“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə

Azərbaycan Respublikasının Milli Məclisi Azərbaycan Respublikası Konstitusiyasının 94-cü maddəsinin I hissəsinin 20-ci bəndini rəhbər tutaraq **qərara alır:**

“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda (Azərbaycan Respublikasının Qanunvericilik Toplusu, 1998, № 6, maddə 364; 2005, № 6, maddə 466; 2006, № 12, maddə 1005; 2007, № 10, maddə 938; 2011, № 3, maddə 162; 2012, № 11, maddə 1051; 2017, № 3, maddə 345; 2019, № 12, maddə 1881; 2020, № 3, maddə 225, № 6, maddə 671; 2021, № 12, maddə 1345) aşağıdakı dəyişikliklər edilsin:

1. 2-ci maddənin iyirmi dördüncü abzasının sonunda nöqtə işarəsi nöqtəli vergül işarəsi ilə əvəz edilsin və aşağıdakı məzmunda iyirmi beşinci – otuz üçüncü abzaslar əlavə edilsin:

“**kritik informasiya infrastrukturu** – dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ya ekologiya sahəsində fəaliyyəti təmin edən və funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vura bilən informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin məcmusu;

kritik informasiya infrastrukturu obyekti – kritik informasiya infrastrukturunun tərkib hissəsi olan informasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və ya informasiya-kommunikasiya şəbəkəsi;

kritik informasiya infrastrukturu subyekti – kritik informasiya infrastrukturu obyektinin sahibi (istifadəçisi) olan dövlət orqanları (qurumları), o cümlədən dövlətə məxsus olan hüquqi şəxslər, dövlət adından yaradılmış publik hüquqi şəxslər, habelə digər hüquqi şəxslər və ya fərdi sahibkarlar (mikro, kiçik və orta sahibkarlıq subyektləri istisna olmaqla);

kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində səlahiyyətli orqan (bundan sonra - səlahiyyətli orqan) – kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi məqsədilə bu Qanunla və bu Qanundan irəli gələn digər normativ hüquqi aktlarla müəyyən edilmiş funksiyaları yerinə yetirən müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum);

kibertəhlükəsizlik xidməti provayderi – kibertəhlükəsizlik xidmətlərinin göstərilməsi sahəsində fəaliyyət göstərən, işçi heyəti, texnoloji resursları və proseslərinə dair müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilən tələblərə cavab verən və kritik informasiya infrastrukturu subyekti ilə bağlanılmış müqavilə əsasında onlara kibertəhlükəsizlik xidməti göstərən hüquqi şəxslər;

informasiya təhlükəsizliyi – informasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsi;

kibertəhdid – informasiya sistemlərinə və ya ehtiyatlarına qanunsuz daxilolma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına səbəb ola bilən amil və ya vəziyyət;

kiberhücum – informasiya sistemlərinin və ya ehtiyatlarının informasiya təhlükəsizliyinə təhdid yaradan, yaxud onların fəaliyyətinin pozulmasına və ya dayanmasına səbəb olan kiberməkan vasitəsilə qəsdən törədilən əməl;

kiberinsident – informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin fəaliyyətinin dayanması və ya pozulması, yaxud həmin obyektlərdə informasiya təhlükəsizliyinin pozulmasına səbəb olan hadisə.”.

2. Aşağıdakı məzmunda V-I fəsil əlavə edilsin:

“V-I Kritik informasiya infrastrukturunun təhlükəsizliyi

Maddə 20-1. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydası

20-1.1. Kritik informasiya infrastrukturunun təhlükəsizliyi həmin infrastrukturun təhlükəsizliyinə dair tələblərin müəyyən edilməsi, bu tələblərə uyğunluğunun qiymətləndirilməsi və aşkar olunan uyğunsuzluqların aradan qaldırılması, həmin tələblərə müvafiq olan informasiya təhlükəsizliyini idarəetmə sisteminin tətbiq edilməsi, habelə kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması vəziyyətinə nəzarətin həyata keçirilməsi yolu ilə təmin edilir.

20-1.2. 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.

20-1.3. Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən təsdiq olunur.

Maddə 20-2. Kritik informasiya infrastrukturu obyektləri

20-2.1. Obyektin funksionallığının pozulmasının aşağıdakı nəticələrə səbəb ola bilməsi onun kritik informasiya infrastrukturu obyekti hesab edilməsinə əsasdır:

20-2.1.1. dövlətin müstəqilliyi, suverenliyi, konstitusiya quruluşu, ərazi bütövlüyü və müdafiə qabiliyyətinin pozulmasına təhlükənin, habelə ictimai təhlükəsizliyə mühüm təhdidlərin yaranması;

20-2.1.2. dövlət orqanlarının (qurumlarının) fəaliyyətinin pozulması, həyat təminatı infrastrukturunun normal fəaliyyət göstərməsinə ciddi maneələrin yaranması, nəqliyyat və kommunikasiya əlaqələrinin kəsilməsi və ya səhiyyə xidmətlərinin göstərilməsinin əhəmiyyətli dərəcədə məhdudlaşdırılması nəticəsində əhalinin mühüm təminatlardan məhrum olması;

20-2.1.3. iqtisadi və maliyyə sabitliyinin pozulması, dövlət büdcəsinin formalaşdırılmasına əhəmiyyətli zərərin vurulması;

20-2.1.4. ekoloji tarazlığın pozulması və ekoloji vəziyyətin kəskin pisləşməsi.

20-2.2. Kritik informasiya infrastrukturu obyektlərinin meyarları müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən bu Qanunun 20-2.1-ci maddəsində nəzərdə tutulmuş tələblər nəzərə alınmaqla müəyyən edilir.

20-2.3. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) kritik informasiya infrastrukturu obyektlərinin reyestrini aparır. Reyestrin strukturu, yaradılması və aparılması qaydası müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilir.

Maddə 20-3. Kritik informasiya infrastrukturunun informasiya təhlükəsizliyini idarəetmə sistemi

20-3.1. Kritik informasiya infrastrukturu subyektləri onlara məxsus olan kritik informasiya infrastrukturuna kibertəhdidlərin, kiberhücumların, kiberinsidentlərin, habelə bu əməllərin törədilməsinə cəhdlərin aşkarlanması, qarşısının alınması və zərərli nəticələrinin aradan qaldırılması məqsədilə müvafiq infrastrukturun informasiya təhlükəsizliyini idarəetmə sistemini təşkil etməli və onun fəaliyyətini təmin etməlidirlər.

20-3.2. 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 kritik informasiya infrastrukturu obyektlərinin reyestrində yerləşdirilir. Səlahiyyətli orqan həmin idarəetmə sistemlərinin kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərə uyğunluğunun təmin olunmasını kritik informasiya infrastrukturu subyektindən tələb edə bilər.

20-3.3. Kritik informasiya infrastrukturu subyekti səlahiyyətli orqanla qarşılıqlı əlaqələrin operativliyini təmin etmək məqsədilə kritik informasiya infrastrukturunun təhlükəsizliyi üzrə məsul şəxs təyin edir və bu barədə məlumatı kritik informasiya infrastrukturu obyektlərinin reyestrində yerləşdirir.

20-3.4. Kritik informasiya infrastrukturu subyektləri onlara məxsus olan kritik informasiya infrastrukturuna kibertəhdidlər, kiberhücumlar, kiberinsidentlər, habelə bu əməllərin törədilməsinə cəhdlər barədə məlumatları kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərlə müəyyən edilmiş qaydada səlahiyyətli orqana göndərməlidirlər.

Maddə 20-4. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblər

20-4.1. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələblər müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilir.

20-4.2. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə xüsusi tələblər kritik informasiya infrastrukturunun subyekti tərəfindən kritik informasiya infrastrukturunun təyinatı və onun fəaliyyət xüsusiyyətlərinə müvafiq olaraq müəyyən edilir və kritik informasiya infrastrukturu obyektlərinin reyestrində yerləşdirilir.

20-4.3. Səlahiyyətli orqan kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərin tətbiqi ilə bağlı məsələlər üzrə kritik informasiya infrastrukturu subyektlərinə yazılı və şifahi şəkildə izahlar verir, habelə qarşıya çıxan çətinliklərin aradan qaldırılmasına dair metodiki köməklik göstərir.

20-4.4. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərə riayət edilməsi vəziyyətinin öyrənilməsi məqsədilə səlahiyyətli orqanın kritik informasiya infrastrukturunun subyektinə göndərdiyi sorğular təxirə salınmadan cavablandırılmalıdır.

20-4.5. Kritik informasiya infrastrukturunun subyekti ona məxsus kritik informasiya infrastrukturu obyektinə olan kiberhücumlara qarşı cavab tədbirlərinin görülməsi, habelə kibertəhdidlərin və kiberinsidentlərin qarşısının alınması ilə bağlı səlahiyyətli orqanın həyata keçirdiyi fəaliyyətə zəruri şərait yaratmalı və dəstək verməlidir.

20-4.6. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərin pozulması qanunla müəyyən edilmiş məsuliyyətə səbəb olur.

Maddə 20-5. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətin təşkili

20-5.1. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətin ümumi təşkili və əlaqələndirilməsi səlahiyyətli orqan tərəfindən həyata keçirilir.

20-5.2. Kritik informasiya infrastrukturu subyekti ona məxsus olan kritik informasiya infrastrukturunun təhlükəsizliyini infrastrukturun təhlükəsizliyinə dair müəyyən edilmiş ümumi və xüsusi tələblərə uyğun olaraq təmin edir.

20-5.3. Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətin təşkil edilməsi məqsədilə səlahiyyətli orqan:

20-5.3.1. kritik informasiya infrastrukturunun təhlükəsizliyi sahəsində ümumi vəziyyətin fasiləsiz monitorinqini həyata keçirir;

20-5.3.2. kritik informasiya infrastrukturunun təhlükəsizliyinə yönələn kibertəhdidlərlə mübarizə üzrə əlaqələndirilmiş tədbirlərin görülməsini təşkil edir;

20-5.3.3. kritik informasiya infrastrukturunun təhlükəsizliyinə yönələn kibertəhdidlərin qarşısının alınması məqsədilə təhlükəsizlik boşluqları və riskləri, zərərverici proqram təminatı, qlobal və lokal xarakterli kiberinsidentlər, kritik informasiya infrastrukturuna münasibətdə törədilmiş kiberhücumlar, cəhdlər və bununla bağlı olan digər məlumatları toplayır və təhlil edir, təhdidlərin kritik informasiya infrastrukturunun təhlükəsizliyinə potensial təsirlərini qiymətləndirir;

20-5.3.4. kritik informasiya infrastrukturunun təhlükəsizliyi üzrə məsul şəxslərdən qarşılaşdıqları informasiya təhlükəsizliyinə dair kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə məlumatları toplayır, təhdidlərin qabaqlanması, qarşısının alınması və onlarla mübarizə aparılması üçün zəruri olan məlumatları operativ şəkildə onlara verir, müvafiq tədbirlərin görülməsi üçün köməklik göstərir;

20-5.3.5. kiberhücumlar, təhlükəsizlik boşluqları və riskləri, zərərverici proqram təminatı və kritik informasiya infrastrukturunun təhlükəsizliyinə digər təhdidlərlə bağlı kritik informasiya infrastrukturu subyektlərinə xəbərdarlıqlar və tövsiyələr verir.

Maddə 20-6. Kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarət

20-6.1. Kritik informasiya infrastrukturunun təhlükəsizliyin təmin olunması vəziyyətinə nəzarətin məqsədi kritik informasiya infrastrukturunun təhlükəsizliyinə dair 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 mühafizə edilməsindən ibarətdir.

20-6.2. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət səlahiyyətli orqan və kritik informasiya infrastrukturu subyektləri tərəfindən həyata keçirilir.

20-6.3. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə uyğunluğunun qiymətləndirilməsi və aşkar olunan uyğunsuzluqların aradan qaldırılması, bu tələblərə riayət edilməsinin yoxlanılması, kritik informasiya infrastrukturunun təhlükəsizliyinin fasiləsiz monitorinqinin aparılması, müdaxilə sınaqları və kənar audit yoxlamalarının həyata keçirilməsi vasitəsilə həyata keçirilir.

20-6.4. Kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi və xüsusi tələblərə sahibkarlıq fəaliyyəti subyektləri tərəfindən riayət olunmasının yoxlanılması həmin sahibkarlıq fəaliyyətinin həyata keçirildiyi obyektlərə gəlmədən aparılır.

20-6.5. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) kritik informasiya infrastrukturunun 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 bilər.

20-6.6. Bu Qanunun 20-6.5-ci maddəsinə əsasən həyata keçirilən fəaliyyət zamanı aşkar edilən pozuntulara görə sahibkar məsuliyyətə cəlb edilə bilməz.

20-6.7. Kritik informasiya infrastrukturu subyektləri səlahiyyətli orqan tərəfindən aşkar edilmiş kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərin pozulması hallarını onun tələbinə əsasən təxirə salınmadan aradan qaldırmalı və görülmüş tədbirlərin nəticəsi barədə məlumat verməlidirlər.

20-6.8. 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 müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) göndərilməsini təmin etməlidirlər.”.

İlham Əliyev
Azərbaycan Respublikasının Prezidenti

Bakı şəhəri, 27 may 2022-ci il
№ 539-VIQD