AZƏRBAYCAN RESPUBLİKASININ NAZİRLƏR KABİNETİ

Q Ə R A R

“Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”nın təsdiq edilməsi haqqında

“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə” Azərbaycan Respublikasının 2022-ci il 27 may tarixli 539-VIQD nömrəli Qanununun tətbiqi və Azərbaycan Respublikası Prezidentinin “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə” 1998-ci il 19 iyun tarixli 729 nömrəli və “Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında” 2021-ci il 17 aprel tarixli 1315 nömrəli fərmanlarında dəyişiklik edilməsi barədə” Azərbaycan Respublikası Prezidentinin 2022-ci il 5 iyul tarixli 1738 nömrəli Fərmanının 1.1-ci bəndinin və 2-ci hissəsinin icrasını təmin etmək məqsədilə Azərbaycan Respublikasının Nazirlər Kabineti **qərara alır:**

1. “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları” təsdiq edilsin (əlavə olunur).

2. Bu Qərarda dəyişiklik Azərbaycan Respublikası Prezidentinin 2002-ci il 24 avqust tarixli 772 nömrəli Fərmanı ilə təsdiq edilmiş “İcra hakimiyyəti orqanlarının normativ hüquqi aktlarının hazırlanması və qəbul edilməsi qaydası haqqında Əsasnamə”nin 2.6-1-ci bəndinə uyğun edilə bilər.

Əli Əsədov
Azərbaycan Respublikasının Baş naziri

Bakı şəhəri, 17 iyul 2023-cü il
№ 229

Azərbaycan Respublikası Nazirlər
Kabinetinin 2023-cü il 17 iyul
tarixli 229 nömrəli Qərarı ilə
təsdiq edilmişdir.

Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi

QAYDALARI

1. Ümumi müddəalar

1.1. “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları” (bundan sonra – Qaydalar) “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun 2-ci maddəsinin iyirmi doqquzuncu abzasına, 20-1.3-cü və 20-4.1-ci maddələrinə əsasən hazırlanmışdır və Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydalarını, o cümlədən kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələbləri və kibertəhlükəsizlik xidməti provayderinə, onun işçi heyətinə, texnoloji resurslarına və fəaliyyət proseslərinə dair tələbləri müəyyən edir.

1.2. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində səlahiyyətli orqanın (bundan sonra – səlahiyyətli orqan) funksiyalarını Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti (bundan sonra – Dövlət Təhlükəsizliyi Xidməti), dövlət orqanlarına, dövlət adından yaradılan publik hüquqi şəxslərə, dövlətə məxsus olan hüquqi şəxslərə (bundan sonra – dövlət qurumları) münasibətdə isə Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti (bundan sonra – XRİTDX) ilə birgə həyata keçirir.

1.3. Dövlət sirri təşkil edən məlumatların, habelə fərdi məlumatların toplanılmasını və işlənilməsini həyata keçirən kritik informasiya infrastrukturunun təhlükəsizliyi dövlət sirri və fərdi məlumatlar haqqında qanunvericiliyin tələbləri nəzərə alınmaqla təmin olunur.

2. Əsas anlayışlar

2.1. Bu Qaydalarda istifadə olunan əsas anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. **təhlükəsizlik riski** – təhlükəsizliyi təmin olunan obyektə mümkün təhdidlərin baş verməsinin, bu zaman həmin obyektdəki zəifliklərdən, boşluqlardan və digər uyğunsuzluqlardan istifadə edilməsinin və baş verə biləcək fəsadların birgə ehtimalı;

2.1.2. **təhlükəsizlik üzrə kritik hal** – kritik informasiya infrastrukturu obyektinin fəaliyyətinin yol verilən həddən (müddətdən) artıq dayanması və (və ya) kritik informasiya infrastrukturunun təhlükəsizliyinə dair tələblərin əhəmiyyətli dərəcədə pozulması nəticəsində dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vurulmasına səbəb ola bilən kiberinsident.

2.2. Bu Qaydalarda istifadə olunan digər anlayışlar "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu (bundan sonra – Qanun) və Azərbaycan Respublikasının digər normativ hüquqi aktları ilə müəyyən edilmiş mənaları ifadə edir.

3. Kritik informasiya infrastrukturu obyektlərinin müəyyən edilməsi

3.1. İnformasiya sisteminin, avtomatlaşdırılmış idarəetmə sisteminin və ya informasiya-kommunikasiya şəbəkəsinin funksionallığının pozulmasının Qanunun 20-2.1-ci maddəsində göstərilən nəticələrə səbəb ola bilməsi onun kritik informasiya infrastrukturu obyekti hesab edilməsi üçün əsasdır.

3.2. Kritik informasiya infrastrukturu obyektlərinin siyahısı (bundan sonra – Siyahı) səlahiyyətli orqanın təklifləri əsasında Azərbaycan Respublikasının Nazirlər Kabineti tərəfindən təsdiq edilir.

3.3. İnformasiya sisteminin, avtomatlaşdırılmış idarəetmə sisteminin və ya informasiya-kommunikasiya şəbəkəsinin kritik informasiya infrastrukturu obyekti hesab edilməsi prosesi səlahiyyətli orqan tərəfindən təşkil edilir və aşağıdakı mərhələləri əhatə edir:

3.3.1. dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ya ekologiya sahələri üzrə informasiya sistemləri, avtomatlaşdırılmış idarəetmə sistemləri və informasiya-kommunikasiya şəbəkələri vasitəsilə həyata keçirilən fəaliyyət prosesləri müəyyən edilir;

3.3.2. bu Qaydaların 3.3.1-ci yarımbəndində nəzərdə tutulan fəaliyyət proseslərinin həyata keçirilməsini təmin edən informasiya sistemləri, avtomatlaşdırılmış idarəetmə sistemləri və informasiya-kommunikasiya şəbəkələri müəyyən edilir;

3.3.3. hər bir informasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və informasiya-kommunikasiya şəbəkəsi üzrə onun funksionallığının pozulması nəticəsində vurula biləcək zərər qiymətləndirilir və Qanunun 20-2.1-ci maddəsində göstərilən nəticələrə səbəb ola bilməsi müəyyən edilir;

3.3.4. informasiya sisteminin, avtomatlaşdırılmış idarəetmə sisteminin və ya informasiya-kommunikasiya şəbəkəsinin kritik informasiya infrastrukturu obyekti hesab edilməsinə dair səlahiyyətli orqanın əsaslandırılmış təklifləri Azərbaycan Respublikasının Nazirlər Kabinetinə təqdim olunur.

3.4. İnformasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin sahibləri (istifadəçiləri) kritik informasiya infrastrukturu obyektlərinin müəyyən edilməsi məqsədilə sorğu edilən məlumatları səlahiyyətli orqana 30 (otuz) gün müddətində təqdim etməlidirlər.

3.5. Kritik informasiya infrastrukturu obyektinin statusuna 3 (üç) ildə bir dəfədən gec olmayaraq, habelə həmin obyektin konfiqurasiyasında, funksionallığında və ya uyğun gəlməli olduğu informasiya təhlükəsizliyi üzrə tələblərdə dəyişikliklər olduqda, bu Qaydalara uyğun olaraq yenidən baxılır.

4. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələblər

4.1. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblər kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi və fəaliyyətinin davamlılığının təmin edilməsi məqsədlərinə (hədəflərə) nail olmaq üçün müəyyən edilir. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələblər aşağıdakılardır:

4.1.1. ümumi idarəetmənin təşkili və təhlükəsizlik risklərinin idarə edilməsi məqsədilə:

1. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi və fəaliyyətinin davamlılığına, o cümlədən təhlükəsizlik risklərinin və kiberinsidentlərin idarə olunması məsələlərinə dair təhlükəsizlik prosedurları hazırlanmalı, kritik informasiya infrastrukturu obyektlərinin reyestrində (bundan sonra – Reyestr) yerləşdirilməli və kritik informasiya infrastrukturu obyektlərinin təhlükəsiz və davamlı fəaliyyətinin təmin olunmasında iştirak edən şəxslər: kritik informasiya infrastrukturunun təhlükəsizliyi üzrə müvafiq məsul struktur bölmənin və ya təhlükəsizlik əməliyyatları mərkəzinin rəhbəri və əməkdaşları, o cümlədən kritik informasiya infrastrukturunun təhlükəsizliyi üzrə məsul

şəxs, sistem inzibatçısı, mühafizəçi (bundan sonra – aidiyyəti şəxslər) müvafiq təhlükəsizlik prosedurları ilə tanış edilməlidirlər;

2. təhlükəsizlik riskləri müəyyən olunmalı, qiymətləndirilməli və aidiyyəti şəxslər həmin risklər və onların idarə edilməsi barədə məlumatlandırılmalıdırlar;

3. kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması ilə bağlı səlahiyyətlər müəyyən edilməli, vəzifə bölgüsü aparılmalı və kritik informasiya infrastrukturu obyektinin fəaliyyəti üçün təhlükə yaradan hadisələr zamanı həmin vəzifələri icra edən şəxslərin və onlar barəsindəki məlumatların əlçatanlığı təmin olunmalı, həmin məlumatlar (o cümlədən aidiyyəti şəxslərin əlaqə məlumatları) Reyestrdə yerləşdirilməli və aktuallığı təmin edilməlidir;

4. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə və fəaliyyətinin davamlılığına təsir edə biləcək üçüncü tərəflərlə (informasiya texnologiyaları məhsulları, informasiya texnologiyaları xidmətləri, digər hüquqi şəxsin xidmətlərindən istifadə etməklə həyata keçirilən fəaliyyət, texniki dəstək, çağrı mərkəzləri, qarşılıqlı əlaqə (inteqrasiya) və s. üzrə) bağlanılmış müqavilələrə təhlükəsizliklə bağlı şərtlər (tələblər) daxil edilməlidir;

4.1.2. insan resurslarına dair təhlükəsizliyin təmin olunması məqsədilə:

1. aidiyyəti şəxslər təhlükəsizlik məsələləri üzrə zəruri məlumat, bilik və bacarıqlara sahib olmalı, müvafiq proqram üzrə mütəmadi olaraq təlimlərə və maarifləndirici tədbirlərə cəlb edilməli və bunlara dair təsdiqedici sənədlər Reyestrdə yerləşdirilməlidir;

2. işə qəbul olunan əməkdaşlar təhlükəsizlik prosedurları ilə bağlı məlumatlandırılmalı, kritik informasiya infrastrukturu obyektinin təhlükəsizliyinə dair əldə edilmiş məlumatların açıqlanmaması ilə bağlı öhdəlik sənədini imzalamalı, əmək münasibətlərinə xitam verilməsi və ya dəyişdirilməsi halında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması məqsədilə kritik informasiya infrastrukturu obyektinə aid aktivlərin kritik informasiya infrastrukturu subyektinə geri qaytarılması, o cümlədən fəaliyyəti ilə əlaqədar informasiya ehtiyatlarında və sistemlərində bütün sahib olduğu xidməti hesabların fəaliyyətsizləşdirilməsi (“deaktiv” edilməsi və ya hesaba daxil olmaq üçün tələb edilən məlumatlarının dəyişdirilməsi) dərhal təmin edilməlidir;

4.1.3. kritik informasiya infrastrukturu obyektlərinin fiziki və informasiya təhlükəsizliyinin təmin edilməsi məqsədilə:

1. kritik informasiya infrastrukturu obyektlərinin yerləşdiyi və ona aid olan ərazi və binalara, o cümlədən server, kommutasiya və digər otaqlara və ya kritik informasiya infrastrukturu obyektlərinə birbaşa fiziki qoşulmaya imkan verən məkanlara icazəsiz fiziki girişin, habelə zədə və təsirin qarşısının alınması üçün tədbirlər həyata keçirilməlidir;

2. kritik informasiya infrastrukturu obyektinə aid aktivlərin itirilməsi, zədələnməsi, korlanması, qanunsuz olaraq ələ keçirilməsi və ya vəziyyətinin pisləşməsi və kritik informasiya infrastrukturunun fəaliyyətinin pozulmasının qarşısının alınması üçün tədbirlər görülməlidir;

3. təhlükəsizlik üzrə sertifikatlaşdırılmış və lisenziyalı proqram təminatından və proqram-texniki vasitələrdən istifadə edilməli, məlumatlarla, o cümlədən dövlət sirri və ya qanunla qorunan digər sirr təşkil edən məlumatlarla, yaxud fərdi məlumatlarla bağlı informasiya mübadiləsi zamanı müvafiq normativ hüquqi aktların tələblərinə riayət edilməli, təşkilati, texniki və texnoloji tədbirlər həyata keçirilməklə informasiyanın mühafizəsi təmin edilməlidir;

4. kritik informasiya infrastrukturu obyektlərinin davamlı fəaliyyəti üçün zəruri resurslarla (enerji, soyutma və s.) fasiləsiz təchizat təmin edilməlidir;

5. kritik informasiya infrastrukturu obyektlərinə icazəsiz girişlərin qarşısının alınması üçün tədbirlər görülməli, girişlərə nəzarət qaydaları və mexanizmləri formalaşdırılmalı, sənədləşdirilməli və aktuallığı təmin olunmalı, eləcə də bütün uğurlu girişlər və uğursuz cəhdlərin qeydiyyata alınması (loq-faylların aparılması) və uğursuz giriş cəhdləri barədə bildirişlərin avtomatik olaraq kritik informasiya infrastrukturu subyektinin (və ya xidmət alındığı təqdirdə kibertəhlükəsizlik xidməti provayderinin) təhlükəsizlik əməliyyatları mərkəzinə göndərilməsi təmin edilməlidir;

6. kritik informasiya infrastrukturu obyektlərinin informasiya təhlükəsizliyinin təmin edilməsi, qanunsuz müdaxilə hallarının qarşısının alınması, o cümlədən təhlükəsizliyə dair məlumatların konfidensiallığının qorunması məqsədilə tədbirlər həyata keçirilməlidir;

4.1.4. əməliyyatların effektiv idarə edilməsi məqsədilə:

1. kritik informasiya infrastrukturu obyektlərinin təhlükəsiz və davamlı fəaliyyətinin təmin edilməsi üçün zəruri əməliyyat prosedurları və bu prosedurlar üzrə məsuliyyət bölgüsü sənədləşdirilməli və aidiyyəti şəxslər üçün əlçatanlığı təmin edilməlidir;

2. kritik informasiya infrastrukturu obyektləri ilə əlaqədar dəyişikliklərin idarə edilməsi prosesini tənzimləyən prosedurlar hazırlanmalı, sənədləşdirilməli və tətbiqi təmin edilməlidir;

3. kritik informasiya infrastrukturu obyektlərinə aid aktivlər və konfiqurasiyalar müəyyənləşdirilməli, bu aktivlərin inventar qeydiyyatı aparılmalı və mütəmadi yenilənməsi təmin edilməli, o cümlədən bu aktivlərin istifadəsi və onlardan istifadə imkanları monitorinq edilməli, tənzimlənməli və fəaliyyət üzrə potensial ehtiyaclar nəzərə alınmaqla proqnozlaşdırılmalıdır;

4. kritik informasiya infrastrukturu obyektlərinin texniki layihə sənədlərinin ekspertizası təşkil edilməlidir;

4.1.5. kiberinsidentlərin davamlı və effektiv idarə edilməsi məqsədilə:

1. kiberinsidentlərin idarə edilməsi üzrə prosedurlar hazırlanmalı və işçilər üçün əlçatanlığı təmin olunmaqla tətbiq edilməlidir;

2. kiberinsidentlərin aşkar olunması üçün zəruri tədbirlər həyata keçirilməli, kiberinsidentlərin davamlı qeydiyyatı, monitorinqi və kommunikasiyası təmin edilməlidir;

3. kiberinsidentlərə adekvat reaksiyanın verilməsi məqsədilə aydın səlahiyyət bölgüsü və zəruri kommunikasiya kanalları müəyyən edilməli və kiberinsidentlər barədə məlumatlandırma müvafiq idarəetmə kanalları vasitəsilə real vaxt rejimində həyata keçirilməlidir;

4. kiberinsidentlərlə bağlı siyahısı formalaşdırılmış və icrasına nəzarətin həyata keçirildiyi tədbirlər görülməli, kiberinsidentlər qiymətləndirilməli və hadisənin kiberinsident olub-olmaması haqqında qərar qəbul edilməli, kiberinsident aradan qaldırıldıqdan sonra hesabatlılığı aparılmalıdır;

4.1.6. kritik informasiya infrastrukturunun fəaliyyətinin fasilə-sizliyinin təmin edilməsi məqsədilə:

1. fövqəladə hallar zamanı kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin və fəaliyyətinin davamlılığının təmin edilməsi məqsədilə strategiya hazırlanmalı, prosedurlar və idarəetmə üsulları təyin edilməli, sənədləşdirilməli, tətbiq olunmalı və aktuallığı təmin edilməlidir;

2. fövqəladə hallarda kritik informasiya infrastrukturu obyektlərinin fəaliyyətinin davamlılıq planı, eləcə də bərpa planı hazırlanmalı, təsdiq olunmalı, ildə bir dəfə sınağı həyata keçirilməli və sınaq nəticələri Reyestrdə yerləşdirilməlidir;

3. kritik informasiya infrastrukturu obyektinin fəaliyyətinin dayanmasının yol verilən həddi (müddəti) müəyyən olunmalıdır;

4.1.7. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə monitorinq, audit yoxlamaları və müdaxilə sınaqlarının həyata keçirilməsi məqsədilə:

1. bütün kritik informasiya infrastrukturu obyektləri barədə məlumatların Azərbaycan Respublikası Nazirlər Kabinetinin müəyyən etdiyi kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydasına uyğun olaraq Reyestrə daxil edilməsi təmin edilməlidir;

2. kritik informasiya infrastrukturu obyektlərinin fəaliyyətinin fasiləsiz (24/7 rejimdə) monitorinqi və qeydiyyata alınması (loq-faylların aparılması) həyata keçirilməli və hadisə loqları ən azı bir il müddətinə saxlanılmalıdır;

3. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin auditinə dair daxili plan təsdiq edilməli, Reyestrdə yerləşdirilməli və icrası təşkil edilməlidir;

4. kritik informasiya infrastrukturu obyektinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların aşkar olunması məqsədilə müdaxilə sınaqlarının keçirilməsinə dair illik və (və ya) cari plana uyğun olaraq ildə 1 (bir) dəfədən az olmayaraq (bu tədbirlərin keçirilməsindən ən azı 7 (yeddi) gün əvvəl Dövlət Təhlükəsizliyi Xidmətinin Kibertəhlükəsizlik Əməliyyatları Mərkəzini (bundan sonra – Milli kibermərkəz), dövlət qurumlarına münasibətdə həmçinin XRİTDX-nin kibermərkəzini (bundan sonra – Dövlət qurumları üzrə kibermərkəz) məlumatlandırmaqla) müdaxilə sınaqları keçirilməli və nəticələr Reyestrdə yerləşdirilməlidir;

5. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin fasiləsiz (24/7 rejimdə) monitorinqinin kritik informasiya infrastrukturu subyektinin aidiyyəti struktur bölməsi (təhlükəsizlik əməliyyatları mərkəzi) vasitəsilə birbaşa yerində və (və ya) kibertəhlükəsizlik xidməti provayderi vasitəsilə məsafədən həyata keçirilməsi təmin edilməli, əldə olunan məlumatlar, o cümlədən kiberinsidentlər barədə məlumatlar real vaxt rejimində mərkəzləşmiş nəzarət üçün Milli kibermərkəzə, dövlət qurumlarına münasibətdə həmçinin Dövlət qurumları üzrə kibermərkəzə (bundan sonra – aidiyyəti kibermərkəz) təqdim edilməlidir;

6. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasına dair yoxlamaların, habelə kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin

olunması vəziyyətinə real vaxt rejimində mərkəzləşmiş nəzarətin, o cümlədən fasiləsiz (24/7 rejimdə) monitorinqin həyata keçirilməsi üçün zəruri informasiya mənbələri (sübutlar) olan qeydiyyatların formalaşdırılması, bu qeydiyyatlarda kritik informasiya infrastrukturu obyektinin konfiqurasiyası, funksionallığı və onlara aid texniki xidmətlər (qulluqlar) barədə məlumatların müvafiq resurslarda xronoloji toplanılması, onların konfidensiallığı, tamlığı və əlçatanlığı təmin edilməlidir.

5. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə xüsusi tələblərin müəyyən edilməsi

5.1. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə xüsusi tələblər kritik informasiya infrastrukturunun təyinatı və subyektinin fəaliyyət xüsusiyyətlərinə uyğun olaraq kritik informasiya infrastrukturu subyekti tərəfindən müəyyən edilir və Reyestrdə yerləşdirilir.

5.2. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə xüsusi tələblərin müəyyən edilməsi üçün əsas mənbələr aşağıdakılardır:

5.2.1. Qanunun tələbləri;

5.2.2. kritik informasiya infrastrukturu təhlükəsizliyinə dair ümumi tələblər;

5.2.3. informasiya təhlükəsizliyi ilə əlaqəli olan texniki normativ hüquqi aktlar, o cümlədən “Texniki tənzimləmə haqqında” Azərbaycan Respublikası Qanununun 18.2-ci maddəsinə uyğun olaraq hüquqi qüvvəsini saxlamış standartlar;

5.2.4. kritik informasiya infrastrukturu subyektinin informasiya təhlükəsizliyi sahəsində hüquqi aktları, informasiya təhlükəsizliyinə aidiyyəti olan texniki sənədləri, müqavilələri və öhdəlikləri.

5.3. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə xüsusi tələblər müəyyən olunarkən aşağıdakılar nəzərə alınır:

5.3.1. kritik informasiya infrastrukturu obyektinin fəaliyyətinin davamlılığının təmin edilməsi üçün kritik informasiya infrastrukturu obyektlərinin konfiqurasiyasının yararlılıq, yetərlilik və etimadlılıq vəziyyəti;

5.3.2. kritik informasiya infrastrukturu obyektinin yaradılması, istismarı və ləğv edilməsinin idarə olunması vəziyyəti;

5.3.3. kritik informasiya infrastrukturu obyektinin həyata keçirdiyi proseslərin təkmillik səviyyələri;

5.3.4. kritik informasiya infrastrukturu obyektinin həyata keçirdiyi proseslərin subyektləri arasında müvafiq sahələr üzrə vəzifə bölgüsü və onların kompetensiya səviyyələri;

5.3.5. kritik informasiya infrastrukturu obyektinin həyata keçirdiyi proseslərə aid texniki xidmətlərin (qulluqların) razılaşdırma səviyyələri;

5.3.6. təhlükəsizlik tələblərinə riayət olunma səviyyəsi üzrə əvvəlki qiymətləndirmə nəticələri.

6. Kibertəhlükəsizlik xidməti provayderinə, onun işçi heyətinə, texnoloji resurslarına və fəaliyyət proseslərinə dair tələblər

6.1. Kritik informasiya infrastrukturu subyektinə kibertəhlükəsizlik xidmətləri göstərən provayderə dair ümumi tələblər aşağıdakılardır:

6.1.1. provayderin təsisçisi və onun səlahiyyətli nümayəndəsi Azərbaycan Respublikasının vətəndaşı olmalıdır;

6.1.2. provayder kritik informasiya infrastrukturu obyektlərinə xidmət göstərilməsi üçün ayrılmış fiziki məkana sahib olmalıdır;

6.1.3. provayder kritik informasiya infrastrukturu obyektlərinə xidmət göstərən işçi heyətə dair məlumatların Reyestrə daxil edilməsini təmin etməlidir;

6.1.4. provayder kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi tələblərə riayət etməlidir.

6.2. Provayderin kritik informasiya infrastrukturu subyektinə kibertəhlükəsizlik xidmətləri göstərən işçi heyətinə dair tələblər aşağıdakılardır:

6.2.1. provayderin kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətinə rəhbərlik edən şəxs Azərbaycan Respublikasının vətəndaşı olmalı, kibertəhlükəsizlik və ya informasiya təhlükəsizliyi sahəsində zəruri bilik və bacarıqlara, kibertəhlükəsizlik və ya informasiya təhlükəsizliyi sahəsində azı 3 (üç) il iş təcrübəsinə (o cümlədən azı 1 (bir) il idarəetmə təcrübəsinə) malik olmalıdır;

6.2.2. provayderin kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətinə cəlb edilmiş digər əməkdaşları aşağıdakılara uyğun olmalıdırlar:

1. Azərbaycan Respublikasının vətəndaşı olmalıdırlar;

2. informasiya texnologiyaları və ya informasiya təhlükəsizliyi sahəsində zəruri bilik və bacarıqlara malik olmalı, ildə 1 (bir) dəfədən

az olmayaraq kibertəhlükəsizlik üzrə təlimlərə və maarifləndirici tədbirlərə cəlb edilməlidirlər;

3. təhlükəsizlik əməliyyatları mərkəzinin fəaliyyətini və müdaxilə sınaqlarını həyata keçirəcək əməkdaşları informasiya texnologiyaları, kibertəhlükəsizlik və ya informasiya təhlükəsizliyi sahəsində azı 1 (bir) il iş təcrübəsinə malik olmalıdırlar;

4. audit nəticələrini imzası ilə təsdiq edən şəxs informasiya təhlükəsizliyi sahəsində audit fəaliyyəti üzrə azı 1 (bir) il iş təcrübəsinə malik olmalıdır.

6.3. Provayderin texnoloji resurslarına dair tələblər aşağıdakılardır:

6.3.1. provayder kritik informasiya infrastrukturu obyektlərinə fasiləsiz, dayanıqlı və təhlükəsiz xidmət göstərilməsi üçün zəruri texniki-texnoloji infrastruktura (təhlükəsizlik əməliyyatları mərkəzi və zəruri aparat-proqram təminatına, fasiləsiz (24/7 rejimdə) iş şəraitinə, perimetr və fiziki təhlükəsizlik həllərinə və s.) sahib olmalıdır;

6.3.2. kritik informasiya infrastrukturu obyektlərinə xidmətlərin göstərilməsində xarici təchizatçılar və şirkətlərdən alınan həllərlə yanaşı, milli texniki-texnoloji həllərdən istifadə olunmalıdır;

6.3.3. provayderin müvafiq infrastrukturu fasiləsiz xidmətin təmin edilməsi üçün əsas və alternativ texnoloji infrastruktur, eləcə də əsas və alternativ enerji mənbələri ilə təmin olunmalıdır;

6.3.4. provayder təhlükəsizlik üzrə kritik halların səlahiyyətli orqana bildirilməsi üçün şifrələnmiş kommunikasiya (şəbəkə kanalı) imkanlarına malik olmalıdır.

6.4. Provayderin fəaliyyət proseslərinə dair tələblər aşağıdakılardır:

6.4.1. kritik informasiya infrastrukturu obyektlərinə xidmət göstərilməsində istifadə olunan informasiya infrastrukturunun təhlükəsizliyi üçün zəruri tədbirlər görülməlidir;

6.4.2. kritik informasiya infrastrukturu obyektlərinə xidmət üzrə fəaliyyətin digər fəaliyyətlərdən aparat, proqram, təşkilati səviyyələrdə tamamilə təcrid edilməsi (ayrılması) təmin olunmalıdır;

6.4.3. təhlükəsizlik prosedurları mövcud olmalı və aidiyyəti şəxslər bu prosedurlarla tanış edilməlidir;

6.4.4. xidmət göstərilən kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması ilə bağlı səlahiyyətlər müəyyən edilməli, vəzifə bölgüsü aparılmalı və təhlükəsizlik hadisələri zamanı həmin vəzifələri icra edən şəxslərin (və onlar barəsindəki

məlumatların) əlçatanlığı təmin olunmalı, həmin məlumatlar Reyestrdə yerləşdirilməli və aktuallığı təmin edilməlidir;

6.4.5. provayderə məxsus aktivlərin itirilməsi, zədələnməsi, korlanması, qanunsuz olaraq ələ keçirilməsi və ya vəziyyətinin pisləşməsi, həmçinin xidmət göstərilən kritik informasiya infrastrukturu obyektinin fəaliyyətinin pozulmasının qarşısının alınması üçün tədbirlər görülməlidir;

6.4.6. provayderin kritik informasiya infrastrukturu obyektinə xidmət göstərilməsində istifadə olunan informasiya infrastrukturu obyektlərinin informasiya təhlükəsizliyinin təmin edilməsi məqsədilə zəruri tədbirlər həyata keçirilməlidir;

6.4.7. provayderin kritik informasiya infrastrukturuna xidmət göstərilməsində istifadə olunan informasiya infrastrukturu obyektlərinə münasibətdə baş vermiş kiberinsidentlərin idarə edilməsi üzrə hazırlanmış prosedurlara əsasən həmin kiberinsidentlərin aşkar olunması üçün zəruri tədbirlər həyata keçirilməli, kiberinsidentlərin davamlı qeydiyyatı, monitorinqi və qiymətləndirilməsi, həmçinin kiberinsidentlər barədə məlumatların aidiyyəti kibermərkəzlə operativ mübadiləsi və hesabatlılıq təmin edilməlidir;

6.4.8. fasiləsiz (24/7 rejimdə) təhlükəsizlik əməliyyatları xidməti təşkil olunmalı, kritik informasiya infrastrukturu obyektlərinin fəaliyyətinin fasiləsiz (24/7 rejimdə) monitorinqi, o cümlədən kibertəhdid, kiberhücum və kiberinsidentlərin qeydiyyata alınması (loq-faylların aparılması), həmçinin bu barədə məlumatların aidiyyəti kibermərkəzə göndərilməsi həyata keçirilməlidir;

6.4.9. təhlükəsizlik hadisələri, xətalar, habelə istifadəçilərin fəaliyyəti barədə məlumatlar bir ildən az olmayan müddətdə saxlanılmalıdır;

6.4.10. Milli kibermərkəzlə (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəz vasitəsilə) fasiləsiz məlumat mübadiləsi təmin edilməlidir.

6.5. Provayderin işçi heyəti xidmət göstərilən kritik informasiya infrastrukturu subyekti, onun texnoloji infrastukturu, informasiya ehtiyatları və onlarda olan informasiya barədə əldə olunmuş məlumatların konfidensiallığına görə cavabdehdir.

7. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sistemi

7.1. Kritik informasiya infrastrukturu subyektləri onlara məxsus olan kritik informasiya infrastrukturuna kibertəhdidlərin, kiberhücum-

ların, kiberinsidentlərin, habelə bu əməllərin törədilməsinə cəhdlərin aşkarlanması, qarşısının alınması və zərərli nəticələrinin aradan qaldırılması məqsədilə müvafiq infrastrukturun informasiya təhlükəsizliyini idarəetmə sistemini təşkil edir və onun fəaliyyətini təmin edir.

7.2. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sisteminin tərkibi və fəaliyyət qaydası kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələblər əsasında, kritik informasiya infrastrukturu subyektinin fəaliyyət xüsusiyyətləri nəzərə alınmaqla, onun tərəfindən müəyyən edilir və Reyestrdə yerləşdirilməsi təmin olunur.

7.3. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sisteminin proqram, texniki və mühəndis təminatı vasitələrinin layihə sənədləri kritik informasiya infrastrukturunun layihə sənədlərinin tərkib hissəsidir.

7.4. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sistemi kritik informasiya infrastrukturu obyektlərinin əsas fəaliyyətinə əngəl yaratmamalıdır.

7.5. Kritik informasiya infrastrukturu subyekti səlahiyyətli orqanla qarşılıqlı əlaqələrin operativliyini təmin etmək məqsədilə kritik informasiya infrastrukturunun təhlükəsizliyi üzrə məsul şəxs təyin edir və həmin şəxs barədə məlumatların Reyestrdə yerləşdirilməsi təmin olunur.

7.6. Yeni formalaşdırılan kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sisteminin istismara qəbulu sınaqları kritik informasiya infrastrukturu obyektlərinin istismara qəbul planı əsasında keçirilir.

8. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətin təşkili

8.1. Kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi üzrə fəaliyyətin ümumi təşkili və əlaqələndirilməsi səlahiyyətli orqan tərəfindən həyata keçirilir.

8.2. Dövlət Təhlükəsizliyi Xidmətinin kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması üzrə vəzifələri aşağıdakılardır:

8.2.1. kritik informasiya infrastrukturu təhlükəsizliyinin təmin olunması vəziyyətinə nəzarəti həyata keçirmək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.2. informasiya sisteminin, avtomatlaşdırılmış idarəetmə sisteminin və ya informasiya-kommunikasiya şəbəkəsinin kritik informasiya infrastrukturu obyekti hesab edilməsi prosesini təşkil etmək, həmin obyektlərin Siyahıya daxil edilməsinə və (və ya) Siyahıdan çıxarılmasına dair Azərbaycan Respublikasının Nazirlər Kabinetinə təkliflər vermək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.3. kritik informasiya infrastrukturu obyektlərinin müəyyən olunması məqsədilə informasiya sisteminin, avtomatlaşdırılmış idarəetmə sisteminin və ya informasiya-kommunikasiya şəbəkəsinin sahibindən (istifadəçisindən) bu Qaydaların 3-cü hissəsinə uyğun olaraq məlumatları sorğu etmək;

8.2.4. Reyestrin fəaliyyətini təşkil etmək;

8.2.5. Reyestrə daxil edilmiş kritik informasiya infrastrukturu subyekti olan dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət edilməsinin yoxlanılmasına dair XRİTDX tərəfindən təqdim edilmiş illik planı təsdiq edərək hər il yanvarın 1-dək Reyestrdə yerləşdirilməsini təmin etmək;

8.2.6. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların olub-olmamasının müəyyən edilməsi məqsədilə müdaxilə sınaqlarının keçirilməsinə dair illik və (və ya) cari planları təsdiq etmək;

8.2.7. yoxlama tədbirləri nəticəsində kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin pozulmasına səbəb ola bilən ciddi nöqsanlar aşkar edildikdə, habelə təhlükəsizlik üzrə kritik hal baş verdikdə tədbirlər görmək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.8. kritik informasiya infrastrukturunun təhlükəsizliyinə yönələn kibertəhdidlərlə mübarizə üzrə əlaqələndirilmiş tədbirlərin görülməsini təşkil etmək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.9. kritik informasiya infrastrukturunun təhlükəsizliyinə yönələn kibertəhdidlərin qarşısının alınması məqsədilə təhlükəsizlik riskləri, zərərverici proqram təminatı, qlobal və lokal xarakterli kiberinsidentlər, kritik informasiya infrastrukturuna münasibətdə törədilmiş kiberhücumlar, cəhdlər və bununla bağlı olan digər məlumatları toplamaq və təhlil etmək, təhdidlərin kritik informasiya infrastrukturunun təhlükəsizliyinə potensial təsirlərini qiymətləndirmək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.10. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə məsul şəxslərdən qarşılaşdıqları informasiya təhlükəsizliyinə dair kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə məlumatları toplamaq, təhdidlərin qabaqlanması, qarşısının alınması və onlarla mübarizə aparılması üçün zəruri olan məlumatları operativ şəkildə onlara vermək, müraciət olunduqda müvafiq tədbirlərin görülməsi üçün köməklik göstərmək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.11. kiberhücumlar, təhlükəsizlik riskləri, zərərverici proqram təminatı və kritik informasiya infrastrukturunun təhlükəsizliyinə digər təhdidlərlə bağlı kritik informasiya infrastrukturu subyektlərinə xəbərdarlıqlar və tövsiyələr vermək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.12. kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sisteminin kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərə uyğunluğunun təmin olunmasını kritik informasiya infrastrukturu subyektindən tələb etmək;

8.2.13. kritik informasiya infrastrukturu subyektinin və provayderin müraciəti olduqda aidiyyəti şəxslərin, habelə provayderin kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətinə cəlb edilən şəxslərin müvafiq olaraq bu Qaydaların 4.1.2-ci yarımbəndinin 1-ci abzasında və 6.2-ci bəndində müəyyən olunmuş müvafiq tələblərə uyğunluğu barədə rəy vermək (dövlət qurumlarına münasibətdə XRİTDX ilə birgə);

8.2.14. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi üzrə xüsusi tələblərin müəyyən edilməsi ilə bağlı tövsiyələr vermək;

8.2.15. bu Qaydalarla müəyyən edilmiş digər vəzifələri yerinə yetirmək.

8.3. XRİTDX-nin dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması üzrə vəzifələri aşağıdakılardır:

8.3.1. Dövlət qurumları üzrə kibermərkəz vasitəsilə dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarəti Dövlət Təhlükəsizliyi Xidməti ilə birgə həyata keçirmək;

8.3.2. dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət edilməsinin yoxlanılmasına dair illik planı hər il dekabrın 20-nə kimi Dövlət Təhlükəsizliyi Xidmətinə təqdim etmək;

8.3.3. Dövlət qurumları üzrə kibermərkəz tərəfindən dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların olub-olmamasının müəyyən edilməsi məqsədilə müdaxilə sınaqlarının keçirilməsinə dair planı təsdiq olunması üçün Dövlət Təhlükəsizliyi Xidmətinə təqdim etmək;

8.3.4. yoxlama tədbirləri nəticəsində dövlət qurumunun kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin pozulmasına səbəb ola bilən ciddi nöqsanlar aşkar edildikdə, habelə təhlükəsizlik üzrə kritik hal baş verdikdə Dövlət Təhlükəsizliyi Xidməti ilə birgə tədbirlər görmək;

8.3.5. dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi üzrə xüsusi tələblərin müəyyən edilməsi ilə bağlı tövsiyələr vermək;

8.3.6. dövlət qurumlarının kritik informasiya infrastrukturu obyektlərini AzStateNet internet və data şəbəkəsi ilə təmin etmək;

8.3.7. bu Qaydalarla müəyyən edilmiş digər vəzifələri yerinə yetirmək.

8.4. Dövlət Təhlükəsizliyi Xidmətinin və XRİTDX-nin (dövlət qurumlarına münasibətdə) kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin edilməsi üzrə hüquqları aşağıdakılardır:

8.4.1. bu Qaydalarla həvalə olunmuş vəzifələrinin icrası üçün kritik informasiya infrastrukturu subyektindən kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması vəziyyətinə dair zəruri məlumatları ödənişsiz, birbaşa və dərhal əldə etmək;

8.4.2. kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sisteminin formalaşdırılması və fəaliyyəti üçün kritik informasiya infrastrukturu subyektinə təşkilati dəstək göstərmək və tövsiyələr vermək;

8.4.3. kritik informasiya infrastrukturu obyektlərinin texniki layihə sənədlərinin ekspertizası, habelə kritik informasiya infrastrukturu obyektlərinin texniki layihə sənədlərinə uyğunluğunun sınaqdan keçirilməsi üçün metodiki tövsiyələr vermək;

8.4.4. vəzifələrinin icrası ilə əlaqədar olaraq normativ hüquqi aktlarda nəzərdə tutulmuş digər hüquqları həyata keçirmək.

8.5. Dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinə münasibətdə bu Qaydaların 8.4.2-8.4.4-cü yarımbəndlərində qeyd olunan hüquqlar qarşılıqlı razılıq əsasında həyata keçirilir.

8.6. Milli kibermərkəzin vəzifələri aşağıdakılardır:

8.6.1. bu Qaydaların 3-cü hissəsinə uyğun olaraq kritik informasiya infrastrukturu obyektinin müəyyən edilməsi ilə bağlı təkliflər hazırlamaq;

8.6.2. Reyestrin aparılması, idarə olunması və inkişaf etdirilməsini təmin etmək (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə);

8.6.3. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə bu Qaydaların 8.9.5-ci yarımbəndində qeyd olunmuş subyektlər vasitəsilə real vaxt rejimində mərkəzləşmiş nəzarəti həyata keçirmək, bunun üçün əldə olunmuş məlumatları mərkəzləşmiş qeydiyyata almaq, toplamaq, sistemləşdirmək və təhlil etmək;

8.6.4. dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət edilməsinin yoxlanılmasına dair Dövlət Təhlükəsizliyi Xidmətinin təsdiq etdiyi planı Reyestrdə yerləşdirmək;

8.6.5. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasını (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə) yoxlamaq;

8.6.6. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarət (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə) etmək;

8.6.7. yoxlama tədbirləri nəticəsində kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin pozulmasına səbəb ola bilən ciddi nöqsanlar aşkar edildikdə, zəruri tədbirlərin görülməsi üçün Dövlət Təhlükəsizliyi Xidmətinin rəhbərliyi qarşısında məsələ qaldırmaq;

8.6.8. kritik informasiya infrastrukturu obyektlərinə qarşı yönəlmiş kibertəhdidlər, kiberhücumlar, habelə kiberinsidentlər barədə məlumatları toplamaq, sistemləşdirmək və təhlilini aparmaq, kiberinsidentlərə qarşı cavab tədbirləri görmək, baş vermiş kiberinsidentlə əlaqədar tədqiqatlar həyata keçirmək (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə), əldə olunmuş nəticələri Dövlət Təhlükəsizliyi Xidmətinin rəhbərliyinə təqdim etmək;

8.6.9. kritik informasiya infrastrukturu subyektlərini kibertəhdidlər, kiberinsidentlər, kiberhücumlar və təhlükəsizlik riskləri, onların təhlilinin nəticələri barədə məlumatlandırmaq;

8.6.10. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi ilə əlaqədar daxil olmuş müraciətlərə (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə) baxmaq;

8.6.11. Dövlət Təhlükəsizliyi Xidmətinin rəhbərliyinin tapşırığı əsasında kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə dair hesabatlar, arayışlar və məlumatlar hazırlamaq;

8.6.12. kritik informasiya infrastrukturunun təhlükəsizliyinə dair tələblərin tətbiqi ilə bağlı məsələlər üzrə kritik informasiya infrastrukturu subyektlərinə yazılı və şifahi şəkildə izahlar vermək, habelə qarşıya çıxan çətinliklərin aradan qaldırılmasına dair metodiki köməklik göstərmək;

8.6.13. Dövlət Təhlükəsizliyi Xidməti tərəfindən həvalə olunmuş digər vəzifələri yerinə yetirmək.

8.7. Dövlət qurumları üzrə kibermərkəzin vəzifələri:

8.7.1. bu Qaydaların 3-cü hissəsinə uyğun olaraq dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin müəyyən edilməsi ilə bağlı aidiyyəti üzrə təkliflər hazırlamaq;

8.7.2. dövlət qurumlarının kritik informasiya infrastrukturu obyektləri ilə bağlı məlumatların bu Qaydaların 4.1.7-ci yarımbəndinin 1-ci abzasında nəzərdə tutulan qaydaya uyğun olaraq Reyestrə təqdim edilməsini təmin etmək, həmin məlumatları yoxlamaq və Reyestr vasitəsilə rəyi təqdim etmək;

8.7.3. dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə bu Qaydaların 8.9.5-ci yarımbəndində qeyd olunmuş subyektlər vasitəsilə real vaxt rejimində mərkəzləşmiş nəzarəti həyata keçirmək, bunun üçün əldə edilmiş məlumatları mərkəzləşmiş qeydiyyata almaq, toplamaq, sistemləşdirmək və təhlil etmək;

8.7.4. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə dövlət qurumları tərəfindən riayət olunmasını yoxlamaq (Milli kibermərkəzlə birgə);

8.7.5. yoxlama tədbirləri nəticəsində kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin pozulmasına səbəb ola bilən ciddi nöqsanlar aşkar edildikdə, zəruri tədbirlərin görülməsi üçün Milli kibermərkəzi məlumatlandırmaq;

8.7.6. dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinə qarşı yönəlmiş kibertəhdidlər, kiberhücumlar, habelə kiberinsidentlər barədə məlumatları toplamaq, sistemləşdirmək və təhlilini aparmaq, kiberinsidentlərə qarşı cavab tədbirləri görmək, baş

vermiş kiberinsidentlə əlaqədar tədqiqatlar həyata keçirmək (Milli kibermərkəzlə birgə);

8.7.7. dövlət qurumu olan kritik informasiya infrastrukturu subyektlərini kibertəhdidlər, kiberhücumlar, kiberinsidentlər və təhlükəsizlik riskləri, onların təhlilinin nəticələri barədə məlumatlandırmaq;

8.7.8. dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi ilə əlaqədar daxil olmuş müraciətlərə baxmaq;

8.7.9. XRİTDX-nin rəhbərliyinin tapşırığı əsasında kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə dair hesabatlar, arayışlar və məlumatlar hazırlamaq;

8.7.10. XRİTDX tərəfindən həvalə olunmuş digər vəzifələri yerinə yetirmək.

8.8. Milli kibermərkəzin (dövlət qurumlarına münasibətdə həmçinin Dövlət qurumları üzrə kibermərkəzin) bu Qaydalarla müəyyən olunmuş vəzifələrini həyata keçirmək üçün aşağıdakı hüquqları vardır:

8.8.1. bu Qaydalarla həvalə olunmuş vəzifələrin icrası üçün kritik informasiya infrastrukturu subyektindən kritik informasiya infrastrukturu təhlükəsizliyinin təmin olunması vəziyyətinə dair məlumatları ödənişsiz, birbaşa və dərhal əldə etmək;

8.8.2. kibertəhdidlərə qarşı mübarizəyə, kiberhücumlara, həmçinin kiberinsidentlərə qarşı cavab tədbirlərinin (adekvat reaksiyanın) həyata keçirilməsinə dəstək vermək, bu tədbirləri təşkil etmək və nəticələrini nəzarətdə saxlamaq;

8.8.3. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların olub-olmamasının müəyyən olunması məqsədilə təsdiq edilmiş illik və (və ya) cari planlar üzrə müdaxilə sınaqlarını həyata keçirmək;

8.8.4. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması üçün kritik informasiya infrastrukturu subyektinə təşkilati dəstək göstərmək;

8.8.5. kritik informasiya infrastrukturu obyektlərinə qarşı yönəlmiş kibertəhdid və kiberhücumların qarşısının alınmasına, nəticələrinin aradan qaldırılmasına dair tövsiyələr vermək;

8.8.6. fəaliyyət istiqamətləri üzrə yerli və beynəlxalq təcrübəni öyrənmək və uyğun təcrübənin tətbiqi ilə bağlı təkliflər vermək;

8.8.7. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi ilə bağlı tələblərin pozulması hallarının aradan qaldırılmasını tələb etmək;

8.8.8. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyi ilə bağlı tələbləri pozmuş şəxslərin məsuliyyətə cəlb edilməsi üçün tədbirlər görmək;

8.8.9. səlahiyyətli orqanın kritik informasiya infrastrukturunun təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığı çərçivəsində xarici dövlətlərlə və beynəlxalq təşkilatlarla məlumat mübadiləsi həyata keçirmək;

8.8.10. vəzifələrinin icrası ilə əlaqədar olaraq normativ hüquqi aktlarda nəzərdə tutulmuş digər hüquqları həyata keçirmək.

8.9. Kritik informasiya infrastrukturu subyekti bu Qaydalara uyğun olaraq aşağıdakı fəaliyyəti həyata keçirir:

8.9.1. bu Qaydaların 3-cü hissəsinə uyğun olaraq kritik informasiya infrastrukturu obyektinin müəyyən olunması üçün sorğu edilmiş məlumatları 30 (otuz) gün müddətində səlahiyyətli orqana təqdim edir;

8.9.2. bilavasitə və (və ya) kibertəhlükəsizlik xidməti provayderi vasitəsilə kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyini ümumi və xüsusi tələblərə uyğun olaraq təşkil edir və həmin tələblərə riayət olunmasına nəzarəti təmin edir;

8.9.3. kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sistemini yaradır, onun funksionallığını təmin edir, təhlükəsizlik risklərinin qiymətləndirilməsini, kiberinsidentlərin monitorinqini və cavab tədbirlərini, bu sistemə aidiyyəti olan digər fəaliyyət sahələri arasında əlaqələndirməni təşkil edir;

8.9.4. kritik informasiya infrastrukturu obyektlərinin fəaliyyətinin davamlılığı üçün yararlılıq, yetərlilik və etimadlılıq dərəcələrinin əvvəlcədən təyin olunmuş hədlər çərçivəsində saxlanılmasını təşkil edir;

8.9.5. kritik informasiya infrastrukturu obyektlərinin təhlükəsizlik əməliyyatları mərkəzinin və ya bu mərkəz olmadığı təqdirdə, həmin subyektin informasiya təhlükəsizliyinə məsul olan struktur bölmə və məsul şəxsin, habelə kibertəhlükəsizlik xidməti provayderinin bu infrastrukturun mühafizəsi üzrə funksiyalarını və öhdəliklərini müəyyən edir;

8.9.6. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinə məsul olan struktur bölmənin və ya təhlükəsizlik əməliyyatları mərkəzinin rəhbəri, yaxud digər məsul şəxs barədə məlumatın Reyestrdə yerləşdirilməsini təmin edir;

8.9.7. kritik informasiya infrastrukturu obyektləri ilə bağlı həyata keçirilən layihələr üzrə informasiya təhlükəsizliyinin təmin olunması məqsədilə səlahiyyətli orqanı məlumatlandırır;

8.9.8. kritik informasiya infrastrukturu obyektlərinin müəyyən edilmiş təhlükəsizlik üzrə tələblərə uyğunluğunu mütəmadi qiymətləndirir və uyğunsuzluqları aradan qaldırır, habelə bu Qaydaların 9-cu hissəsində nəzərdə tutulmuş tədbirlərin həyata keçirilməsi üçün zəruri şərait yaradır;

8.9.9. kritik informasiya infrastrukturu obyektlərinin texniki layihə sənədlərinin ekspertizasını təşkil edir;

8.9.10. kritik informasiya infrastrukturu obyektlərinin texniki layihə sənədlərinə uyğunluğunu sınaqdan keçirir və nəticələrinə dair akt tərtib edir;

8.9.11. kritik informasiya infrastrukturu obyektinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların aşkar olunması məqsədilə bu Qaydaların 9.5-ci bəndinə uyğun olaraq müdaxilə sınaqlarının keçirilməsini təşkil edir;

8.9.12. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin fasiləsiz (24/7 rejimdə) monitorinqinin struktur bölməsi (təhlükəsizlik əməliyyatları mərkəzi) vasitəsilə birbaşa yerində və (və ya) kibertəhlükəsizlik xidməti provayderi vasitəsilə məsafədən həyata keçirilməsini təmin edir, əldə olunan məlumatları real vaxt rejimində mərkəzləşmiş nəzarət üçün aidiyyəti kibermərkəzə təqdim edir;

8.9.13. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin auditinə dair daxili planı təsdiq edir və icrasını təşkil edir;

8.9.14. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasına dair yoxlamaların, habelə real vaxt rejimində mərkəzləşmiş nəzarətin, o cümlədən fasiləsiz (24/7 rejimdə) monitorinqin həyata keçirilməsi üçün zəruri informasiya mənbələri (sübutlar) olan qeydiyyatların formalaşdırılmasını, bu qeydiyyatlarda kritik informasiya infrastrukturu obyektinin konfiqurasiyası, funksionallığı və onlara aid texniki xidmətlər (qulluqlar) barədə məlumatların müvafiq resurslarda xronoloji toplanılmasını, onların konfidensiallığını və tamlığını təmin edir;

8.9.15. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasına dair yoxlamaların, xüsusilə də real vaxt rejimində mərkəzləşmiş nəzarətin, o cümlədən fasiləsiz (24/7 rejimdə) monitorinqin həyata keçirilməsi üçün müəyyən edilmiş tələblərə uyğun şərait yaradır, bununla əlaqədar zəruri məlumatların, o cümlədən qeydə alınmış kiberinsidentlər barədə

məlumatların aidiyyəti kibermərkəz tərəfindən ödənişsiz, birbaşa və dərhal əldə olunmasını təmin edir;

8.9.16. kritik informasiya infrastrukturu obyektinə olan kiberhücumlara qarşı cavab tədbirlərinin görülməsi, kibertəhdidlərin və kiberinsidentlərin qarşısının alınması və nəticələrinin aradan qaldırılmasını təmin edir, bu barədə aidiyyəti kibermərkəzi dərhal məlumatlandırır, həmçinin kiberinsidentlərin tədqiqatının tam və hərtərəfli aparılması ilə bağlı aidiyyəti kibermərkəzə zəruri şərait yaradır və dəstək verir;

8.9.17. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərə riayət edilməsi vəziyyətinin öyrənilməsi məqsədilə səlahiyyətli orqandan daxil olan sorğuları təxirəsalınmadan cavablandırır;

8.9.18. bu Qaydaların icrası ilə əlaqədar normativ hüquqi aktlarda nəzərdə tutulmuş digər funksiyaları həyata keçirir.

8.10. Kritik informasiya infrastrukturu obyektlərinə qarşı yönəlmiş kibertəhdidlər, kiberhücumlar, habelə kiberinsidentlərin proqnozlaşdırılması, həmçinin kritik informasiya infrastrukturu obyektlərinin dayanıqlı fəaliyyət göstərməsinə təminat verən tədbirlərin işlənilib hazırlanması məqsədilə əldə edilmiş məlumatlar əsasında Milli kibermərkəz tərəfindən (dövlət qurumlarına münasibətdə Dövlət qurumları üzrə kibermərkəzlə birgə) kritik informasiya infrastrukturu obyektlərində təhlükəsizliyin təmin olunması vəziyyəti qiymətləndirilir və müvafiq hesabat hazırlanaraq səlahiyyətli orqanın rəhbərliyinə təqdim edilir.

9. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət

9.1. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasının təmin edilməsi, o cümlədən bu sahədə kritik informasiya infrastrukturu subyektlərinə kömək göstərilməsi yolu ilə dövlətin və cəmiyyətin qanunla qorunan maraqlarının mühafizəsi məqsədilə səlahiyyətli orqan və kritik informasiya infrastrukturu subyektləri tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət həyata keçirilir.

9.2. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət ümumi və xüsusi tələblərə uyğunluğun qiymətləndirilməsi və aşkar olunan uyğunsuzluqların aradan

qaldırılması, bu tələblərə riayət edilməsinin yoxlanılması, kritik informasiya infrastrukturunun təhlükəsizliyinin fasiləsiz (24/7 rejimdə) monitorinqi, müdaxilə sınaqları və kənar audit yoxlamalarının aparılması vasitəsilə həyata keçirilir.

9.3. Kritik informasiya infrastrukturu obyektinin texniki layihə sənədlərinin uyğunluğunu yoxlama tədbirləri həmin sənədlərin kritik informasiya infrastrukturu subyekti tərəfindən ekspertizası vasitəsilə keçirilir. Kritik informasiya infrastrukturu obyektinin texniki layihə sənədlərinə uyğunluğunun funksional sınağı plan əsasında keçirilir.

9.4. Kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunmasının fasiləsiz (24/7 rejimdə) monitorinqi kritik informasiya infrastrukturu subyektləri tərəfindən təmin edilir və mərkəzləşmiş nəzarəti həyata keçirmək üçün zəruri məlumatlar, o cümlədən kiberinsidentlər barədə məlumatlar real vaxt rejimində aidiyyəti kibermərkəzə göndərilir.

9.5. Müdaxilə sınaqları kritik informasiya infrastrukturu obyektinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların aşkar olunması məqsədilə Dövlət Təhlükəsizliyi Xidməti tərəfindən təsdiq edilmiş plan üzrə aidiyyəti kibermərkəz tərəfindən həyata keçirilir. Kritik informasiya infrastrukturu subyekti tərəfindən kritik informasiya infrastrukturu obyektinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların aşkar olunması məqsədilə müdaxilə sınaqlarının keçirilməsinə dair illik və (və ya) cari plana uyğun olaraq ildə 1 (bir) dəfədən az olmayaraq (bu tədbirlərin keçirilməsindən ən azı 7 (yeddi) gün əvvəl aidiyyəti kibermərkəzi məlumatlandırmaqla), müdaxilə sınaqlarının keçirilməsi təşkil edilir.

9.6. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair tələblərə uyğunluğun təmin edilməsi, o cümlədən informasiya təhlükəsizliyini idarəetmə sisteminin tələblərə müvafiq fəaliyyətini təşkil etmək üçün kritik informasiya infrastrukturu subyektləri ildə bir dəfədən az olmayaraq, kibertəhlükəsizlik xidməti provayderi tərəfindən kənar audit yoxlamalarının keçirilməsini və onun nəticələrinin səlahiyyətli orqana göndərilməsini təmin edir. Kənar audit yoxlamaları təyin olunmuş tələblərə uyğunluq dərəcələrinin qiymətləndirilməsi məqsədilə, habelə proqram, texniki və mühəndis təminatı vasitələrinin yaradılma və istismara qəbul, yenilənmə və təkmilləşdirilmə, tələb olunduqda istismardan çıxarılma mərhələlərində həyata keçirilir.

9.7. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə dövlət qurumu olmayan sahibkarlıq fəaliyyəti subyektləri tərəfindən riayət olunmasının yoxlanılması

həmin sahibkarlıq fəaliyyətinin həyata keçirildiyi obyektlərə gəlmədən aparılır. Milli kibermərkəzin mütəxəssisləri kritik informasiya infrastrukturu təhlükəsizliyi ilə bağlı metodiki köməklik göstərilməsi, məsləhət verilməsi və vəziyyətin qiymətləndirilməsi üçün kritik informasiya infrastrukturu subyektinin dəvəti ilə sahibkarlıq subyektlərinin kritik informasiya infrastrukturu obyektlərinə gələ bilərlər. Bu halda aşkar edilən pozuntulara görə sahibkar məsuliyyətə cəlb edilə bilməz.

9.8. Dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunmasının yoxlanılması Dövlət Təhlükəsizliyi Xidməti tərəfindən təsdiq edilmiş yoxlama planı əsasında keçirilir.

9.9. Dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunmasının həmin qurumların fəaliyyət göstərdikləri yerlərə gəlməklə yoxlanılması müddəti hər bir kritik informasiya infrastrukturu obyekti üzrə 15 (on beş) iş günündən artıq olmamalıdır.

9.10. Bu Qaydaların 9.8-ci bəndində göstərilən yoxlama planından əlavə, dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunmasının yoxlanılması aşağıdakı hallarda keçirilə bilər:

9.10.1. Azərbaycan Respublikası Prezidentinin, Azərbaycan Respublikası Birinci vitse-prezidentinin, Azərbaycan Respublikası vitse-prezidentlərinin və ya Azərbaycan Respublikası Baş nazirinin tapşırığı ilə;

9.10.2. kritik informasiya infrastrukturu obyektlərinə qarşı kibertəhdid, kiberhücum, kiberinsident və ya təhlükəsizlik üzrə kritik hal ilə əlaqədar olaraq, habelə bu barədə aidiyyəti kibermərkəzə daxil olmuş və ya mediada yayımlanan məlumatlar əsasında səlahiyyətli orqanın tapşırığı ilə;

9.10.3. kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunmasının yoxlamanılması zamanı aşkar edilmiş nöqsanların aradan qaldırılması üçün görülmüş tədbirlərin qiymətləndirilməsi məqsədilə;

9.10.4. dövlət qurumunun müraciəti əsasında.

9.11. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunması vəziyyətinin yoxlanılmasının nəticəsi və həmin tələblərə uyğunluğun təmin olunması ilə bağlı görülmüş tədbirlər haqqında səlahiyyətli orqanın rəhbərinə məlumat verilir.

9.12. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunması vəziyyətinin yoxlanılmasını təşkil etmək üçün səlahiyyətli orqan tərəfindən yaradılan komissiyanın tərkibi, yoxlamanın məqsədi, başlanma və qurtarma vaxtı bu Qaydaların 9.8-ci və 9.10-cu bəndlərində qeyd olunan yoxlama planı və ya tapşırıq (müraciət) əsasında müəyyən edilir.

9.13. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə riayət olunması vəziyyətinin yoxlanılması zamanı dövlət qurumunun kritik informasiya infrastrukturu obyektində keçirilmiş sonuncu yoxlama barədə materiallar, təhlükəsizliyin təmin olunması vəziyyətinə dair aidiyyəti kibermərkəzdə olan məlumatlar, o cümlədən baş vermiş kiberhücum və kiberinsidentlər, onların nəticələri, həmçinin görülmüş tədbirlər barədə məlumatlar nəzərə alınır.

9.14. Yoxlama tədbirləri protokollarla, bu tədbirlərin yekun nəticələri isə aktla rəsmiləşdirilir. Yoxlama tədbirlərinə dair protokollar və akt yoxlamada iştirak edən şəxslər tərəfindən imzalanır və komissiyaya rəhbərlik edən şəxs tərəfindən təsdiq edilir. Yoxlama tədbirlərinin yekun nəticəsinə dair aktın nüsxəsi aidiyyəti kritik informasiya infrastrukturu subyektinə göndərilir.

9.15. Kritik informasiya infrastrukturu subyektləri aşkar edilmiş kritik informasiya infrastrukturunun təhlükəsizliyinə dair tələblərin pozulması hallarını təxirəsalınmadan aradan qaldırır və görülmüş tədbirlərin nəticəsi barədə məlumatların Reyestrdə yerləşdirilməsini təmin edir.

9.16. Kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin pozulmasına səbəb ola bilən ciddi nöqsanlar aşkar edildikdə, habelə təhlükəsizlik üzrə kritik hal baş verdikdə, komissiya tərəfindən təxirəsalınmaz tədbirlərin görülməsi məqsədilə səlahiyyətli orqan qarşısında məsələ qaldırıla bilər.

10. Yekun müddəalar

10.1. Bu Qaydalar qüvvəyə mindikdən sonra yaradılan və ya yenilənən (dəyişikliklər aparılan) informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və ya informasiya-kommunikasiya şəbəkələrinin funksionallığının pozulmasının Qanunun 20-2.1-ci maddəsində göstərilən nəticələrə səbəb ola bilməsi həmin sistem və şəbəkələrin layihələndirilməsi mərhələsində onların sahibləri

(istifadəçiləri) tərəfindən müəyyən edilir və bu barədə səlahiyyətli orqana məlumat verilir.

10.2. İnformasiya sistemləri, avtomatlaşdırılmış idarəetmə sistemləri və ya informasiya-kommunikasiya şəbəkələri Siyahıya daxil edildikdən sonra 2 (iki) ay müddətində kritik informasiya infrastrukturu subyektləri tərəfindən həmin obyektlərə dair təhlükəsizlik üzrə xüsusi tələblərin Reyestrin müvafiq bölməsində yerləşdirilməsi təmin edilir.