbəkə infrastrukturunun idarə edilməsi və monitorinqinin aparılması;
- Təşkilat daxilində informasiyanın transferi zamanı təhlükəsizlik tədbirlərinin tətbiq edilməsi;
- İnformasiya təhlükəsizliyi və kibertəhlükəsizlik tədbirlərinin informasiya sistemlərinin istifadə müddəti ərzində həyat dövrü boyunca əhatə olunması;
- İnformasiya təhlükəsizliyi insidentlərinin davamlı və effektiv idarə olunması, o cümlədən informasiya təhlükəsizliyi insidentlərinin və zəifliklərinin kommunikasiyası üzrə tədbirlərin həyata keçirilməsi, xüsusilə:
  - informasiya sistemlərinin zədələnməsi, məhv edilməsi və ya informasiya sistemlərinə kiberhücum təhlükəsi zamanı informasiya təhlükəsizliyinin davamlılığının təmin edilməsi;

- informasiya sistemlərində məlumat itkisinin qarşısının alınması və bu məqsədlə müvafiq nəzarət sistemlərinin tətbiq edilməsi;
- informasiya sistemlərində mövcud olan boşluqların aşkar edilməsi üzrə prosedurların mövcud olması və müvafiq fəaliyyətin davamlı olaraq aparılması;
- informasiya sistemlərində konfiqurasiyaların idarə edilməsi prosedurunun mövcud olması və müvafiq fəaliyyətin davamlı olaraq aparılması;
- insidentlərə cavab reaksiyalarının daxili və xarici maraqlı tərəflərlə effektiv kordinasiyasının aparılması;
- informasiya təhlükəsizliyi üzrə maarifləndirmə tədbirlərinin həyata keçirilməsi;
- kiberhücuma hazırlıq və kiber çalışmalar üzrə fəaliyyətin həyata keçirilməsi.

3. Maliyyə sistemi üzrə dünyada kibertəhlükəsizlik trendləri və başlıca çağırışlar

Son zamanlar qlobal maliyyə sistemləri kibercinayətkarların başlıca hədəflərinə çevrilmiş, nəticədə kiberhücumların tezliyi artmış, tətbiq ssenariləri mürəkkəbləşmiş, xüsusilə də hücuma məruz qalan tərəflər üçün daha "bahalı" olmuşdur. Aparılmış araşdırmalara əsasən Amerika Birləşmiş Ştatlarında (ABŞ) 2022-ci ildə kiberhücumlar nəticəsində məlumat sızıntısı üzrə zərərin orta dəyəri 9.44 mln. ABŞ dolları həcmində olmuşdur[4]. Bu təhdidlərlə mübarizə aparmaq üçün maliyyə institutları real vaxt rejimində kibertəhdidləri aşkar etməyə və onlara cavab verməyə imkan verən yeni nəsil təhlükəsizlik həlləri tətbiq etməkdədirlər. Maliyyə sistemində ən çox təsadüf olunan kiberhücum trendləri aşağıda göstərilmişdir:

Maliyyə sektoruna təsir edən ən çox yayılmış kiberhücum növlərindən biri "fişinq"dir. Fişinq hücumları adətən istifadəçilərin giriş məlumatlarının və ya fərdi məlumat kimi həssas məlumatların əldə edilməsi yolu ilə saxta e-poçt və ya internet səhifələrdən istifadəni əhatə edir. 2022-ci ilin 2-ci rübündə qeydiyyata alınmış fişinq hücumlarının ən böyük payı (27.6%) məhz maliyyə institutlarının üzərinə düşür[5]. Kibercinayətkarlar sosial mühəndislik metodlarından istifadə edərək insanları fərdi və maliyyə məlumatlarını təqdim

[4] *IBM Cost of a Data Breach Report (https://www.ibm.com/security/data-breach)*
[5] *Phishing Activity Trends Report, 2Q 2022 (https://apwg.org/trendsreports/)*

etməyə inandıra bilirlər. Bu təhdidlərə qarşı mübarizə aparmaq üçün maliyyə institutları fişinq hücumlarını tanımaq (ayırd etmək) məqsədilə aktiv kommunikasiya tədbirlərini həyata keçirir, çoxfaktorlu autentifikasiya və digər texniki nəzarət alətlərini tətbiq edirlər.

Maliyyə sektoru üçün daha bir artan təhlükə "ransomware" (ransom) zərərverici proqram təminatlarıdır. PwC tərəfindən aparılan təhlillərə əsasən ransom zərərverici proqram təminatından istifadə edilməklə həyata keçirilən kiberhücumlar 2021-ci ildə əksər təşkilatların üzləşdiyi ən əhəmiyyətli kiber təhlükə olmuşdur[6]. Belə ki, həmin ildə maliyyə sistemi iştirakçılarının 55%-i hədəfə alınmış və maliyyə xidmətlərinə edilmiş ransom kiberhücumları nəticəsində məlumat sızması iki dəfə artmışdır[7]. Ransom hücumlarından qorunmaq üçün təşkilatlar bir sıra təhlükəsizlik tədbirlərini həyata keçirməlidirlər. Buraya əsasən sosial mühəndislik kiberhücumları barədə maarifləndirmə tədbirlərinin həyata keçirilməsi, çoxfaktorlu autentifikasiya həllərinin tətbiqi və məlumatların müntəzəm əsasda ehtiyat nüsxələrinin yaradılması prosedurları daxildir.

Daxili kibertəhdidlər də maliyyə sektoru üçün ciddi narahatlıq doğurur. Daxili kibertəhdidlər həssas məlumatları oğurlamaq və ya əməliyyatların həyata keçirilməsi prosesini pozmaq məqsədilə təşkilatın əməkdaşları və ya kontragentlər tərəfindən imtiyazlı girişlərin ələ keçirilməsi yolu ilə aparılır. Xarici kibertəhlükəsizlik təhdidlərinin qarşısını almaq və ya ilk növbədə texniki alətlər vasitəsilə aşkar etmək mümkün olsa da, bir çox hallarda həmin alətlər daxili təhdidlərin qarşısını almaq üçün yetərli deyildir. Bu xüsusda, daxili təhdidlərdən qorunmaq məqsədilə təkmil siyasət və prosedurların, aktual təhlükəsizlik və texnoloji həllərin, davamlı məlumatlandırma və maarifləndirmə tədbirlərinin həyata keçirilməsi mütləqdir.

Paylanmış Xidmətdən İmtina (DDoS) hücumları maliyyə sektorunun üzləşdiyi digər təhlükədir. DDoS hücumları hədəflənmiş informasiya sisteminin şəbəkə-trafik kanallarını yükləyərək onu əlçatmaz olmasına səbəb olur. Belə ki, ötən illərdə olduğu kimi 2021-ci ildə maliyyə sektorunda DDoS hücumlarında iki dəfə artım müşahidə edilmişdir[8]. Bu səbəbdən təşkilatlar müvafiq kiberhücumların qarşısını almaq məqsədilə şəbəkələrində filtrləmə, trafiklərdə müvafiq limitlərin tətbiq edilməsi, şəbəkə sistemlərində ötürülən

---

[6] *Cyber threats 2021: a year in retrospect (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf)*

[7] *Global threat report (https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf)*

[8] *Cyber threats and trends (https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf)*

məlumatların paylanılmış kanallar vasitəsilə yönləndirilməsi, şəbəkəyə edilən müraciətlərin mənbə ünvanlarına görə sazlanması və digər kimi preventiv tədbirlərin icrasını həyata keçirirlər.

Son zamanlar dünyanın əksər mərkəzi bankları informasiya texnologiyaları və təhlükəsizliyi üzrə risklərin idarə edilməsi ilə bağlı nəzarət tədbirlərini gücləndirmiş və bu sahəyə diqqəti artırmışlar. Mərkəzi bankların nəzarət bölmələri tərəfindən kibertəhlükəsizliklə bağlı risklərin idarə olunması üzrə mütəmadi olaraq nəzarət yoxlamaları aparmaqdadırlar. Bu yoxlamalar, keçirilən tematik təhlillər və aparılan davamlı nəzarət işi ilə yanaşı, kibertəhlükəsizliyin və risklərin idarə olunması ilə bağlı boşluqların aşkar edilməsinə imkan verməkdədir. Bu xüsusda, maliyyə institutları informasiya təhlükəsizliyi, həmçinin kibertəhlükəsizlik üzrə riskləri tənzimləyərkən əsasən aşağıda qeyd edilən tədbirlərin həyata keçirilməsini hədəfləyirlər:

- İnformasiya texnologiyaları strategiyasının ümumi biznes strategiyası ilə əlaqələndirilməsi;
- İnformasiya texnologiyaları, informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə risklərə təşkilati risk idarəetmə çərçivəsində baxılması, hərtərəfli risk reyestrinin formalaşdırılması, o cümlədən müvafiq risklərin identifikasiyası, monitorinqi və aradan qaldırılması mexanizmlərinin tətbiq edilməsi;
- İşçi heyətinin kibertəhlükəsizlik riskləri üzrə adekvat təlim və maarifləndirmə tədbirləri ilə əhatə olunması;
- Məlumatların təsnifatı ilə bağlı müvafiq siyasət və prosedurların formalaşdırılması və tətbiq edilməsi;
- Sanksiyaolunmamış girişlərin məhdudlaşdırılması, o cümlədən girişlərin idarə edilməsi mexanizmlərinin tətbiq edilməsi və adekvat nəzarət prosedurları ilə əhatə olunması;
- Kənar xidmət təchizatçılarının (kontragentlərin) cəlb edilməsi prosesinin effektiv idarə edilməsi, həmin xidməti münasibətlər formalaşmaqdan öncə və sonra davamlı informasiya təhlükəsizliyi üzrə nəzarət mexanizmləri ilə əhatə olunması;
- Köhnə texnologiyaya əsaslanan həllərin informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə adekvat nəzarət mexanizmləri ilə əhatə olunması;

- Fövqəladə hallar zamanı bərpa və biznesin davamlığı planlarının adekvatlığının təmin olunması və davamlı olaraq müxtəlif ssenarilər üzərindən testləşdirilməsi.

4. Bençmark ölkələrin qabaqcıl təcrübələri

Strategiyanın formalaşdırılması zamanı Avstraliya, ABŞ, Avropa Birliyi ("AB"), Yaponiya və Sinqapur kimi ölkələrin kibertəhlükəsizlik sahəsində qabaqcıl təcrübələri təhlil edilmişdir. Sözügedən ölkələrin kibertəhlükəsizlik ekosistemləri dörd müxtəlif meyar üzrə müqayisə edilmişdir: (i) kibertəhlükəsizlik siyasəti və strategiyası; (ii) tənzimləyici çərçivələr; (iii) kibertəhlükəsizlik mədəniyyəti və (iv) kibertəhlükəsizlik üzrə maarifləndirmə, təlim və bacarıqlar.

4.1. Avstraliya

Kibertəhlükəsizlik siyasəti və strategiyası	Avstraliya requlyatoru (APRA) tərəfindən 2020-2024-cü illəri əhatə edən Avstraliyanın kibertəhlükəsizlik Strategiyası hazırlanmışdır. Strategiya üzrə prioritet sahələr aşağıdakılardır: ▪ Qabaqcıl kiber təcrübələrin tətbiq edilməsi, kiber informasiya mübadiləsinin təkmilləşdirilməsi və kiber insidentlərə effektiv cavab reaksiyalarının hazırlanması üzrə kiber nəzarət bazasının formalaşdırılması; ▪ Maliyyə institutlarının rəhbər şəxsləri tərəfindən kiber hadisələrə effektiv nəzarət edilməsi və dəyişikliklərin idarə edilməsi üzrə bacarıqların yaradılması; ▪ Maliyyə ekosistemi daxilində zəifliklərin aradan qaldırılması üzrə kiber qiymətləndirmənin, maliyyə sistemində kiber nəzarət və tənzimləmə üzrə təbliğatın aparılması.
Tənzimləyici çərçivələr	▪ 2019-cu ildə APRA tərəfindən nəzarət subyektlərində kibertəhlükələrə qarşı davamlığın gücləndirilməsi məqsədilə kibertəhlükəsizlik sahəsində prudensial standartlar və tələblər müəyyən edilmişdir. Nəzarət subyektləri tərəfindən aşağıdakı tələblərə riayət edilməlidir: ▪ Təşkilatda rəhbərliyin informasiya təhlükəsizliyi ilə bağlı vəzifə və səlahiyyətlərinin müəyyən edilməsi; ▪ İnformasiya texnologiyaları aktivləri üzrə kibertəhdidlərin ölçüsü və miqyasına uyğun olaraq informasiya təhlükəsizliyi tədbirlərinin həyata keçirilməsi; ▪ İnformasiya texnologiyaları aktivlərinin qorunması üzrə nəzarət tədbirlərinin həyata keçirilməsi;

	▪ Təhlükəsizlik insidentləri barədə APRA-nın məlumatlandırılması.
Kibertəhlükəsizlik mədəniyyəti	İllik kibertəhlükəsizlik hesabatı: ▪ Kiber insidentlərin böyük hissəsi “orta səviyyəli insident” (36,5%) və “əhəmiyyətli” (33,3%) kateqoriyasına aid insidentlərdir; ▪ Ən çox müşahidə edilən kiber insident növləri “fişinq” (27%) və “ələ keçirilmiş sistemlər” (24,4%) kimi qruplaşdırılır.
Kibertəhlükəsizlik üzrə maariflənmə, təlim və bacarıqlar	Avstraliya on ildə 1,6 mlrd. AUD məbləğində investisiya qoyulmasını planlaşdırır: ▪ Sertifikatlaşdırılmış kibertəhlükəsizlik mütəxəssislərinin sayının artırılması; ▪ Avstraliyanın kiberbacarıqlar zəncirinin formalaşdırılması üzrə əməkdaşlığın genişləndirilməsi; ▪ Kiçik və orta müəssisələrdə kiber davamlığın gücləndirilməsi üzrə tövsiyələrin verilməsi; ▪ Kibertəhlükələrlə bağlı ekosistemin məlumatlılığının artırılması.

4.2. ABŞ

Kibertəhlükəsizlik siyasəti və strategiyası	Kibertəhlükəsizlik səviyyəsinin gücləndirilməsi və bu sahədə strateji prioritetlərin müəyyənləşdirilməsi məqsədilə ABŞ-ın müxtəlif qurumları tərəfindən kibertəhlükəsizlik strategiyaları və tədbirləri hazırlanmışdır.
Tənzimləyici çərçivələr	ABŞ Federal Ehtiyat Sistemi müxtəlif maliyyə institutlarından NIST, ISACA və COBIT (kart prosessinq mərkəzləri eyni zamanda PCI-DSS) standart və metodoloji çərçivələrə riayət etmələrini tələb edir.
Kibertəhlükəsizlik mədəniyyəti	“Pew Tədqiqat Mərkəzi”nin məlumatına əsasən: ▪ Əksər hallarda əhali kibertəhlükəsizliklə bağlı qabaqcıl təcrübələrə riayət etmir; ▪ Aparılmış sorğulara əsasən respondentlərin 64%-i informasiyanın sızması hallarına məruz qaldığını bildirmişlər.
Kibertəhlükəsizlik üzrə maariflənmə, təlim və bacarıqlar	▪ NIST tərəfindən davamlı olaraq kibertəhlükəsizlik üzrə tədbirlər və nəşrlər dərc olunur; ▪ Milli Kibertəhlükəsizlik Təhsil Təşəbbüsü (NICE) çərçivəsində kibertəhlükəsizlik üzrə təhsil, təlim və işçi qüvvəsinə yönəlmiş hökumət, akademik dairələr və özəl sektor arasında mövcud olan birgə əməkdaşlıq münasibətləri formalaşdırılmışdır; ▪ Kibertəhlükəsizlik karyeraları və tədqiqatları üzrə milli təşəbbüs çərçivəsində kibertəhlükəsizlik sahəsində təhsil, təlim və karyera imkanları yaradan onlayn portal formalaşdırılmışdır.

4.3. Avropa Birliyi

Kibertəhlükəsizlik siyasəti və strategiyası	AB-də maliyyə bazarları iştirakçıları üçün nəzərdə tutulmuş kiber dayanıqlıq strategiyası CPMI-IOSCO Kiber Təlimatına əsaslanır və bu strategiya üç hissədən ibarətdir: ▪ Maliyyə institutlarının kiber dayanıqlığı: Avropa Mərkəzi Bankı "Kiber dayanıqlıq nəzarəti gözləntiləri"ni (CROE) dərc etmiş və maliyyə institutlarının kibertəhlükəsizlik üzrə yetkinlik səviyyəsini üç bölməyə ayırmışdır: (i) İnkişaf səviyyəsi: bütün ödəniş sistemləri inkişaf gözləntilərinə cavab verməli və qabaqcıl səviyyəyə çatmağa səy göstərməlidirlər; (ii) Qabaqcıl səviyyə: inkişaf səviyyəsini özündə ehtiva etməli və əlavə olaraq bütün sistem əhəmiyyətli ödəniş sistemləri qabaqcıl səviyyə üzrə gözləntiləri qarşılamalı, innovasiya səviyyəsinə çatmağa səy göstərməlidirlər; (iii) İnnovasiya səviyyəsi: inkişaf səviyyəsini, qabaqcıl yetkinlik səviyyəsini və əlavə olaraq son səviyyəni özündə əhatə etməlidir. Eyni zamanda, Avropa Mərkəzi Bankı AB-də maliyyə infrastrukturu və institutlarında kiberhücumların qarşısını almaq üçün tətbiq edilən tədbirlərin yoxlanılması və təkmilləşdirilməsi məqsədilə TIBER-EU çərçivəsini formalaşdırmışdır. ▪ Sektorun dayanıqlığı: UNITAS vasitəsilə maliyyə bazarlarında kibertəhlükəsizlik çalışmasının həyata keçirilmə ssenarisi və kommunikasiyası qaydası formalaşdırılmışdır.
Tənzimləyici çərçivələr	Avropa Nəzarət Orqanlarının Birgə Komitəsi (EBA, ESMA və EIOPA) tərəfindən AB-nin maliyyə sistemində informasiya təhlükəsizliyinin və kibertəhlükəsizliyin gücləndirilməsi üzrə hazırladığı təşəbbüslərə aşağıdakılar daxildir: ▪ Bulud həllərinə əsaslanan maliyyə xidmətlərini təqdim edən üçüncü tərəf təchizatçıları üzrə nəzarət çərçivəsinin hazırlanması; ▪ Sistem əhəmiyyətli maliyyə institutlarının kiber davamlığını yoxlamaq üçün müvafiq çərçivənin hazırlanması.
Kibertəhlükəsizlik mədəniyyəti	AB-nin 2020-ci il üzrə kibercinayətkarlıq sorğusuna əsasən respondentlərin: ▪ 52%-i kibercinayətkarlıq haqqında aydın təsəvvürə malikdirlər; ▪ 59%-i kibercinayətkarlıqdan özlərini kifayət qədər qoruya bildiklərini bildirmişlər; ▪ 10%-i kibertəhdidlər səbəbindən onlayn ticarət etməkdən ehtiyat edirlər.
Kibertəhlükəsizlik üzrə maariflənmə, təlim və bacarıqlar	Avropa İttifaqının Kibertəhlükəsizlik Agentliyi (ENISA) tərəfindən kibertəhlükəsizlik sahəsində maarifləndirmə üzrə bir çox təşəbbüslər həyata keçirilir: ▪ Kibertəhlükəsizliyin gücləndirilməsi üçün təlimatın hazırlanması;

	▪ “Avropa kibertəhlükəsizlik ayı”nın təşkil edilməsi; ▪ “Avropa kibertəhlükəsizlik çağırışı” adlı tədbirlərinin keçirilməsi; ▪ Kiber insidentlər və böhran idarəetməsi üçün mexanizmlərin hazırlanması.

4.4. Yaponiya

Kibertəhlükəsizlik siyasəti və strategiyası	Maliyyə Xidmətləri Agentliyi (FSA) 2018-ci ildə rəqəmsallaşma ilə bağlı fəaliyyəti həyata keçirmək üçün “Maliyyə Sektorunda Kibertəhlükəsizliyin Gücləndirilməsinə dair Siyasət Yanaşmaları” nəşr etmişdir. Daha sonra, 2020-ci ildə FSA maliyyə institutlarının ümumi çətinliklərini təsvir edən “Maliyyə Xidmətləri Kibertəhlükəsizlik Hesabatı”nı dərc etmişdir. FSA kiçik və orta maliyyə institutlarının kibertəhlükəsizlik üzrə idarəetmə sistemlərinin effektivliyinin artırılması məqsədilə ölkənin digər aidiyyəti qurumları ilə əməkdaşlığın gücləndirilməsini, həmçinin daha böyük maliyyə institutları üzrə risklərin idarə edilməsi siyasətlərinin təkmilləşdirilməsini və kibertəhdidlərə qarşı mübarizə tədbirlərinin daha da inkişaf etdirilməsini təşviq edir.
Tənzimləyici çərçivələr	FSA tərəfindən “Maliyyə sahəsində şəxsi məlumatların mühafizəsi üzrə təlimatlar” hazırlanmışdır. Eyni zamanda, Agentlik tərəfindən maliyyə institutlarında və digər nəzarət subyektlərində məlumat sızmasının, itkisinin və ya zədələnməsinin qarşısının alınması üçün kibertəhlükəsizlik üzrə tələblər müəyyən edilmiş və tətbiqi həyata keçirilməkdədir. Həmçinin Yaponiyada kritik infrastrukturların kibertəhlükəsizlik vəziyyətinin gücləndirilməsi məqsədilə Kibertəhlükəsizlik üzrə milli Strategiya (NISC) hazırlamışdır. Qurum tərəfindən təşkilatların kibertəhlükəsizlik üzrə ən yaxşı təcrübələrə riayət etmələri təşviq edilir.
Kibertəhlükəsizlik mədəniyyəti	Son kibertəhlükəsizlik sorğusuna əsasən respondentlərin: ▪ 81%-i əsas kibertəhdidləri informasiya sistemlərinə edilən hücumlar kimi səciyyələndirir; ▪ 84%-i kiberhücumların nəticəsindən narahat olduqlarını qeyd etmişlər.
Kibertəhlükəsizlik üzrə maariflənmə, təlim və bacarıqlar	Yaponiyada hökumət orqanları, tədqiqat/təhsil müəssisələri tərəfindən kibertəhlükəsizlik üzrə təhsil və təlim proqramları keçirilməkdədir: ▪ Universitetlər tələbələrin informasiya və kibertəhlükəsizlik sahəsi üzrə zəruri bacarıqlarla yiyələnməsi üzrə xüsusi proqramlar keçirir;

	▪ Kibertəhlükəsizlik Strategiyası Qərargahı təhlükəsizlik standartlarını inkişaf etdirmək, məlumatlılığı artırmaq və riskləri idarə etmək etmək üçün tədbirləri təşviq edir; ▪ İqtisadiyyat, Ticarət və Sənaye Nazirliyi və İnformasiya Texnologiyalarının Təşviqi Agentliyi birgə fəaliyyət nəticəsində kibertəhlükəsizlik risklərinin tanınması üçün "Kibertəhlükəsizliyin idarə edilməsi təlimatları" nəşr etməkdədir.

4.5. Sinqapur

Kibertəhlükəsizlik siyasəti və strategiyası	Sinqapur Kibertəhlükəsizlik Agentliyi (CSA) tərəfindən kibertəhlükəsizlik strategiyası hazırlanmışdır. Strategiyada əsas dörd məqam üzrə vizyon və məqsədlər müəyyən edilmişdir: ▪ Kritik informasiya infrastrukturlarının dayanıqlığının artırılması; ▪ Kibertəhlükəsiz mühitin yaradılması üçün biznesin mobilizasiyası; ▪ Bacarıqlı insan kapitalı və texnoloji cəhətdən təkmil şirkətlərdən ibarət ekosistemin inkişaf etdirilməsi; ▪ Beynəlxalq tərəfdaşlıqların qurulması.
Tənzimləyici çərçivələr	Sinqapur Monetar Qurumu (MAS) tərəfindən kiber dayanıqlı maliyyə sektorunu yaratmaq mandatına əsaslanaraq üç əsas təlimat (həmçinin bildiriş) toplusu nəşr edilmişdir: ▪ Texnoloji risklərin idarə edilməsi təlimatı; ▪ Texnoloji risklərin idarə edilməsi üzrə bildirişlər; ▪ Kibergigiyena üzrə bildirişlər. MAS sürətlə dəyişən kiber mənzərə və bulud texnologiyaları, API və tətbiqi-proqram təminatlarının inkişafına artan zərurəti nəzərə alaraq, "Texnoloji risklərin idarə edilməsi təlimatı"nı nəşr etdirmişdir. Təlimatın tələbləri banklara, ödəniş təşkilatlarına, broker və sığorta şirkətlərini əhatə edir.
Kibertəhlükəsizlik mədəniyyəti	Kibertəhlükəsizlik sorğusuna əsasən respondetlərin: ▪ Kiber insidentlərlə bağlı narahatlıq səviyyəsi yüksəkdir; ▪ Yalnız 4%-i fişinq məktublarını müəyyən edə bilir; ▪ Bir çoxu kiber insidentlərlə üzləşməyəcəklərinə inanırlar.
Kibertəhlükəsizlik üzrə maariflənmə, təlim və bacarıqlar	Kiber Təhlükəsilzik Agentliyi (CSA) dövlət qurumları və tərəfdaşlarla birgə əməkdaşlıq çərçivəsində kibertəhlükəsizlik üzrə təlim və maarifləndirmə tədbirlərini həyata keçirir. Bunlardan:

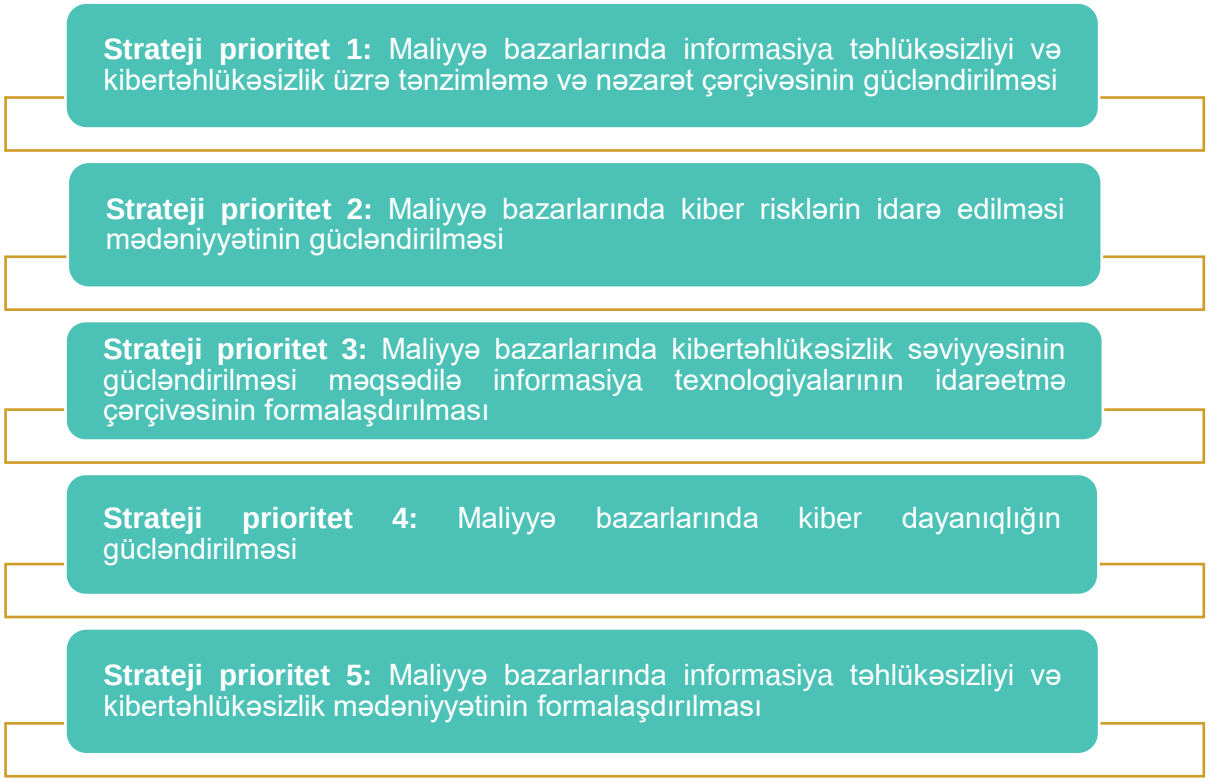
	▪ İKT peşəkarlarını hazırlamaq və bacarıqlarını artırmaq məqsədilə “Kibertəhlükəsizlik karyera mentorluq Proqramı”nın hazırlanması; ▪ Sinqapurda kibertəhlükəsizlik ekosistemini gücləndirmək məqsədilə ICE71 “start up hub”ının formalaşdırılması; ▪ Qadınların kibertəhlükəsizlik peşəsinə yiyələnməyə həvəsləndirmək üçün “Kiber qadın təşəbbüsü”nün həyata keçirilməsi.

5. Maliyyə bazarları üzrə kibertəhlükəsizlik strategiyası

Maliyyə bazarları üzrə kibertəhlükəsizlik strategiyasının əhatə dairəsi formalaşdırılarkən onun vizyonunun, missiyasının və başlıca strateji hədəflərinin müəyyən edilməsi zəruridir. Belə ki, AMB-nin kibertəhlükəsizlik strategiyası üzrə vizyonu **“maliyyə sabitliyinin təmin edilməsi üçün artan kibertəhdidlər fonunda ölkənin maliyyə bazarlarında kiber dayanıqlığın gücləndirilməsidir”**.

Strategiyanın missiyası **kibertəhlükəsizlik sahəsində etibarlı təhlükəsizlik infrastrukturu, təkmil bilik və bacarıqlara malik olan insan kapitalı, kibertəhdidlər barədə məlumatların qarşılıqlı kommunikasiyası həyata keçirilən effektiv əməkdaşlıq münasibətləri, habelə adekvat tənzimləmə çərçivəsi ilə əhatə olunmuş maliyyə sisteminin formalaşdırılması və onun kiber dayanıqlığının təmin edilməsidir.** Bu missiyanın həyata keçirməsi üçün AMB-nin başlıca strateji hədəfləri **1)** ölkənin maliyyə bazarlarında kibertəhlükəsizlik ekosisteminin formalaşdırılması, o cümlədən kibertəhdidlərə adekvat reaksiyanın verilməsi və kibertəhlükəsizlik səviyyəsinin yüksəldilməsi; **2)** kibergigiyena tədbirlərinə, həmçinin qarşılıqlı tərəfdaşlıq çərçivəsində davamlı məlumat mübadiləsinə üstünlük verərək maliyyə sisteminin dayanıqlığının yüksəldilməsi; **3)** AMB-nin mandatı çərçivəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik ilə bağlı normativ-metodoloji bazanın formalaşdırılması, davamlı aktuallaşdırılması və bununla da ölkənin maliyyə bazarlarında maliyyə sabitliyinin təmin edilməsidir.

Startegiyadan irəli gələn hədəflərin effektiv icrası məqsədilə 2023-2026-cı illər ərzində aşağıda qeyd edilən beş strateji prioritet üzrə tədbirlərin realizasiyası nəzərdə tutulmuşdur:



5.1. Strateji prioritet 1: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə tənzimləmə və nəzarət çərçivəsinin gücləndirilməsi

5.1.1. Risk əsaslı nəzarət və tənzimləmə çərçivəsinin formalaşdırılması

İnformasiya və kommunikasiya texnologiyalarının mürəkkəbləşməsi, təhlükəsizlik risklərinin davamlı olaraq artması, həmçinin informasiya təhlükəsizliyi ilə bağlı insidentlərin (kiber insidentlər daxil olmaqla) intensivləşməsi maliyyə institutlarının əməliyyat fəaliyyətinə əhəmiyyətli şəkildə təsir göstərməkdədir. Eyni zamanda, müasir dövrdə maliyyə institutları bir-biri ilə sıx əlaqədə fəaliyyət göstərdiklərindən informasiya təhlükəsizliyi və / və ya kibertəhlükəsizlik sahəsində baş verə bilən kritik insidentlər potensial olaraq bütün maliyyə sisteminə təsir edə bilər. Bu baxımdan maliyyə bazarlarına nəzarət orqanları tərəfindən aidiyyəti üzrə risk əsaslı nəzarət və tənzimləmə çərçivələri formalaşdırılır və tətbiqinin həyata keçirilməsi daim diqqət mərkəzində saxlanılır.

Maliyyə sektorunda risk əsaslı nəzarət və tənzimləmə çərçivələrinin tətbiqi maliyyə institutlarının üzləşə biləcəyi potensial risklərin vaxtında müəyyən edilməsinə və qiymətləndirilməsinə, həmin risklərin azaldılması istiqamətində effektiv mitiqasiya tədbirlərinin müəyyən edilməsinə imkan yaradır. Bununla yanaşı, risk əsaslı nəzarət və

tənzimləmə fəaliyyətinin həyata keçirilməsi maliyyə institutlarına müvafiq risklərinin idarə olunması üçün nəzarət gözləntilərini daha yaxşı başa düşməyi təmin etmək məqsədi daşıyır. Bu xüsusda, risk əsaslı nəzarət və tənzimləmə çərçivəsinin tətbiqi maliyyə institutlarına öz risklərini effektiv şəkildə idarə etməyə, o cümlədən kibertəhdidlərə və onları əhatə edən risklərə qarşı hazırlıq səviyyələrini yüksəltməyə köməklik edəcəkdir.

Risk əsaslı nəzarət və tənzimləmənin formalaşdırılması üzrə AMB-nin gözləntiləri:

1. Maliyyə insitututları tərəfindən informasiya təhlükəsizliyinə dair minimum tələblərə riayət edilməsi və bununla da maliyyə bazarlarında dayanıqlı informasiya təhlükəsizliyi və kibertəhlükəsizlik mühitinin formalaşması;
2. Maliyyə institutları tərəfindən kibertəhlükəsizlik risklərinin proaktiv identifikasiyasının təmin edilməsi;
3. Kibertəhdid və təhlükə mənzərəsinin dəyişməsi halında yaranan risklərin proqnozlaşdırılması və adekvat tədbirlərin görülə biləcəyinə əminliyin artırılması;
4. Kibertəhlükəsizlik risklərinin əhəmiyyətli təhlükəyə çevrilməmişdən öncə qabaqlayıcı tədbirlərin görülməsi;
5. Kibertəhlükəsizlik üzrə nəzarət və tənzimləmə çərçivəsinin beynəlxalq standartlara və qabaqcıl təcrübələrə uyğunlaşdırılması fonunda maliyyə institutlarının kiber dayanıqlıq səviyyəsinin yüksəldilməsi;
6. Kiber insidentlərin ehtimalının və təsirinin azaldılması, həmçinin maliyyə institutlarının kiber insidentlərə hazırlıq səviyyəsinin yüksəldilməsi;
7. Maliyyə institutlarının reputasiyasının yaxşılaşdırılması, həmçinin kiberdayanıqlığa əminliyin artırılması fonunda maliyyə sektoruna inamın yüksəldilməsi.

5.1.2. Maliyyə sektorunda sahəvi FinCert-in yaradılması

Müasir dövrdə artan kibertəhdidlər fonunda informasiya sistemlərində təhlükəsizlik boşluqlarının mövcudluğu kibertəhlükəsizlik insidentlərinin yaranmasına və bununla da təşkilatların gündəlik iş fəaliyyətlərində dayanmalara səbəb olur. Qloballaşan dünyada müxtəlif kibercinayətkarların hədəfinə çevrilmiş təşkilatlara, xüsusilə də maliyyə institutlarına qarşı çoxşaxəli və texnoloji cəhətdən müxtəlif olan hücumların sayı artmaqdadır. Təşkilatlar bu cür hücumlara qarşı cavab olaraq fövqəladə hallar zamanı əməliyyatların davamlılığı və bərpa planlarını hazırlayır və müxtəlif ssenarilər üzərindən yoxlamalar həyata keçirir. Bu cür

planlar informasiya aktivlərinə təsir edən təhlükəsizlik hadisələrinin aşkarlanması, qiymətləndirilməsi və aradan qaldırılması kimi tədbirlədən ibarət prosesləri özündə ehtiva edir. Ən sadə zərərverici proqram təminatı yoluxmalarından tutmuş, itirilən və ya oğurlanan şifrələnməmiş mobil cihazlar, icazəsiz giriş səlahiyyətləri və məlumat bazalarının açıqlanmasının qısa və uzunmüddətli nəticələri istənilən maliyyə institutunun biznes uğursuzluğuna təsir göstərə bilir.

Maliyyə sistemini əhatə edən kiberhücumların artım tempini nəzərə alaraq, AMB tərəfindən nəzarət subyektləri üçün insidentlərin idarə edilməsi platformasının formalaşdırılması mövcud şəraitdə kiberhücumların vaxtında aşkar edilməsi, effektiv kommunikasiyası və mənfi təsirlərinin azaldılmasına imkan verəcəkdir. Beynəlxalq təcrübədə sahəvi CERT-lərin formalaşması, əsasən də maliyyə sistemində müvafiq fəaliyyətin təmin edilməsi bu sahədə insidentlərin idarə edilməsinin, həmçinin insidentlərə adekvat reaksiyaların verilməsi, insidentlər barədə çevik məlumatlandırılma və qabaqlayıcı tədbirlərin planlaşdırılmasına imkan yaradır. CERT-in əsas məqsədi kompüter təhlükəsizliyi ilə bağlı insidentlərə operativ reaksiya verməklə kibertəhlükəsizlik üzrə insidentlərin effektiv idarə olunmasının təmin edilməsidir.

AMB mandatından irəli gələn fəaliyyətin təmin edilməsi üçün qanunvericilik bazasını gücləndirərək maliyyə bazarlarında kibertəhlükəsizlik sahəsində fəaliyyətin idarə edilməsini təmin edəcək, həmçinin maliyyə sistemində kiber-risklərin idarə edilməsi, adekvat nəzarət mexanizmlərinin qurulması və məlumatlılığının artırılması məqsədilə sahəvi CERT xidmətinin yaradılmasını nəzərdə tutur. AMB-də insidentlərin idarə edilməsi mərkəzinin formalaşdırılması maliyyə bazarlarında kibertəhlükəsizliyin pozulmasına yönəlmiş hərəkətlərin aşkarlanmasına, qarşısının alınması üçün profilaktik tədbirlərin görülməsinə, habelə bütövlükdə milli CERT-lərlə birgə ölkədə təhlükəsiz kiberməkanın yaradılmasına xidmət edəcəkdir.

AMB-də FinCERT-in formalaşdırılması aşağıda qeyd olunan üç aspektin müəyyən edilməsini vacib edir:

- FinCERT-in missiyası;
- FinCERT mümkün strukturları;
- Vəzifə və səlahiyyətlər.

FinCERT-in “necə” strukturlaşdırılacağı maliyyə sisteminin ehtiyaclarından asılıdır. Bu zaman FinCERT-in 24/7 rejimində fəaliyyət göstərməsi, zəruri bilik və bacarıqlara malik insan resurslarının mövcudluğu, müvafiq texnoloji infrastrukturun yaradılması üzrə əməliyyat və investisiya xərcləri və digər bu kimi məsələlər nəzərə alınmalıdır. Bu baxımdan FinCERT-in qurulmasında əsas səbəblər aşağıdakılardır:

- Maliyyə bazarlarında FinCERT-in yaradılması yolu ilə koordinasiyalı şəkildə dayanıqlı kibertəhlükəsizlik ekosisteminin qurulması;
- Beynəlxalq təcrübəyə uyğun olaraq maliyyə sisteminin kritik infrastruktur kimi müəyyən edilməsi;
- Xüsusi proqram təminatlarından istifadə edərək maliyyə sektorunun kiber kəşfiyyat məlumatlarının birgə və ya müstəqil toplanılması, araşdırılması və məlumatlandırılmanın təmin edilməsi;
- Maliyyə bazarlarında dayanıqlı infrastrukturun təmin edilməsi məqsədilə kiberinsidentlərə cavab tədbirləri və bərpa planlarının hazırlanması;
- Milli və beynəlxalq tərəfdaşlıq fəaliyyətini genişləndirməklə kibertəhlükəsizlik tələblərinin və ən yaxşı təcrübələrin tətbiq edilməsi;
- Kiber-risklərin idarəedilməsi proseslərini formalaşdırmaqla maliyyə institutlarında kibertəhlükəsizlik səviyyəsinin gücləndirilməsi;
- Maraqlı tərəfləri cəlb etməklə daha mürəkkəb ssenarilərlə müntəzəm sahəvi kibertəhlükəsizlik təlimlərinin keçirilməsi;
- Kibertəhlükəsizlik sahəsində ixtisaslı işçi qüvvəsinin formalaşdırılması məqsədilə maliyyə institutlarında təlim proqramlarının həyata keçirilməsi.

5.1.3. FinCERT-in missiyası

FinCERT tərəfindən maliyyə institutlarına aşağıdakı xidmətlərin təqdim edilməsi missiyanın vacib elementlərindən hesab edilir:

1. **İnsident barədə məlumatların əldə olunması.** Kiberinsidentlərlə bağlı məlumatların maliyyə institutlarından əldə olunması üçün onlar ilk növbədə FinCERT-in mövcud olduğunu bilməlidirlər. Eyni zamanda, maraqlı tərəflər FinCERT tərəfindən həyata keçirilməsi nəzərdə tutulan xidmətlər və həmin xidmətlərin təqdim edilməsi şərtləri barədə məlumatlı olmalıdırlar.

Bu məqsədlə, FinCERT öz missiyasını və xidmətlərini müəyyən etməli, bu barədə maraqlı tərəfləri məlumatlandırmalı və müvafiq xidmətlər barədə fəaliyyət qaydalarını bəyan etməlidir. Funksional imkanların effektiv şəkildə həyata keçirilməsi üçün FinCERT müvafiq infrastruktur imkanlarına malik olmalıdır:

- Qanunvericiliyə uyğun olaraq FinCERT çətir kimi çıxış etməli və milli CERT-lərlə əməkdaşlıq etməlidir;
- Maliyyə bazarlarında kibertəhlükəsizlik səviyyəsinin gücləndirilməsi məqsədilə FinCERT ilə milli CERT-lər arasında effektiv kommunikasiya təşkil edilməlidir;
- FinCERT-in fəaliyyətində ən yaxşı beynəlxalq təcrübələri mənimsəmək üçün beynəlxalq səviyyədə fəaliyyət göstərən müxtəlif maliyyə CERT-ləri/FS-ISAC-ları ilə əlaqələr qurulmalıdır.

2. **İnsidentlər barədə məlumatların analiz edilməsi.** İnsident barədə məlumatlar əldə olunduqdan sonra FinCERT onun baş vermə səbəblərini təhlil edir. FinCERT daha sonra fəaliyyətin bərpa edilməsi və insident nəticəsində dəyə biləcək zərərin minimallaşdırılması məqsədilə ilkin cavab reaksiyasının hazırlanmasında iştirak edir. FinCERT milli CERT-lərə kibertəhlükəsizlik insidentləri barədə məlumat verərkən, maliyyə sistemində baş verən təhdidlərin nümunələrini və maliyyə sisteminə təsirini başa düşmək üçün kiber insidentlərin təhlilini apararmalıdır.

3. **İnsidentlər üzrə fəaliyyətin effektiv koordinasiyası və nəticələrin araşdırılması sahəsində köməklik göstərilməsi.** FinCERT-in fəaliyyət istiqamətindən asılı olaraq aşağıdakı tədbirlərin təmin olunması zəruridir:

- İnsidentlərə cavab vermə prosesinin təşkilinə dəstək göstərilməsi;
- İnsidentlərə cavab vermə prosesində maraqlı tərəflərlə, habelə milli CERT-lərlə koordinasiyanın həyata keçirilməsi;
- Maliyyə sistemində kiber dayanıqlığın gücləndirilməsi məqsədilə kibertəhlükəsizlik sahəsində zəruri bilik və bacarıqların artırılması, həmçinin maarifləndirmə üzrə təşəbbüslərin həyata keçirilməsi.

Eyni zamanda, FinCERT maliyyə ekosistemində kibergigiyena mühitinin yaradılmasını təşviq etməli, yeniliklərlə bağlı məlumatlılığı artırmalı və davamlı olaraq bu fəaliyyəti diqqət

mərkəzində saxlamalıdır. Bu fəaliyyət çərçivəsində aşağıda qeyd olunan tədbirlərin həyata keçirilməsi vacibdir:

- Müxtəlif dövlət və özəl təşkilatlar cəlb olunmaqla geniş miqyasda kibertəhlükəsizlik üzrə maarifləndirmə və məlumatlandırma səviyyəsinin artırılması, həmçinin maliyyə ekosistemində hər bir əməkdaşın informasiya kommunikasiya texnologiyalarından təhlükəsiz istifadə mədəniyyətinin yüksəldilməsi yolu ilə dayanıqlı kibertəhlükəsizlik mühitinin qurulması;

- Milli CERT-lərlə sıx əməkdaşlıq çərçivəsində rəqəmsal kanallar vasitəsilə kibertəhlükəsizlik üzrə məlumatların yayımlanması.

5.1.4. Mümkün FinCERT strukturları

AMB-nin nəzərə ala biləcəyi bir neçə mümkün CERT strukturları aşağıda təqdim edilmişdir:

1. Mərkəzləşdirilmiş CERT. Mərkəzləşdirilmiş CERT strukturu yanaşmasında təşkilat daxilində vahid insidentlərə cavabvermə qrupu formalaşdırılır və insidentlərin idarə olunması məhz bu qrup tərəfindən həyata keçirilir;

2. Paylanmış CERT. Paylanmış CERT strukturunda bir neçə müstəqil insidentlərə cavabvermə qrupu olur. CERT resurslarının paylanması təşkilatın geniş coğrafi dairəsindən və ya onun kritik infrastrukturunun yerləşdiyi yerdən asılı ola bilər;

3. Əlaqələndirici CERT. Bu tip strukturlu CERT digər, çox vaxt tabeli CERT-ləri idarə edir. Belə ki, CERT insidentlərə cavab tədbirlərini, məlumat axını və iş axınını digər əlaqəli qruplar arasında koordinasiya edir. Əlaqələndirici CERT özü müstəqil şəkildə hər hansı bir insidentə cavab tədbirini təqdim etmir, yalnız əlaqəli qruplar arasında fəaliyyəti əlaqələndirir;

4. Hibrid CERT/SOC. Bu tip ixtisaslaşmış hibrid modeldə Təhlükəsizlik Əməliyyatları Mərkəzi (SOC) insidentlər barədə bildirişlərin və məlumatların əldə olunmasına cavabdehdir. SOC əlavə təhlil üçün yardım tələb edildiyi təqdirdə CERT fəaliyyətini aktivləşdirir. Əsasən, SOC hadisənin aşkar edilməsini həyata keçirir və daha sonra insidentlər üzrə fəaliyyətin effektiv koordinasiyası və nəticələrin araşdırılması sahəsində köməklik göstərilməsi məqsədilə CERT fəaliyyətinə ötürür.

Maliyyə bazarlarında kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi nəticələrinə nəzər saldıqda, **hibrid CERT/SOC** modelinin tətbiqi məqsədəuyğun hesab edilmişdir. Maliyyə bazarlarında insidentlərinin mərkəzləşdirilmiş şəkildə toplanılması, maliyyə

ekosisteminin iştirakçılarına insidentlər barədə məlumatların vaxtında və çevik çatdırılması, həmçinin adekvat tədbirlərin görülməsi maliyyə sisteminin sabitliyinin təmin edilməsinə dəstək olacaqdır.

5.1.5. Vəzifə və səlahiyyətlər

Qrupun daxili təşkilatlanması, həmçinin əsas komanda üzvləri və funksiyalararası komanda münasibətlərində məsiliyyət bölgüsünün dəqiq müəyyən edilməsi əsas vacib məqamlardandır. Xüsusilə də maliyyə institutlarının nəzarət orqanı ilə, texniki heyət ilə (əlavə məlumatları toplamaq və məsələləri araşdırmaq üçün), həmçinin digər şəxslərlə (digər komandalara, rəhbərliyə və hətta bəzi hallarda hüquq-mühafizə orqanlarına, mətbuata, müştərilərə, kontragentlərə və sair) kommunikasiyanın təşkil edilməsi vacibdir. Bu məqsədlə maliyyə institutları tərəfindən aşağıdakı minimum tədbirlərin icrası təmin edilməlidir:

- İnformasiya təhlükəsizliyinin təmin edilməsi məqsədilə daxili informasiya və kibertəhlükəsizlik siyasətinin, prosedurların və təlimatların hazırlanması;
- Təhlükəsizlik insidentlərinə cavab reaksiyasının verilməsi və risklərin idarə edilməsi daxil olmaqla xüsusi tədbirlərin həyata keçirilməsi;
- İnformasiya texnologiyaları və digər funksional komandalarla sıx əməkdaşlıq çərçivəsində informasiya təhlükəsizliyi layihələrinin icrasına nəzarət edilməsi;
- İnformasiya təhlükəsizliyinə təsir edən cari və potensial hüquqi və tənzimləyici çatışmazlıqların müəyyən edilməsi, həmçinin hüquqi və komplayens komandaları ilə birlikdə onların təsirinin qiymətləndirilməsi;
- Davamlı olaraq informasiya təhlükəsizliyi üzrə risk qiymətləndirilməsinin həyata keçirilməsi;
- Öz müştərilərinə adekvat xidmətlər göstərmək qabiliyyətinə, onun nüfuzuna və ya maliyyə vəziyyətinə əhəmiyyətli və mənfi təsir göstərə biləcək informasiya təhlükəsizliyi və kibertəhlükəsizlik insidentləri barədə AMB-yə məlumatın verilməsi;
- İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi məqsədilə (müəyyən edilməsi, cavablandırılması, aradan qaldırılması və hesabat) maliyyə sistemində informasiya təhlükəsizliyinin monitorinqinin həyata keçirilməsi.

Dayanıqlı kibermühitin yaradılması, koordinasiya prosesinin effektivliyinin təmin edilməsi, insidentlərə çevik reaksiyanın verilməsi və maraqlı tərəflərin vəziyyətlə bağlı

məlumatlandırılması mövcud kibertəhlükəsizlik səviyyəsinin gücləndirilməsinə zəmin yaradacaqdır. Bu fəaliyyət çərçivəsində FinCERT-in vəzifə və öhdəlikləri aydın şəkildə formalaşdırılmalı və maraqlı tərəflərə çatdırılmalıdır.

Strategiyanın əhatə etdiyi dövr ərzində FinCERT tərəfindən aşağıda qeyd olunan tədbirlərin həyata keçirilməsi nəzərdə tutulur:

- Maliyyə sektorunun kibertəhlükəsizlik ekosisteminin gücləndirilməsi məqsədilə siyasət və tənzimləyici çərçivənin müəyyən edilməsi və daha təhlükəsiz kiberməkanın yaradılması;
- Maliyyə bazarlarında baş verən kiberinsidentlər barədə məlumatların toplanılması, təhlili və yayımlanması;
- Baş verə biləcək kibertəhlükəsizlik insidentlərinin proqnozlaşdırılması və məlumatlandırmanın həyata keçirilməsi yolu ilə dayanıqlı maliyyə sektoru infrastrukturunun yaradılması üçün təxirəsalınmaz tədbirlərin görülməsi;
- Kiber insidentlərə cavab tədbirlərinin və bu sahədə fəaliyyətin əlaqələndirilməsi, həmçinin informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə metodoloji dəstəyin göstərilməsi;
- Dayanıqlı kibertəhlükəsizlik infrastrukturunun qurulması istiqamətində maliyyə sisteminin fəaliyyətinə nəzarətin təmin edilməsi, habelə nəzarət subyektləri və ümumilikdə ictimaiyyət arasında məlumatlılığın artırılması;
- Rəqəmsal kanallar vasitəsilə kibertəhlükəsizlik üzrə maarifləndirmə tədbirlərinin həyata keçirilməsi və kibertəhlükəsizlik üzrə savadlılığın artırılması yolu ilə kibergigiyena mühitinin formalaşdırılması;
- İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə mədəniyyət səviyyəsinin artırılması məqsədilə kibertəhlükəsizlik tədbirlərinin keçirilməsi;
- Kibertəhlükəsizlik üzrə tərəfdaşlığın gücləndirilməsi məqsədilə milli, eləcə də beynəlxalq CERT-lərlə aktiv əməkdaşlıq çərçivəsinin qurulması.

5.2. Strateji prioritet 2: Maliyyə bazarlarında kiber risklərin idarə edilməsi mədəniyyətinin gücləndirilməsi

İnformasiya texnologiyaları üzrə risklərin idarəetmə çərçivəsi ümumi əməliyyat risklərinin idarə edilməsi çərçivəsinin tərkib hissəsi olmalıdır. Sözügedən çərçivə əhatəli olmalı və maliyyə institutunda informasiya texnologiyaları üzrə risklərin effektiv qiymətləndirilməsini dəstəkləməlidir. Təşkilatda informasiya texnologiyaları üzrə risklərin idarəetmə fəlsəfəsi davamlı və proaktiv olmalı, təkcə texnologiyaya deyil, texnologiyadan istifadə edən insan və proseslərə nəzarəti də ehtiva etməlidir. Maliyyə institutları informasiya texnologiyaları üzrə insidentlərin təsir dairəsini azaltmaq və riskləri mitiqasiya etmək məqsədilə detallı olaraq hazırlanmış və sınaqdan keçirilmiş insidentlərə reaksiya planları və proseslərini tətbiq etməlidir.

Kiber risklərin idarə edilməsi üzrə AMB-nin gözləntiləri:

İnformasiya texnologiyaları üzrə risklərin idarə edilməsi:

1. Maliyyə institutu tərəfindən informasiya texnologiyaları üzrə risklərin idarə edilməsi çərçivəsinin hazırlaması, tətbiq edilməsi, davamlı yenilənməsi və kommunikasiya edilməsi;
2. Maliyyə institutunda kənar kontragentlər tərəfindən göstərilən xidmətlər üzrə dəqiq və aydın şəkildə vəzifə və səlahiyyətlərin bölgüsünun aparılması, fəaliyyətə nəzarət və risk qiymətləndirilməsi prosesinin həyata keçirilməsi;
3. İnformasiya texnologiyaları aktivləri üzrə biznesə təsir analizinin həyata keçirilməsi, təsnifləşdirilməsi, qeydiyyatının aparılması və davamlı olaraq aktuallaşdırılması;
4. İnformasiya texnologiyaları üzrə risklərin aktual siyahısının (risk reyestri) tərtib edilməsi və davamlı yenilənməsi;
5. Proaktiv idarəetmənin təmin edilməsi məqsədilə reyestrdə qeydiyyatı aparılan risklərin prioritetləşdirilməsi və risklər üzrə zəruri detalların qeyd edilməsi;
6. Kiber risklərin minimallaşdırılması məqsədilə rəhbərlik tərəfindən təsdiq edilən, davamlı olaraq yenilənən strukturlaşmış və sənədləşdirilmiş mitiqasiya planının olması;
7. Maliyyə institutunda informasiya texnologiyaları üzrə insidentlərin müəyyən edilməsi, kommunikasiyası və eskalasiyası üzrə adekvat idarəetmə proseslərinin tətbiq edilməsi;

8. Maliyyə institutunda davamlı olaraq informasiya texnologiyaları üzrə nəzarət mexanizmlərinin müstəqil yoxlanılması, həmçinin təşkilatın informasiya və kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi və müdaxilə sınaq yoxlamalarının aparılması.

Fəaliyyətin bərpası və əməliyyatların davamlılığı üzrə planlaşdırma:

1. Fəaliyyətin bərpası və əməliyyatların davamlılığı üzrə fəaliyyətin planlaşdırılması, testləşdirilməsi və tətbiqi üzrə adekvat resursların cəlb edilməsi;
2. Fövqəladə hallar zamanı maliyyə institutunda informasiya texnologiyaları infrastrukturunun bərpası və biznes əməliyyatlarının davamlığının təmin edilməsi məqsədi ilə Fəaliyyətin Bərpa və Əməliyyatların Davamlığı Planlarının hazırlanması və tətbiqi;
3. Maliyyə institutunda Fəaliyyətin Bərpa və Əməliyyatların Davamlığı Planları hazırlanarkən müxtəlif fövqəladə hadisə və qəza ssenariləri, o cümlədən kibertəhlükəsizlik hadisələrinin nəzərə alınması;
4. Kibertəhlükəsizlik insidenti zamanı sənədləşdirilmiş bərpa planına müvafiq olaraq kritik əməliyyatların davamlılığının təmin edilməsi imkanının yaradılması;
5. Maliyyə institutlarında kritik informasiya sistemlərinin bərpa prosesinin düzgün yerinə yetirilməsinin yoxlanılması məqsədilə kritik məlumatların bərpası proses(lər)inin hazırlanması, həmçinin periodik olaraq məlumatların ehtiyat surətlərdən bərpası sınaqlarının aparılması;
6. Müxtəlif ssenarilərə əsaslanan Fəaliyyətin Bərpa və Əməliyyatların Davamlığı Planları üzrə sınaq yoxlamalarının həyata keçirilməsi və nəticələri barədə Şuranın periodik olaraq məlumatlandırılması.

5.3. Strateji prioritet 3: Maliyyə bazarlarında kibertəhlükəsizlik səviyyəsinin gücləndirilməsi məqsədilə informasiya texnologiyalarının idarəetmə çərçivəsinin formalaşdırılması

AMB-nin daxili və xarici kibertəhlükəsizlik fəaliyyətləri, xüsusilə AMB-nin mandatından irəli gələn funksiyaların dəstəklənməsinə xidmət edən kritik informasiya sistemlərinin, o cümlədən ödəniş sistemləri, klirinq və hesablaşmar sistemlərinin təhlükəsizliyinin təmin edilməsi üzrə fəaliyyətlər öz aralarında qarşılıqlı əlaqəlidir. Bu xüsusda dövlət – özəl

sektorları arasında sıx tərəfdaşlıq münasibətləri mühüm əhəmiyyətə malikdir. İnformasiya mübadiləsi bütün tərəflərə maliyyə sistemində potensial olaraq mövcud olan kiber boşluqlar və riskləri müəyyən etməyə və onları effektiv idarə etməyə imkan verir. Eyni zamanda, bu əməkdaşlıq müəyyən fərdə və ya daha geniş seqmentə yönəlmiş kiberhücumlara adekvat cavab reaksiyasının seçilməsi, həmçinin artıq reallaşmış insidentlər üzrə düzgün bərpa planlarının müəyyən edilməsinə imkan verir.

Bu xüsusda AMB ölkədə fəaliyyət göstərən maliyyə sektorunun iştirakçıları, həmçinin kiber risklərin idarə edilməsinə məsul olan dövlət təhlükəsizlik təşkilatları və müvafiq assosiasiyalarla əməkdaşlıq etməkdədir. Beynəlxalq müstəvidə isə AMB kibertəhlükəsizliyin gücləndirilməsi üzrə prioritetlərin düzgün harmonizasiyası məqsədilə bir sıra mərkəzi banklarla əməkdaşlıq edir.

Bu bölmə AMB-nin informasiya təhlükəsizliyinin və risklərin idarə edilməsi ilə əlaqədar hazırki inkişaf yanaşmasını və fəaliyyət istiqamətlərini ehtiva edir. AMB-nin bu istiqamətlərdə təşəbbüsü nəzarət və siyasət çərçivələrinin gücləndirilməsi məqsədilə bilik və bacarıqların dərinləşdirilməsi üzrə fəaliyyəti davam etdirməkdir. Bu sahədə gələcək siyasət çərçivəsinin hazırlanması və tətbiqi ilə bağlı AMB maliyyə institutları və müvafiq tərəfdaşlarla birgə açıq dialoq aparmağa davam edəcəkdir. Belə ki, bu bölmə üç hissəni özündə ehtiva edir: (i) idarəetmə; (ii) risklərin idarə edilməsi; (iii) kibertəhlükəsizlik.

Müşahidə Şurası (Şura) risklərin idarə edilməsi strategiyası və siyasəti çərçivəsində maliyyə institutunun məqsədlərinə və bu məqsədlərə nail olmaq üçün görülən tədbirlərə uyğun olaraq hazırlanmış informasiya təhlükəsizliyi siyasətini təsdiq edir. Eyni zamanda, Şura maliyyə institutunun biznes və informasiya texnologiyaları üzrə strategiyalarının effektiv tətbiqini təmin edir. Əksər maliyyə institutlarında informasiya texnologiyaları kritik biznes funksiyalarını dəstəkləyən və eyni zamanda biznesin inkişafına təkan verən əsas drayverdir. Bu xüsusda informasiya texnologiyaları üzrə strategiya əhatəli olmalı və ümumi biznes strategiyasına uyğunlaşaraq təşkilatın cari və gələcək strateji inkişaf istiqamətlərini dəstəkləməlidir.

Eyni zamanda, maliyyə institutunun informasiya texnologiyaları üzrə risklərin idarə edilməsi çərçivəsi hərtərəfli olmalı və həmin risklərin biznes əməliyyatlarına təsirinin effektiv qiymətləndirilməsinə kömək etməklə yanaşı, kritik biznes əməliyyatlarına təsir göstərən

risklərin mitiqasiyası zamanı düzgün qərarların qəbul edilməsi prosesinin dəstəklənməsi məqsədi daşımalıdır.

Şura səviyyəsində informasiya texnologiyaları üzrə məsələlərə effektiv nəzarət və qərarların qəbul edilməsində aktiv iştirak edilməsi maliyyə institutunda texnoloji və təhlükəsizlik risk mədəniyyətinin formalaşmasına zəmin yaradır. Belə ki, təşkilatda informasiya texnologiyaları üzrə risklərin idarə edilməsi mədəniyyətinin formalaşması üçün "rəhbərliyin düzgün ton"unun olması xüsusi əhəmiyyətə malikdir.

İnformasiya texnologiyalarının idarəetmə çərçivəsinin formalaşadırılması üzrə AMB-nin gözləntiləri:

1. Maliyyə institutu tərəfindən ümumi biznes strategiyasını dəstəkləyən əhatəli informasiya texnologiyaları strategiyasının hazırlanması və təsdiq edilməsi;
2. Biznes-yönümlü informasiya texnologiyaları strategiyasının icrası məqsədilə adekvat resursların, o cümlədən büdcə, insan və bacarıqların ayrılması;
3. Şuraya informasiya texnologiyaları üzrə strateji təşəbbüslərin icrası zamanı zəruri məsələlər, prioritetlər, həmçinin informasiya təhlükəsizliyi üzrə insidentlər və risklər barədə davamlı hesabatlılığın təqdim olunması;
4. Şuranın və ümumilikdə rəhbərliyin maliyyə institutunun üzləşdiyi informasiya texnologiyaları üzrə risklər barədə qənaətbəxş səviyyədə bilik və anlayışlarının olması, eyni zamanda həmin risklərin düzgün idarə edilməsinin və nəzarət qurumuna kommunikasiyasının təmin edilməsi;
5. Maliyyə institutunda informasiya texnologiyaları üzrə risklərin effektiv idarə edilməsi məqsədilə adekvat informasiya texnologiyaları üzrə idarəetmə strukturunun olması;
6. Maliyyə institutunda informasiya texnologiyaları üzrə sənədləşdirilmiş siyasət, prosedur və qaydaların mövcud olması;
7. Maliyyə institutunda informasiya texnologiyaları üzrə risklərin idarə edilməsi, o cümlədən fövqəladə və krizis hallarında qərarların qəbul olunması üzrə vəzifə və səlahiyyətlərin aydın şəkildə müəyyən edilməsi və müvafiq tərəflərə effektiv kommunikasiyası;
8. Xarici maliyyə institutlarının yerli nümayəndəlikləri xarici maliyyə institutlarının qəbul etdiyi informasiya texnologiyaları strategiyasını və idarəetmə çərçivələrini

Azərbaycanın yerli qanunvericiliyinə və nəzarət orqanı tərəfindən müəyyən edilmiş qaydalara uyğunlaşdıraraq tətbiq edilməsi;

9. Maliyyə institutunun idarəetmə strukturu tərəfindən informasiya texnologiyaları üzrə risklərin idarəetmə, daxili nəzarət və ümumilikdə idarəetmə proseslərinin effektiv təşkili üzrə əminliyin olması.

5.4. Strateji prioritet 4: Maliyyə bazarlarında kiber dayanıqlığın gücləndirilməsi

Kiberhücumların tezliyinin artması və hədəf-yönümlü olması səbəbindən maliyyə institutları getdikcə daha çox kiberhücumlara məruz qalır, həmçinin bu kimi kibertəhdidlərin qarşısını almaq və müvafiq riskləri mitiqasiya etmək daha da mürəkkəbləşir. Bundan əlavə, hazırkı və uzun müddətli texnoloji meyllər (məsələn, bulud texnologiyaları, böyük verilənlər, mobil qurğular, maliyyə texnologiyaları və əşyaların interneti texnologiyaları) kiber riskləri daha da intensivləşdirəcəkdir. Təşkilatlarda çox sayda qarşılıqlı əlaqəli risk və həssaslıqları idarə etməyin tələb olduğu bir zamanda rəqəmsal cəmiyyətin fəaliyyət istiqamətlərindən irəli gələn texniki mürəkkəbliklər əhəmiyyətli çağırışlara səbəb olur. Bu xüsusda kiber risklərin effektiv idarə edilməsi üçün maliyyə institutları adekvat mitiqasiya-nəzarət mexanizmləri tətbiq etməlidirlər. Bu təhdidlərlə mübarizə aparmağın “universal” həllinin və ya yanaşmasının olmadığını nəzərə alaraq maliyyə institutları reallaşmış kiberhücumların yarada biləcəyi neqativ təsir və nəticələri öncədən təhlil etməlidirlər. İnformasiya texnologiyaları üzrə risklərin idarə edilməsi çərçivəsinin kiber risklərin idarə edilməsi elementləri, o cümlədən müvafiq siyasət və prosedurlar statik hesab edilməməlidir. Bu səbəbdən maliyyə institutları təhlükəsizlik təhdidlərinin qarşısını proaktiv qaydada almaq məqsədilə texnoloji infrastrukturlarını, həmçinin müvafiq təhlükəsizlik siyasətlərini müntəzəm nəzərdən keçirməli və yeniləməlidirlər. Bu baxımdan informasiya sistemlərinin, tətbiqi-proqram təminatlarının, verilənlərin və şəbəkə sistemlərinin təhlükəsizliyini aktiv şəkildə təmin etməklə maliyyə institutları təhlükəsizlik insidentlərinin reallaşması tezliyini azalda bilər. İnsidentlərin idarə edilməsi üzrə adekvat bacarıqların yaradılması, o cümlədən insidentlərin aradan qaldırılması üzrə planların mövcudluğu təhlükəsizlik insidentlərinin təsirlərini minimallaşdırmağa imkan verir. Bununla yanaşı, maliyyə institutlarında informasiya təhlükəsizliyi üzrə maarifləndirilmənin zəif olması kiber risklərin artmasına səbəb olan amillərdəndir. Belə ki, maliyyə institutlarında davamlı olaraq müvafiq təlimlərin

keçirilməsi və istifadəçilərin təhlükəsizlik səlahiyyətlərinə nəzarətin gücləndirilməsi ilə təşkilat daxili təhlükəsizlik mədəniyyətini təşviq etmək mümkündür.

Kiber dayanıqlığın gücləndirilməsi üzrə AMB-nin gözləntiləri:

1. Kiber risklərin informasiya texnologiyaları üzrə risklərin idarə edilməsi kontekstində nəzərə alınması;
2. Maliyyə institutunda informasiya təhlükəsizliyi və kibertəhlükəsizlik risklərinin effektiv idarə edilməsini dəstəkləyən davamlı yenilənən prosedur və qaydaların mövcud olması və təsdiq edilməsi;
3. Təşkilat daxilində kibertəhlükəsizlik vəzifələrinin və səlahiyyətlərinin müəyyən edilməsi, sənədləşdirilməsi və müvafiq tərəflərlə kommunikasiya edilməsi;
4. Maliyyə institutu tərəfindən informasiya təhlükəsizliyi üzrə təlim proqramının hazırlanması və tətbiq edilməsi;
5. Kiber risklərin idarə edilməsi üzrə ən azı aşağıdakıların nəzərə alınması:
   - Təhdidlərin, boşluqların və risklərin müəyyən edilməsi, həmçinin maliyyə institutuna təsir aspektlərinin qiymətləndirilməsi;
   - Təhlükəsizlik hadisələrinin və insidentlərinin müəyyən edilməsi və onlara adekvat cavab reaksiyasının verilməsi, o cümlədən baş verdiyi halda təsirinin azaldılması fonunda insidentlərin effektiv idarəedilməsi;
   - Təhlükəsizlik insidenti baş verdikdən dərhal sonra zərurət olduqda, əməliyyatların davamlılığının təmin edilməsi məqsədilə fəaliyyətin bərpası planlarının tətbiq edilməsi.
6. Daxili və xarici təhdidlər müəyyən edilməklə bərabər kiber risk qiymətləndirilməsinin periodik olaraq həyata keçirilməsi;
7. Kibertəhlükəsizlik hadisələrinin və insidentlərinin qarşısını almaq məqsədilə zəruri təhlükəsizlik tədbirlərinin həyata keçirilməsi;
8. Maliyyə institutunda saxlanılan, emal edilən və ötürülən məlumatların (habelə fərdi məlumatların) təsnifatlaşdırılması üzrə proseslərin hazırlanması, tətbiq edilməsi və aktuallaşdırılması, eyni zamanda konfidensial, məxfi və açıq məlumatların düzgün müəyyən edilməsi və adekvat təhlükəsizlik tədbirlərinin tətbiq olunması;
9. Maliyyə institutunda informasiya sistemlərinə daxildən və kənardan edilən girişlərin idarə edilməsi mexanizmlərinin tətbiq edilməsi;

10. İnformasiya sistemlərinə və aktivlərə nəzarət mexanizmlərinin tətbiq edilməsi, o cümlədən təhlükəsizlik hadisələrinin və insidentlərinin zamanında aşkar edilməsi üçün prediktiv indikatorların tətbiqi və aşkaretmə mexanizmlərinin effektivliyinin periodik olaraq yoxlanılması;
11. Maliyyə institutlarının həm daxili insan resursları hesabına, həm də etibarlı kənar kontragentlər tərəfindən müdaxilə sınaq yoxlamalarının keçirilməsi;
12. Maliyyə institutunda qeydə alınmış təhlükəsizlik insidenti zamanı özündə sistematik və kompleks tədbirləri ehtiva edən cavab reaksiyalarının və insidentlərdən bərpa planının hazırlanması və tətbiqi;
13. Kibertəhlükəsizlik insidentləri nəticəsində müəyyən edilən “tapıntılar” əsasında bilik bazasının formalaşdırılması, insidentlərə cavab reaksiyalarının və bərpa planlarının davamlı olaraq aktuallaşdırılması.

5.5. Strateji prioritet 5: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması

Kibertəhlükəsizlik və informasiya təhlükəsizliyi mədəniyyətinin davamlı olaraq inkişaf etdirilməsi daim rəqəmsallaşan maliyyə-bank sektorunun mühüm istiqamətlərindən birinə çevrilmişdir. Təqdim olunan xidmətlərin əlçatanlığının artırılması üçün maliyyə institutları getdikcə texnologiyaya daha çox üstünlük verir və nəticədə artan kibertəhdidlər və hücumlar fonunda onları kiber risklərə münasibətdə daha həssas edir. Bu da öz növbəsində maliyyə itkilərinə, reputasiyanın zədələnməsinə və müştərilərin etibarının itirilməsinə səbəb ola bilər. Bu xüsusda, maliyyə bazarlarında müştəri məlumatlarının (o cümlədən fərdi məlumatların) qorunması və maliyyə fırıldaqçılığının qarşısının alınması üçün informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə proaktiv tədbirlərin həyata keçirilməsi mühüm əhəmiyyətə malikdir.

Bu kontekstdə AMB maliyyə institutlarının effektiv kibertəhlükəsizlik təcrübələrinin yaradılmasında və müvafiq qaydalara və standartlara əməl etməsində mühüm rol oynayır. AMB maliyyə bazarlarında kibertəhlükəsizlik tədbirlərinin sürətləndirilməsi və güclü informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması istiqamətində maliyyə institutları ilə birgə fəaliyyət göstərəcəkdir. Bu istiqamətdə aparılan işlər çərçivəsində maliyyə institutları və aidiyyəti qurumlarla sıx kommunikasiyada güclü kibergigiyena təcrübələrinin yaradılması, kibertəhlükəsizlik üzrə maarifləndirmə proqramlarının həyata keçirilməsi, kibertəhlükəsizlik

üzrə təlim keçmiş və sertifikatlaşdırılmış ekspertlərin hazırlanması və digər təhlükəsizlik tədbirlərinin realizasiyası nəzərdə tutulmuşdur. Nəticədə, bu gözləntiləri qarşılamaqla, maliyyə institutları maliyyə sisteminə etibarı artıra və inamı təşviq edən təhlükəsiz mühiti yarada biləcəkdir.

İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması üzrə AMB-nin gözləntiləri:

1. Kibertəhdidləri müəyyən etmək və təsirlərini minimallaşdırmaq üçün maliyyə institutları və aidiyyəti qurumlar ilə əməkdaşlıq etməklə effektiv koordinasiyasının təşkil edilməsi;
2. Maliyyə sisteminin sabitliyinin təmin edilməsi məqsədilə güclü kibergigiyena mühitinin yaradılması;
3. Maliyyə institutlarında heyətin və müştərilərin kibertəhlükəsizlik məlumatlılığını artırmaq üçün proqramların və təşəbbüslərin həyata keçirilməsi;
4. Maliyyə sektorunun kiber dayanıqlığının təmin edilməsi üçün müvafiq sahələr üzrə təlim keçmiş və sertifikatlaşdırılmış kibertəhlükəsizlik ekspertlərinin yetişdirilməsi;
5. Maliyyə bazarlarında təqdim olunan maliyyə xidmətlərinə inamın artırılması məqsədilə kibertəhlükəsizlik insidentlərindən sığortalanma təcrübələrinin araşdırılması və tətbiq edilməsi ehtimallarının qiymətləndirilməsi.

6. Gözlənilən nəticələr

Strategiya üzrə nəzərdə tutulmuş tədbirlərin effektiv icrası **1)** maliyyə sektorunun sabitliyini gücləndirməyə, **2)** kibertəhlükəsizlik tədbirlərinin həyata keçirilməsində əməkdaşlığı və kommunikasiyanı inkişaf etdirməyə, **3)** maliyyə institutlarında kibertəhlükəsizlik tədbirlərinin tətbiqini intensivləşdirməyə və müvafiq bacarıqları formalaşdırmağa və **4)** kibertəhdidlərin qarşısının alınması üzrə proaktiv kibertəhlükəsizlik tədbirlərini həyata keçirməyə imkan verəcəkdir. Strategiyanın icrası çərçivəsində gözlənilən əsas nəticələr aşağıdakılardır:

- AMB qarşılıqlı əməkdaşlıq çərçivəsində kibertəhlükəsizlik üzrə dayanıqlıq tədbirlərini həyata keçirməklə maliyyə sisteminin sabitliyin gücləndirilməsini təmin edəcək;
- Ölkənin maliyyə sistemində kibertəhlükəsizlik üzrə risklər müəyyən ediləcək, analiz edilərək sənədləşdiriləcək, o cümlədən kiber risklərin azaldılması üzrə adekvat cavab mexanizmləri tətbiq ediləcək;

- Ölkənin maliyyə sektorunda kibertəhlükəsizlik risklərinin düzgün identifikasiyası, kommunikasiyası və idarə edilməsi məqsədilə milli və beynəlxalq tərəfdaşlarla əməkdaşlıq çərçivələri formalaşdırılacaq;
- Maliyyə sistemində kiber sabitliyin təmin olunması üçün maliyyə bazarları iştirakçıları üzərində effektiv risk yönümlü nəzarət çərçivəsi formalaşdırılacaq. Bu xüsusda kibertəhlükəsizlik siyasətlərini və requlyativ təşəbbüsləri tətbiq etməklə kiber sabitlik gücləndiriləcək;
- AMB dinamik olaraq intensivləşən rəqəmsallaşma üzrə trendlərdən irəli gələn kibertəhdidlərə adekvat cavab reaksiyaları tətbiq edəcək, bu xüsusda özəl və dövlət tərəfdaşlığını inkişaf etdirəcək.

Strategiyanın icrası çərçivəsində AMB tərəfindən illik əsasda beynəlxalq standartların və kibertəhlükəsizlik sahəsində mövcud çərçivə sənədlərinə əsasən sorğular keçiriləcək və maliyyə institutlarında kibertəhlükəsizlik vəziyyəti qiymətləndiriləcəkdir. Bu xüsusda, maliyyə bazarları iştirakçılarının kibertəhlükəsizlik üzrə yetkinlik səviyyəsinin müvafiq hədəf göstəricilərinə çatdırılması nəzərdə tutulmuşdur.

Cədvəl 2: Kibertəhlükəsizlik üzrə əsas fəaliyyət indikatorları

№	Maliyyə bazarlarının seqmentləri	Cari göstərici	Hədəf göstərici (2026-cı il)
1	**Bank sektoru**[9]	2.14	3.5
1.1	*o cümlədən, sistem əhəmiyyətli banklar*	*3.08*	*3.7*
2	**Sığorta sektoru**[10]	1.85	2.5
3	**Kapital bazarları**[11]	-	2.5
4	**Ödəniş bazarı**[12]	2.85	3.5
Maliyyə bazarları üzrə ümumi göstərici		**2.28**	**3.0**

Strategiya çərçivəsində icrası nəzərdə tutulan strateji prioritetlər, tədbirlər, həmçinin nəticə indikatorları Tədbirlər Planında ehtiva edilmişdir.

[9] *Banklar, bank olmayan kredit təşkilatları*
[10] *İSB, sığortaçılar*
[11] *Fond birjası, klirinq təşkilatı, investisiya şirkətləri*
[12] *Ödəniş sistemi operatorları, elektron pul təşkilatları. Bu indikatorun ölçülməsinə ödəniş xidmətləri və ödəniş sistemləri sahəsində qanunvericilik bazası formalaşdıqdan sonra başlanılacaqdır.*

7. Maliyyə bazarları üzrə kibertəhlükəsizlik strategiyasının Tədbirlər Planı

№	Tədbirlərin adı	İcra dövrü	Məsul tərəf(lər)	Nəticə indikatorları		
				ilkin nəticə(lər)	aralıq nəticə(lər)	yekun nəticə(lər)
Strateji prioritet 1: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə tənzimləmə və nəzarət çərçivəsinin gücləndirilməsi						
1.1	**Risk əsaslı nəzarət və tənzimləmə çərçivəsinin formalaşdırılması**					
1.1.1	İnformasiya təhlükəsizliyinin idarə edilməsi qaydalarının əhatə dairəsinin genişləndirilməsi	2023-2024	AMB	Beynəlxalq təcrübənin öyrənilməsi	Maliyyə institutları üzrə informasiya təhlükəsizliyinə dair minimum tələblərin formalaşdırılması	
1.1.2	Maliyyə bazarlarının kibertəhlükəsizlik vəziyyəti üzrə yetkinlik səviyyəsinin qiymətləndirilməsi və hesabatlılığı	2023-2026	AMB	Risk əsaslı nəzarət çərçivəsinin yaradılması	Hərtərəfli və tematik yoxlamaların həyata keçirilməsi	Yetkinlik səviyyəsinin qiymətləndirilməsi və hesabatlığın hazırlanması
1.2	**Kiber sabitliyin təmin edilməsi çərçivəsində maliyyə bazarları üzrə sahəvi CERT-in (FinCERT) yaradılması**					
1.2.1	Maliyyə institutları tərəfindən insidentlərin tərtibi və təqdim edilməsi qaydasının formalaşdırılması	2023-2024	AMB	Maliyyə institutları tərəfindən insidentlərin tərtibi və təqdim edilməsi qaydasının hazırlanması		
1.2.2	Maliyyə bazarlarında insidentlərin mübadiləsi sisteminin yaradılması	2024-2026	AMB, maliyyə institutları	İnsidentlərin təqdim edilməsi üzrə məsul koordinatorların müəyyən olunması	Sistemin yaradılması və istismara verilməsi	İnsidentlər üzrə “bilik bazası”nın formalaşdırılması

1.2.3	Maliyyə bazarları üzrə sahəvi CERT-in (FinCERT) formalaşdırılması	2023-2025	AMB	Qanunvericlik bazasının təkmilləşdirilməsi	Təşkilatdaxili institusional tədbirlərin həyata keçirilməsi	FinCERT-in yaradılması
1.2.4	Maliyyə bazarlarında kibertəhdidlərin analizinin aparılması	2024-2025	AMB, maliyyə institutları	Kiber kəşfiyyat üzrə texniki alətlərin tətbiq edilməsi imkanlarının qiymətləndirilməsi		
Strateji prioritet 2: Maliyyə bazarlarında kiber risklərin idarə edilməsi mədəniyyətinin gücləndirilməsi						
2.1	Kiber risklərin əhatə olunduğu təşkilat daxili risklərin idarəedilməsi çərçivəsinin formalaşdırılması	2024-2026	Maliyyə institutları	Risklərin idarə edilməsi çərçivəsinin formalaşdırılması və kiber risk iştahasının müəyyən edilməsi	Risklərə nəzarət məqsədilə özünüqiymətləndirmə təhlillərinin həyata keçirilməsi	Təşkilat üzrə kiber risklərin müəyyən edilməsi və cavab strategiyalarının formalaşdırılması
2.2	İnformasiya sistemlərinin kritiklik səviyyəsinə müvafiq olaraq təsnifləşdirilməsi	2024-2026	Maliyyə institutları	Biznesə təsir analizinin aparılması	Reyestrin formalaşdırılması	Reyestrin aktuallığının təmin edilməsi
2.3	Fövqəladə hallar zamanı əməliyyatların davamlılığının təmin edilməsi	2024-2026	Maliyyə institutları	Əməliyyatların davamlılığı və bərpa planlarının hazırlanması	Müxtəlif ssenarilər nəzərə alınmaqla əməliyyatların davamlılığı və bərpası üzrə sınaq yoxlamalarının keçirilməsi	
Strateji prioritet 3: Maliyyə bazarlarında kibertəhlükəsizlik səviyyəsinin gücləndirilməsi məqsədilə informasiya texnologiyalarının idarəetmə çərçivəsinin formalaşdırılması						
3.1	Təşkilatın biznes-yönümlü inkişaf hədəflərini dəstəkləyən informasiya texnologiyaları üzrə strategiyasının formalaşdırılması	2023-2024	Maliyyə institutları	İnformasiya texnologiyaları üzrə strategiyanın hazırlanması, təsdiq edilməsi və icra edilməsi		

3.2	İnformasiya texnologiyalarının idarə edilməsi üzrə prosedur və qaydaların hazırlanması	2024-2026	Maliyyə institutları	İnformasiya texnologiyalarının idarə edilməsi proseslərinin sənədləşdirilməsi və tətbiq edilməsi		
Strateji prioritet 4: Maliyyə bazarlarında kiber dayanıqlığın gücləndirilməsi						
4.1	İnformasiya sistemlərinin müasir çağırışlara yönəlmiş kiberhücum və təhdidlərə qarşı dayanıqlı mühafizə sistemlərinin qurulması	Mütəmadi əsasda	Maliyyə institutları	Müasir tələblərə uyğun mühafizə sistemlərinin qurulması	“Sıfır etibar” siyasətinin tətbiq edilməsi	Mühafizə sistemlərinin davamlı olaraq aktuallaşdırılması
4.2	İnsidentlərin idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi	2024-2026	Maliyyə institutları	Qayda və prosedurların hazırlanması	İnsidentlərin monitorinqi və hesabatlığı tədbirlərinin həyata keçirilməsi	İnsidentlər barədə məlumatların aidiyyəti təşkilatlara təqdim edilməsi
4.3	Sistem jurnallarının (loqların) idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi	2024-2026	Maliyyə institutları	Qayda və prosedurların hazırlanması	Fəaliyyətin davamlı olaraq təmin edilməsi	
4.4	Zəifliklərin idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi	2024-2026	Maliyyə institutları	Qayda və prosedurların hazırlanması	Fəaliyyətin davamlı olaraq təmin edilməsi	
4.5	Müdaxilə sınaq yoxlamaları üzrə fəaliyyətin həyata keçirilməsi	2024-2026	Maliyyə institutları	Qayda və prosedurların hazırlanması	Fəaliyyətin davamlı olaraq təmin edilməsi	
4.6	Kibertəhlükəsizlik sahəsi üzrə təcrübəli insan kapitalının formalaşdırılması	Mütəmadi əsasda	Maliyyə institutları	Müvafiq sahə üzrə təlim proqramlarının müəyyən edilməsi və həyata keçirilməsi		Müvafiq sahə üzrə sertifikatlı mütəxəssislərin yetişdirilməsi
Strateji prioritet 5: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması						

5.1	Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik məsələləri üzrə koordinasiyanın gücləndirilməsi	2023	AMB, assosiasiyalar, maliyyə institutları	İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə məsələlərə məsul olan şəxslərdən ibarət işçi qrupunun yaradılması		
5.2	Yerli və beynəlxalq CERT-lərlə əməkdaşlıq münasibətlərinin yaradılması	Mütəmadi əsasda	AMB, yerli və beynəlxalq təşkilatlar	CERT-lərlə əməkdaşlıq çərçivəsinin formalaşdırılması		
5.3	Maliyyə bazarlarında kibergigiyena mühitinin formalaşdırılması	Mütəmadi əsasda	AMB, assosiasiyalar, yerli və xarici təşkilatlar, maliyyə institutları	Maarifləndirmə üzrə prioritet istiqamətlərin müəyyən edilməsi	Kibertəhlükəsizlik üzrə “dəyirmi masa”ların keçirilməsi	Maarifləndirmə tədbirlərinin keçirilməsi
5.4	Kibertəhlükəsizlik üzrə akselerasiya proqramlarının həyata keçirilməsi	Mütəmadi əsasda	AMB, assosiasiyalar, yerli və xarici təşkilatlar, maliyyə institutları	Kibertəhlükəsizlik forumlarının həyata keçirilməsi		Akselerasiya proqramlarının (“hackathon”, “bootcamp” və s.) həyata keçirilməsi
5.5	Maliyyə bazarlarında kibertəhlükəsizlik insidentlərindən sığortalanmanın təşviq edilməsi	2024-2026	AMB, assosiasiyalar, müvafiq maliyyə institutları	Sığorta mexanizminin yaradılması üzrə beynəlxalq təcrübənin öyrənilməsi		Kibertəhlükəsizlik insidentlərindən sığortalanmanın təşviqi

8. Maliyyə bazarları üzrə kibertəhlükəsizlik strategiyasının icrası üzrə Zaman Cədvəli

№	Tədbirlərin adı	2023				2024				2025				2026			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
Strateji prioritet 1: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə tənzimləmə və nəzarət çərçivəsinin gücləndirilməsi																	
1.1	**Risk əsaslı nəzarət və tənzimləmə çərçivəsinin formalaşdırılması**																
1.1.1	*İnformasiya təhlükəsizliyinin idarə edilməsi qaydalarının əhatə dairəsinin genişləndirilməsi*																
	Beynəlxalq təcrübənin öyrənilməsi																
	Maliyyə institutları üzrə informasiya təhlükəsizliyinə dair minimum tələblərin formalaşdırılması																
1.1.2	*Maliyyə bazarlarının kibertəhlükəsizlik vəziyyəti üzrə yetkinlik səviyyəsinin qiymətləndirilməsi və hesabatlılığı*																
	Risk əsaslı nəzarət çərçivəsinin yaradılması																
	Hərtərəfli və tematik yoxlamaların həyata keçirilməsi																
	Yetkinlik səviyyəsinin qiymətləndirilməsi və hesabatlığın hazırlanması																
1.2	**Kiber sabitliyin təmin edilməsi çərçivəsində maliyyə bazarları üzrə sahəvi CERT-in (FinCERT) yaradılması**																
1.2.1	*Maliyyə institutları tərəfindən insidentlərin tərtibi və təqdim edilməsi qaydasının formalaşdırılması*																
	Maliyyə institutları tərəfindən insidentlərin tərtibi və təqdim edilməsi qaydasının hazırlanması																
1.2.2	*Maliyyə bazarlarında insidentlərin mübadiləsi sisteminin yaradılması*																
	İnsidentlərin təqdim edilməsi üzrə məsul koordinatorların müəyyən olunması																

	Sistemin yaradılması və istismara verilməsi																
	İnsidentlər üzrə “bilik bazası”nın formalaşdırılması																
1.2.3	*Maliyyə bazarları üzrə sahəvi CERT-in (FinCERT) formalaşdırılması*																
	Qanunvericlik bazasının təkmilləşdirilməsi																
	Təşkilatdaxili institusional tədbirlərin həyata keçirilməsi																
	FinCERT-in yaradılması																
1.2.4	*Maliyyə bazarlarında kibertəhdidlərin analizinin aparılması*																
	Kiber kəşfiyyat üzrə texniki alətlərin tətbiq edilməsi imkanlarının qiymətləndirilməsi																
Strateji prioritet 2: Maliyyə bazarlarında kiber risklərin idarə edilməsi mədəniyyətinin gücləndirilməsi																	
2.1	**Kiber risklərin əhatə olunduğu təşkilat daxili risklərin idarəedilməsi çərçivəsinin formalaşdırılması**																
	Risklərin idarə edilməsi çərçivəsinin formalaşdırılması və kiber risk iştahasının müəyyən edilməsi																
	Risklərə nəzarət məqsədilə özünüqiymətləndirmə təhlillərinin həyata keçirilməsi																
	Təşkilat üzrə kiber risklərin müəyyən edilməsi və cavab strategiyalarının formalaşdırılması																
2.2	**İnformasiya sistemlərinin kritiklik səviyyəsinə müvafiq olaraq təsnifləşdirilməsi**																
	Biznesə təsir analizinin aparılması																
	Reyestrin formalaşdırılması																
	Reyestrin aktuallığının təmin edilməsi																
2.3	**Fövqəladə hallar zamanı əməliyyatların davamlılığının təmin edilməsi**																

	Əməliyyatların davamlılığı və bərpa planlarının hazırlanması																	
	Müxtəlif ssenarilər nəzərə alınmaqla əməliyyatların davamlılığı və bərpası üzrə sınaq yoxlamalarının keçirilməsi																	
Strateji prioritet 3: Maliyyə bazarlarında kibertəhlükəsizlik səviyyəsinin gücləndirilməsi məqsədilə informasiya texnologiyalarının idarəetmə çərçivəsinin formalaşdırılması																		
3.1	**Təşkilatın biznes-yönümlü inkişaf hədəflərini dəstəkləyən informasiya texnologiyaları üzrə strategiyasının formalaşdırılması**																	
	İnformasiya texnologiyaları üzrə strategiyanın hazırlanması, təsdiq edilməsi və icra edilməsi																	
3.2	**İnformasiya texnologiyalarının idarə edilməsi üzrə prosedur və qaydaların hazırlanması**																	
	İnformasiya texnologiyalarının idarə edilməsi proseslərinin sənədləşdirilməsi və tətbiq edilməsi																	
Strateji prioritet 4: Maliyyə bazarlarında kiber dayanıqlığın gücləndirilməsi																		
4.1	**İnformasiya sistemlərinin müasir çağırışlara yönəlmiş kiberhücum və təhdidlərə qarşı dayanıqlı mühafizə sistemlərinin qurulması**																	
	Müasir tələblərə uyğun mühafizə sistemlərinin qurulması																	
	“Sıfır etibar” siyasətinin tətbiq edilməsi																	
	Mühafizə sistemlərinin davamlı olaraq aktuallaşdırılması																	
4.2	**İnsidentlərin idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi**																	
	Qayda və prosedurların hazırlanması																	
	İnsidentlərin monitorinqi və hesabatlığı tədbirlərinin həyata keçirilməsi																	
	İnsidentlər barədə məlumatların aidiyyəti təşkilatlara təqdim edilməsi																	

4.3	**Sistem jurnallarının (loqların) idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi**																	
	Qayda və prosedurların hazırlanması																	
	Fəaliyyətin davamlı olaraq təmin edilməsi																	
4.4	**Zəifliklərin idarə edilməsi üzrə fəaliyyətin həyata keçirilməsi**																	
	Qayda və prosedurların hazırlanması																	
	Fəaliyyətin davamlı olaraq təmin edilməsi																	
4.5	**Müdaxilə sınaq yoxlamaları üzrə fəaliyyətin həyata keçirilməsi**																	
	Qayda və prosedurların hazırlanması																	
	Fəaliyyətin davamlı olaraq təmin edilməsi																	
4.6	**Kibertəhlükəsizlik sahəsi üzrə təcrübəli insan kapitalının formalaşdırılması**																	
	Müvafiq sahə üzrə təlim proqramlarının müəyyən edilməsi və həyata keçirilməsi																	
	Müvafiq sahə üzrə sertifikatlı mütəxəssislərin yetişdirilməsi																	
Strateji prioritet 5: Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması																		
5.1	**Maliyyə bazarlarında informasiya təhlükəsizliyi və kibertəhlükəsizlik məsələləri üzrə koordinasiyanın gücləndirilməsi**																	
	İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə məsələlərə məsul olan şəxslərdən ibarət işçi qrupunun yaradılması																	
5.2	**Yerli və beynəlxalq CERT-lərlə əməkdaşlıq münasibətlərinin yaradılması**																	
	CERT-lərlə əməkdaşlıq çərçivəsinin formalaşdırılması																	

5.3	**Maliyyə bazarlarında kibergigiyena mühitinin formalaşdırılması**																	
	Kiber maarifləndirmə üzrə prioritet istiqamətlərin müəyyən edilməsi																	
	Kibertəhlükəsizlik üzrə “dəyirmi masa”ların keçirilməsi																	
	Maarifləndirmə tədbirlərinin keçirilməsi																	
5.4	**Kibertəhlükəsizlik üzrə akselerasiya proqramlarının həyata keçirilməsi**																	
	Kibertəhlükəsizlik forumlarının həyata keçirilməsi																	
	Akselerasiya proqramlarının (“hackathon”, “bootcamp” və s.) həyata keçirilməsi																	
5.5	**Maliyyə bazarlarında kibertəhlükəsizlik insidentlərindən sığortalanmanın təşviq edilməsi**																	
	Sığorta mexanizminin yaradılması üzrə beynəlxalq təcrübənin öyrənilməsi																	
	Kibertəhlükəsizlik insidentlərindən sığortalanmanın təşviqi																	