AZƏRBAYCAN RESPUBLİKASININ NAZİRLƏR KABİNETİ

Q Ə R A R

“Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası”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 1.3-cü bəndinin icrasını təmin etmək məqsədilə Azərbaycan Respublikasının Nazirlər Kabineti **qərara alır:**

1. “Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası” 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
№ 230

Azərbaycan Respublikası Nazirlər
Kabinetinin 2023-cü il 17 iyul
tarixli 230 nömrəli Qərarı ilə
təsdiq edilmişdir.

Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması

QAYDASI

1. Ümumi müddəalar

1.1. “Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası” (bundan sonra – Qayda) “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun 20-2.3-cü maddəsinə əsasən hazırlanmışdır və kritik informasiya infrastrukturu obyektlərinin reyestrinin (bundan sonra – Reyestr) strukturunu, yaradılması və aparılmasının hüquqi, təşkilati və texnoloji əsaslarını müəyyən edir.

1.2. Reyestr kritik informasiya infrastrukturu obyektləri ilə bağlı informasiya proseslərinin (məlumatların yaradılması, toplanılması, işlənilməsi, saxlanılması, axtarışı, mühafizəsi və mübadiləsi) həyata keçirilməsi, eləcə də kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizənin həyata keçirilməsi ilə bağlı tədbirlərin planlaşdırılması və icra olunması məqsədilə təhlillərin aparılması üçün nəzərdə tutulan informasiya sistemidir.

1.3. Reyestrin sahibi (bundan sonra – sahib) normativ hüquqi aktlarla müəyyən edilmiş qaydada Reyestr üzərində sahiblik və istifadə hüququnu həyata keçirən, habelə Reyestrin təşkili və aparılmasını təmin edən Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidmətidir. Dövlət orqanlarına, dövlət adından yaradılan publik hüquqi şəxslərə, dövlətə məxsus olan hüquqi şəxslərə (bundan sonra – dövlət qurumları) münasibətdə Reyestrin təşkili, istifadəsi və aparılmasını sahib Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti ilə birgə həyata keçirir.

1.4. Reyestrin operatoru (bundan sonra – operator) Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidmətinin Kibertəhlükəsizlik Əməliyyatları Mərkəzidir. Dövlət qurumlarına münasibətdə operatorun funksiyası Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin kibermərkəzi ilə birgə həyata keçirilir.

1.5. Reyestrin iştirakçıları (bundan sonra – iştirakçılar) kritik informasiya infrastrukturu subyektləridir.

1.6. Reyestr Azərbaycan Respublikasının mülkiyyətidir.

1.7. Bu Qaydanın məqsədləri üçün istifadə olunan anlayışlar "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda, Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"nda, Azərbaycan Respublikası Nazirlər Kabinetinin müəyyən etdiyi Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydalarında, həmçinin Azərbaycan Respublikasının digər normativ hüquqi aktlarında nəzərdə tutulmuş mənaları ifadə edir.

1.8. Dövlət sirri təşkil edən məlumatların, habelə fərdi məlumatların toplanılması və işlənilməsi dövlət sirri və fərdi məlumatlar haqqında qanunvericiliyin tələbləri nəzərə alınmaqla təmin olunur.

1.9. Reyestrin fəaliyyətinin təşkili, idarə olunması və təkmilləşdirilməsi ilə bağlı zəruri xərclər dövlət büdcəsi və qanunla qadağan olunmayan digər mənbələr hesabına maliyyələşdirilir.

1.10. Reyestrin yaradılmasına, aparılmasına və inteqrasiyasına dair bu Qayda ilə tənzimlənməyən məsələlər Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"na, həmçinin Azərbaycan Respublikası Nazirlər Kabinetinin müəyyən etdiyi Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydalarına, eləcə də Azərbaycan Respublikasının digər normativ hüquqi aktlarına uyğun tənzimlənir.

2. Reyestrin fəaliyyətinin prinsipləri

2.1. Reyestrin yaradılması və aparılması Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"nda müəyyən edilən prinsiplər nəzərə alınmaqla aşağıdakı prinsiplər əsasında həyata keçirilir:

2.1.1. **mütənasiblik** – Reyestrdə görülən tədbirlərin risk səviyyəsinə mütənasib olması;

2.1.2. **operativlik** – Reyestr vasitəsilə məlumat mübadiləsinin mümkün ən qısa müddətdə həyata keçirilməsi;

2.1.3. **funksionallıq və davamlı inkişaf** – Reyestrin inkişaf etdirilməsi imkanını təmin edən proqram-texniki komponentlərin olması, həmçinin ən son texnologiyalardan istifadə edilməklə Reyestrin daim təkmilləşdirilməsi;

2.1.4. **əməkdaşlıq** – Reyestrin fəaliyyətinin təmin edilməsi ilə bağlı sahibin, operatorun və iştirakçıların qarşılıqlı əməkdaşlıq və təhlükəsizlik tədbirlərinin görülməsində fəal iştirak etməsi.

3. Reyestrin texniki-texnoloji infrastrukturu

3.1. Reyestrin texniki-texnoloji infrastrukturu aşağıdakı əsas komponentlərdən ibarətdir:

3.1.1. aparat-texniki vasitələr və proqram təminatı;

3.1.2. telekommunikasiya kanalları və vasitələri;

3.1.3. Reyestrin ehtiyat nüsxəsi;

3.1.4. Reyestrin informasiya ehtiyatı və onun idarəetmə paneli;

3.1.5. “Məlumatların daxil edilməsi” modulu;

3.1.6. “Məlumatlara baxış” modulu;

3.1.7. “Hesabatlar” modulu;

3.1.8. “Reyestr üzrə xəbərdarlıq” modulu;

3.1.9. “Kibertəhdidlərə dair məlumat mübadiləsi” modulu;

3.1.10. “Reyestrin təhlükəsizliyi” modulu;

3.1.11. Reyestrin test mühiti.

3.2. Aparat-texniki vasitələr və proqram təminatı Reyestrin bu Qaydanın 1.2-ci bəndində qeyd edilən funksiyalarının həyata keçirilməsini, fəaliyyətinin etibarlılığını və təhlükəsizliyini təmin edir.

3.3. Reyestr fəaliyyətinin etibarlılığını, təhlükəsizliyini, habelə operativ və keyfiyyətli məlumat mübadiləsini təmin edən dayanıqlı, mühafizəli, yüksək ötürücülü fiber-optik əsas və digər ehtiyat telekommunikasiya kanallarına və vasitələrinə malikdir.

3.4. Reyestrin ehtiyat nüsxəsi informasiya sisteminin sıradan çıxması və ya məlumatların itirilməsi zamanı məlumatların və sistemin işinin bərpa olunması məqsədilə yaradılır.

3.5. Reyestrdə yaradılan, ora daxil və mübadilə edilən məlumatlar Reyestrin informasiya ehtiyatında saxlanılır.

3.6. Reyestrin idarəetmə paneli informasiya ehtiyatlarının formalaşdırılmasını və idarə edilməsini, o cümlədən həmin informasiya ehtiyatlarından istifadəni təmin edir.

3.7. “Məlumatların daxil edilməsi” modulu vasitəsilə bu Qaydanın 4-cü hissəsində qeyd olunan məlumatların daxil edilməsi, “Məlumatlara baxış modulu” vasitəsilə Reyestrdə toplanılmış məlumatlar üzrə axtarış edilməsi və məlumatlara baxılması, “Hesabatlar” modulu vasitəsilə müxtəlif parametrlərə görə hesabatların tərtib olunması təmin edilir.

3.8. “Reyestr üzrə xəbərdarlıq” modulu vasitəsilə aşağıdakılar təmin edilir:

3.8.1. operator və iştirakçılar arasında kritik informasiya infrastrukturunun təhlükəsizliyi üzrə qabaqcıl təcrübə, metodiki dəstək və tövsiyələrin mübadiləsi;

3.8.2. kritik informasiya infrastrukturu obyektləri ilə bağlı həyata keçirilən layihələr üzrə informasiya təhlükəsizliyinin təmin olunması məqsədilə operatorun məlumatlandırılması;

3.8.3. Reyestrin fəaliyyət istiqaməti üzrə operator tərəfindən iştirakçılara sorğuların verilməsi və həmin sorğuların operativ cavablandırılması.

3.9. “Kibertəhdidlərə dair məlumat mübadiləsi” modulu operator və iştirakçılar arasında kibertəhdidlərlə bağlı operativ qaydada və səmərəli şəkildə məlumat mübadiləsinin aparılmasını təmin edir.

3.10. “Reyestrin təhlükəsizliyi” modulu vasitəsilə aşağıdakılar təmin edilir:

3.10.1. çoxfaktorlu mühafizə mexanizmləri ilə təmin olunmuş vahid giriş sistemi vasitəsilə sahibin, operatorun və iştirakçıların eyniləşdirilməsi;

3.10.2. Reyestrə icazəsiz girişlərin qarşısının alınması;

3.10.3. Reyestrə daxil edilmiş məlumatların şifrələnmiş formada saxlanılması;

3.10.4. Reyestrdə aparılmış əməliyyatların qeydiyyata alınması (loq-fayllarının aparılması);

3.10.5. Reyestrin fəaliyyətində informasiyanı mühafizə vasitələrinin tətbiqinin təmin olunması.

3.11. Reyestrdə aparılan dəyişikliklərin yoxlanılması test mühitində həyata keçirilir.

4. Reyestrin strukturu və ona daxil edilən məlumatlar

4.1. Reyestrin strukturu aşağıdakılardan ibarətdir:

4.1.1. kritik informasiya infrastrukturu subyektləri barədə məlumatlar;

4.1.2. kritik informasiya infrastrukturu obyektləri barədə məlumatlar;

4.1.3. kritik informasiya infrastrukturu obyektinin təhlükəsizliyi üzrə xüsusi tələblər, təhlükəsizlik prosedurları və planlar;

4.1.4. kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarət məqsədilə həyata keçirilmiş tədbirlərin nəticələri.

4.2. Reyestrə bu Qaydanın 4.1.1-ci yarımbəndində qeyd edilənlər barədə aşağıdakı məlumatlar daxil edilir:

4.2.1. adı, hüquqi ünvanı, təşkilati-hüquqi forması, VÖEN-i, rəsmi elektron poçt ünvanı, faks və telefon nömrələri;

4.2.2. Reyestrə məsul şəxsin məlumatları (FİN-i, soyadı, adı, ata adı, vəzifəsi, əlaqə məlumatları (rəsmi elektron poçt ünvanı, faks və telefon nömrələri);

4.2.3. informasiya təhlükəsizliyini idarəetmə sisteminin tərkibi və fəaliyyət qaydası.

4.3. Reyestrə bu Qaydanın 4.1.2-ci yarımbəndində qeyd olunanlar barədə aşağıdakı məlumatlar daxil edilir:

4.3.1. kritik informasiya infrastrukturu obyektinin bağlandığı şəbəkə və şəbəkə cihazları, proqram təminatı, kritik informasiya infrastrukturu obyekti ilə əlaqəli xidmətlər, kritik informasiya infrastrukturu obyektinə aid verilənlər bazası və kritik informasiya infrastrukturu obyektinə aid digər aktivlər;

4.3.2. kritik informasiya infrastrukturu obyektinin formalaşdırılma və istifadə məqsədi, o cümlədən təyinatı;

4.3.3. kritik informasiya infrastrukturu obyektinin yerləşdiyi infrastruktur;

4.3.4. kritik informasiya infrastrukturu obyektinin istismar müddəti;

4.3.5. kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin təmin edilməsi ilə bağlı səlahiyyətlər, kritik informasiya infrastrukturu obyektinin təhlükəsiz və davamlı fəaliyyətinin təmin olunmasında iştirak edən şəxslərə: təhlükəsizlik üzrə müvafiq məsul struktur bölmənin və ya təhlükəsizlik əməliyyatları mərkəzinin rəhbərinə və əməkdaşlarına, o cümlədən təhlükəsizlik üzrə məsul şəxsə, sistem inzibatçısına, mühafizəçiyə (bundan sonra – aidiyyəti şəxslər) dair məlumatlar (FİN-i, soyadı, adı, ata adı, vəzifəsi, əlaqə məlumatları (rəsmi elektron poçt ünvanı, faks və telefon nömrələri);

4.3.6. aidiyyəti şəxslərin təhlükəsizlik məsələləri ilə bağlı zəruri məlumat, bilik və bacarıqlara sahib olmalarına, müvafiq proqram üzrə

mütəmadi olaraq təlimlərə və maarifləndirici tədbirlərə cəlb edilmələrinə dair təsdiqedici sənədlər;

4.3.7. kritik informasiya infrastrukturu obyekti ilə bağlı həyata keçirilən layihələr və bağlanılmış müqavilələrə dair məlumatlar;

4.3.8. kritik informasiya infrastrukturu obyektinə kibertəhlükəsizlik xidmətləri göstərildiyi halda provayderə dair məlumatlar (işçi heyəti, səlahiyyətləri, vəzifə bölgüsü, aidiyyəti şəxslərə dair məlumatlar (FİN-i, soyadı, adı, ata adı, əlaqə məlumatları) və s.).

4.4. Reyestrə bu Qaydanın 4.1.3-cü yarımbəndində qeyd olunanlar barədə aşağıdakı məlumatlar daxil edilir:

4.4.1. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə kritik informasiya infrastrukturu subyekti tərəfindən müəyyən edilmiş xüsusi tələblər;

4.4.2. kritik informasiya infrastrukturu obyektinin təhlükəsizliyi və fəaliyyətinin davamlılığına dair təhlükəsizlik prosedurları;

4.4.3. kritik informasiya infrastrukturu obyektinin fəaliyyətinin davamlılıq və bərpa planları;

4.4.4. kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin auditinə dair kritik informasiya infrastrukturu subyektinin daxili planı, o cümlədən audit yoxlamasının həyata keçirilməsində iştirak edəcək şəxslərə dair məlumatlar (FİN-i, soyadı, adı, ata adı, zəruri bilik və bacarıqlarını təsdiq edən sənədlər, əlaqə məlumatları);

4.4.5. kritik informasiya infrastrukturunda təhlükəsizliyə dair boşluqların, zəifliklərin və digər uyğunsuzluqların aşkar olunması məqsədilə kritik informasiya infrastrukturu subyekti tərəfindən təşkil olunacaq müdaxilə sınaqlarına dair plan, o cümlədən müdaxilə sınaqlarının həyata keçirilməsində iştirak edəcək şəxslərə dair məlumatlar (FİN-i, soyadı, adı, ata adı, zəruri bilik və bacarıqlarını təsdiq edən sənədlər, əlaqə məlumatları);

4.4.6. dövlət qurumları tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət edilməsinin yoxlanılmasına dair illik plan.

4.5. Reyestrə bu Qaydanın 4.1.4-cü yarımbəndində qeyd olunanlar barədə aşağıdakı məlumatlar daxil edilir:

4.5.1. kritik informasiya infrastrukturu obyektinin təhlükəsizliyinin auditinə dair daxili planı üzrə kritik informasiya infrastrukturu subyekti tərəfindən həyata keçirilmiş audit yoxlamasının yekun nəticələri;

4.5.2. kritik informasiya infrastrukturunun təhlükəsizliyinə dair kənar audit yoxlamasının yekun nəticələri;

4.5.3. müdaxilə sınaqlarının keçirilməsinə dair plan üzrə kritik informasiya infrastrukturu subyekti tərəfindən təşkil olunmuş müdaxilə sınaqlarının yekun nəticələri;

4.5.4. aşkar edilmiş kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərin pozulması halları ilə əlaqədar görülmüş tədbirlərin nəticəsi barədə məlumatlar;

4.5.5. bu Qaydanın 4.4.3-cü yarımbəndində qeyd olunan planlar üzrə keçirilmiş sınaqların nəticələri;

4.5.6. informasiya təhlükəsizliyini idarəetmə sisteminin qiymətləndirilməsinin nəticələri.

5. Reyestrin aparılması

5.1. Reyestrin fəaliyyətinin təşkili və funskionallığının həyata keçirilməsi kritik informasiya infrastrukturu subyektləri tərəfindən Reyestrə bu Qaydanın 4.2-4.5-ci bəndlərinə uyğun olaraq təqdim edilən məlumatlar əsasında təmin edilir.

5.2. Reyestrə məlumatların təqdim edilməsi operatorun metodiki tövsiyələrinə və təqdim etdiyi nümunələrə uyğun həyata keçirilir.

5.3. İnformasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və ya informasiya-kommunikasiya şəbəkəsi Azərbaycan Respublikası Nazirlər Kabinetinin təsdiq etdiyi kritik informasiya infrastrukturu obyektlərinin siyahısına daxil edildikdən sonra həmin kritik informasiya infrastrukturu subyekti:

5.3.1. Reyestrə məsul şəxsi təyin edir;

5.3.2. bu Qaydanın 4.2-4.5-ci bəndlərində qeyd olunmuş məlumatları müəyyən edərək, məsul şəxs vasitəsilə Reyestrə təqdim edir;

5.3.3. Reyestrə daxil edilmiş məlumatların aktuallığını təmin edir;

5.3.4. operatorun sorğularını operativ cavablandırır.

5.4. Bu Qaydanın 4.2-4.5-ci bəndlərində qeyd olunan məlumatlar Reyestrə təqdim edildikdən sonra operator 15 (on beş) iş günü müddətində həmin məlumatların bu Qaydanın tələblərinə uyğunluğunu yoxlayır. Dövlət qurumlarının kritik informasiya infrastrukturu obyektlərinə münasibətdə kritik informasiya infrastrukturu subyekti tərəfindən Reyestrə təqdim edilmiş məlumatlar Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin kibermərkəzi tərəfindən 10 (on) iş günü müddətində yoxlanılır və hər bir obyekt üzrə rəyi Reyestrdə yerləşdirilir.

5.5. Operator Reyestrə təqdim edilmiş məlumatlarda uyğunsuzluq aşkar etdikdə, həmçinin Reyestrdə dəyişikliklər edilməsi zərurəti yarandıqda və ya oradan çıxarılmalı olan məlumatlar aşkar edildikdə uyğunsuzluğun aradan qaldırılması, o cümlədən müvafiq əlavə və dəyişikliklərin olunması üçün kritik informasiya infrastrukturu subyektinə Reyestr vasitəsilə elektron formada sorğu göndərilir.

5.6. Reyestrə təqdim edilmiş məlumatlarla bağlı bu Qaydanın 5.5-ci bəndində qeyd olunan sorğuya kritik informasiya infrastrukturu subyekti tərəfindən 5 (beş) iş günü müddətində baxılır və yenilənmiş məlumatlar Reyestrə təqdim olunur.

5.7. Reyestrə təqdim edilmiş yenilənmiş məlumatlar bu Qaydanın 5.4-cü bəndinə uyğun olaraq yoxlanılır.

5.8. Reyestrə təqdim olunan məlumatlarda uyğunsuzluq aşkar edilmədikdə, məlumatlar operator tərəfindən təyin edilmiş məsul şəxs tərəfindən təsdiq olunaraq Reyestrə daxil edilir. Reyestrə daxil edilmiş hər bir kritik informasiya infrastrukturu obyektinin avtomatlaşdırılmış rejimdə müvafiq proqram təminatı vasitəsilə verilən təkrarlanmayan (unikal) reyestr nömrəsi, təsdiq edilmə tarixi və vaxtı göstərilir.

5.9. Kritik informasiya infrastrukturu subyektinin Reyestrdən istifadəsi müvafiq internet informasiya ehtiyatında gücləndirilmiş elektron imza vasitəsilə eyniləşdirildikdən sonra Reyestr tərəfindən avtomatik qaydada formalaşdırılan elektron kabineti vasitəsilə həyata keçirilir.

5.10. Kritik informasiya infrastrukturu subyekti bu Qaydanın 4.2-4.5-ci bəndlərində qeyd olunan məlumatları aşağıdakı müddətlərdə elektron kabineti vasitəsilə (təyin etdiyi məsul şəxs vasitəsilə) Reyestrə təqdim edir, habelə həmin məlumatları mütəmadi olaraq yeniləyir:

5.10.1. informasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və ya informasiya-kommunikasiya şəbəkəsinin kritik informasiya infrastrukturunun obyekti kimi bu Qaydanın 5.3-cü bəndində nəzərdə tutulan siyahıda müəyyən edilməsindən sonra Reyestrə daxil edilməsi üçün – 30 (otuz) iş günü müddətində;

5.10.2. kibertəhdid müəyyən edildikdən sonra – dərhal;

5.10.3. kibertəhdidlərə qarşı əks tədbirlər görüldükdən sonra – 1 (bir) iş günü müddətində;

5.10.4. kritik informasiya infrastrukturu obyekti ilə bağlı Reyestrə daxil edilən məlumatlarda hər hansı dəyişiklik olduqda – 5 (beş) iş günü müddətində;

5.10.5. operatorun sorğusu olduqda – bu Qaydanın 5.6-cı bəndində qeyd olunan halda 5 (beş) iş günü müddətində, digər hallarda sorğuda göstərilən müddətdə.

6. Sahibin funksiyaları

6.1. Reyestrin fəaliyyətini təmin etmək üçün sahibin aşağıdakı funksiyaları vardır:

6.1.1. Reyestrin yaradılması, aparılması, istifadəsi, inteqrasiyası, mühafizəsi və arxivləşdirilməsi işlərini layihələrə, texniki reqlamentlərə və normativ hüquqi aktlarla müəyyən edilmiş tələblərə uyğun formada aparmaq;

6.1.2. kibertəhlükəsizlik sahəsində fəaliyyətin təkmilləşdirilməsi məqsədilə beynəlxalq təcrübəni və standartları öyrənmək, bu sahədə ölkədaxili və beynəlxalq qurumlarla (təşkilatlarla) əməkdaşlıq etmək;

6.1.3. Reyestrə çıxışı olan, habelə Reyestrin aparılmasında iştirak edən əməkdaşlarını gücləndirilmiş elektron imza ilə təmin etmək;

6.1.4. tələb edilən sənədlər barədə məlumatlar dövlət informasiya ehtiyatında və sistemində olduqda, həmin məlumatların ilkin mənbədən əldə edilməsi üçün tədbirlər görmək;

6.1.5. Reyestrin dayanıqlı və fasiləsiz fəaliyyətini təmin etmək, habelə Reyestrdə dəyişikliklər və təkmilləşdirmələr aparmaq;

6.1.6. Reyestrdən istifadə və onun funksiyaları ilə bağlı maarifləndirilmə və məlumatlandırılma işləri aparmaq;

6.1.7. informasiya sistemləri, avtomatlaşdırılmış idarəetmə sistemləri və ya informasiya-kommunikasiya şəbəkələri sahiblərinin (istifadəçilərinin) Reyestrin fəaliyyəti ilə bağlı müraciətlərini cavablandırmaq, habelə qeyd edilən müraciətlər əsasında zəruri sənədləri (məlumatları) normativ hüquqi aktların tələblərinə uyğun onlara təqdim etmək.

7. Operatorun funksiyaları

7.1. Operator aşağıdakı funksiyalara malikdir:

7.1.1. bu Qaydaya əsasən Reyestrin fəaliyyətini təşkil etmək, idarə etmək və inkişaf etdirmək;

7.1.2. Reyestrin fəaliyyətinin təmin olunması ilə bağlı zəruri sənədləri (məlumatları) əldə etmək üçün kritik informasiya infrastrukturu subyektlərinə sorğular vermək və həmin subyektlərdən belə sənədləri (məlumatları) almaq;

7.1.3. Reyestrə daxil edilmiş məlumatların mühafizəsi ilə bağlı təşkilati və texniki tədbirlər görmək, həmçinin məlumatların aktuallığını, etibarlılığını, əlçatanlığını, tamlığını, konfidensiallığını, habelə onların ehtiyat surətlərinin saxlanılmasını və qorunmasını, informasiya təhlükəsizliyini və fərdi məlumatların qorunmasını təmin etmək;

7.1.4. Reyestrlə bağlı metodiki, informasiya-linqvistik, proqram-texniki dəstəyi təmin etmək;

7.1.5. Reyestrə məlumatların təqdim edilməsinə və bu məlumatların yenilənməsinə nəzarət etmək;

7.1.6. Reyestrə daxil edilmiş məlumatları monitorinq etmək, təhlillər aparmaq və müvafiq hesabatlar hazırlayaraq sahibə təqdim etmək;

7.1.7. Reyestrin fəaliyyəti və təhlükəsizliyinin təmin edilməsi ilə bağlı sahibə təkliflər vermək;

7.1.8. Reyestrə daxil edilmiş məlumatları arxivləşdirmək və saxlamaq;

7.1.9. Reyestrin dayanıqlı, fasiləsiz işləməsini və informasiya təhlükəsizliyini təmin etmək;

7.1.10. kritik informasiya infrastrukturu subyektlərinin Reyestrə dair müraciətlərinə aidiyyəti üzrə baxmaq.

8. İştirakçıların funksiyaları

8.1. İştirakçılar Reyestrin fəaliyyəti üzrə aşağıdakı funksiyalara malikdirlər:

8.1.1. Reyestrin fəaliyyətinin davamlılığının və təhlükəsizliyinin pozulmasına səbəb ola biləcək əməllərə yol verməmək;

8.1.2. Reyestrə qoşulmuş informasiya ehtiyatlarının və sistemlərinin təhlükəsizliyini, dayanıqlı və fasiləsiz fəaliyyətini təmin etmək;

8.1.3. bu Qayda ilə müəyyən edilmiş məlumatları Reyestrə təqdim etmək;

8.1.4. Reyestrin fəaliyyətində iştirak edən əməkdaşlarını gücləndirilmiş elektron imza ilə təmin etmək;

8.1.5. Reyestrin fəaliyyətində istifadə olunan elektron imza vasitələrinin təhlükəsizliyini təmin etmək;

8.1.6. operatorun sorğularını normativ hüquqi aktların tələblərinə uyğun olaraq cavablandırmaq, habelə qeyd edilən sorğular əsasında zəruri sənədləri (məlumatları) onlara təqdim etmək;

8.1.7. “Reyestr üzrə xəbərdarlıq” modulunda paylaşılan məlumatları izləmək;

8.1.8. Reyestrə daxil edilən məlumatların aktuallığını, tamlığını, unikallığını, təhrifolunmazlığını və konfidensiallığını təmin etmək;

8.1.9. məlumat mübadiləsi zamanı aşkar olunmuş çatışmazlıqların və yaranan nasazlıqların aradan qaldırılması ilə bağlı tədbirlər görmək və bu barədə operatora məlumat vermək;

8.1.10. öz təşəbbüsü, habelə sahibin əsaslandırılmış təklifi əsasında Reyestrə qoşulmuş informasiya ehtiyatlarında və sistemlərində zəruri dəyişikliklər və təkmilləşdirmələr aparmaq;

8.1.11. Reyestrdə olan məlumatlardan yalnız xidməti məqsədlər üçün istifadə etmək;

8.1.12. Reyestrin fəaliyyətinin təkmilləşdirilməsi ilə bağlı sahibə təkliflər vermək;

8.1.13. normativ hüquqi aktların tələblərinə uyğun olaraq informasiya təhlükəsizliyini və fərdi məlumatların mühafizəsini təmin etmək.