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

Azərbaycan Respublikasının Milli Məclisi Azərbaycan Respublikası Konstitusiyasının 94-cü maddəsinin I hissəsinin 10-cu, 20-ci və 23-cü bəndlərini rəhbər tutaraq **qərara alır:**

“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda (Azərbaycan Respublikasının Qanunvericilik Toplusu, 1998, № 6, maddə 364 (Cild I); 2024, № 1, maddə 18, № 7, maddə 769; 2025, № 7, maddə 626; 2026, № 1, maddə 17; Azərbaycan Respublikasının 2026-cı il 21 aprel tarixli 387-VIIQD nömrəli Qanunu) aşağıdakı dəyişikliklər edilsin:

1. 1-ci maddə üzrə:

1.1. birinci hissəyə “mühafizəsi” sözündən sonra “, informasiya təhlükəsizliyi, o cümlədən kibertəhlükəsizliyin təmini” sözləri əlavə edilsin;

1.2. ikinci hissəyə “Qanun” sözündən sonra “Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi, “Əməliyyat-axtarış fəaliyyəti haqqında”, “Kəşfiyyat və əks-kəşfiyyat fəaliyyəti haqqında”,” sözləri əlavə edilsin;

1.3. aşağıdakı məzmunda üçüncü hissə əlavə edilsin:

“Bu Qanundan irəli gələrək aparılan icraat “İnzibati icraat haqqında” Azərbaycan Respublikasının Qanunu, dövlət sirri və kommersiya sirri təşkil edən məlumatların, maliyyə bazarlarını tənzimləyən qanunlarla qorunan məlumatların, habelə fərdi məlumatların toplanılmasını, işlənilməsini və mühafizəsini təmin edən informasiya infrastrukturunun kibertəhlükəsizliyi ilə bağlı münasibətlər “Dövlət sirri haqqında”, “Kommersiya sirri haqqında”, “Fərdi məlumatlar haqqında” və maliyyə bazarlarını tənzimləyən Azərbaycan Respublikası qanunlarının tələbləri nəzərə alınmaqla həyata keçirilir.”.

2. 2-ci maddənin birinci hissəsi üzrə:

2.1. birinci abzas aşağıdakı redaksiyada verilsin:

“Bu Qanunun məqsədləri üçün istifadə olunan əsas anlayışlar aşağıdakı mənaları ifadə edir:”;

2.2. otuz dördüncü abzasın sonunda nöqtə işarəsi nöqtəli vergül işarəsi ilə əvəz edilsin və aşağıdakı məzmunda otuz beşinci – əlli üçüncü abzaslar əlavə edilsin:

“**informasiya infrastrukturu** – informasiya-telekommunikasiya şəbəkələrinin, internet informasiya ehtiyatlarının, informasiya ehtiyatlarının və sistemlərinin, o cümlədən avtomatlaşdırılmış idarəetmə sistemlərinin məcmusu;

informasiya infrastrukturu subyekti – informasiya infrastrukturunun obyekti üzərində sahiblik, istifadə və sərəncam hüquqlarını həyata keçirən yerli özünüidarəetmə orqanı, fiziki və ya hüquqi şəxs, habelə sahibliyinə informasiya infrastrukturu obyekti verilmiş dövlət orqanı (qurumu);

informasiya infrastrukturu obyekti – informasiya infrastrukturunun tərkib hissəsi olan və ya ayrılıqda informasiya infrastrukturu ola bilən informasiya-telekommunikasiya şəbəkələri, informasiya ehtiyatları və sistemləri, o cümlədən avtomatlaşdırılmış idarəetmə sistemləri;

ictimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturu – kritik informasiya infrastrukturu, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin, kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektlərinin informasiya infrastrukturu istisna olmaqla, ölkə və cəmiyyət üçün mühüm əhəmiyyət kəsb edən sahələrdə fəaliyyəti, o cümlədən xidmətlərin göstərilməsini təmin edən, funksional fəaliyyətinin pozulması və ya əlçatanlığının məhdudlaşması ölkənin siyasi, sosial və iqtisadi dayanıqlılığına ciddi zərər vuran informasiya infrastrukturu;

kibertəhlükəsizlik – informasiya infrastrukturunun kibertəhdidlərdən, kiberhücumlardan və kiberinsidentlərdən mühafizə edilməsi və kiberdayanıqlılığının (kiberinsidentlərə qarşı davamlılıq, həmin insidentlər zamanı fəaliyyətin saxlanılması və sonradan operativ bərpası qabiliyyəti) təmin edilməsi;

proaktiv kibertəhlükəsizlik tədqiqatı – kibertəhdidlər, onların mənbəyi, törədilmə vasitələri və üsulları barədə məlumatların toplanması və təhlili;

kompüter insidentlərinə qarşı mübarizə mərkəzi (bundan sonra – CERT) – informasiya infrastrukturunun kibertəhlükəsizliyinin pozulması hallarının, hadisələrinin və faktlarının aşkarlanması, səbəblərinin araşdırılması, habelə qarşısının alınması üçün qabaqlayıcı tədbirlər həyata keçirən ixtisaslaşmış qurum və ya struktur;

Milli kompüter insidentlərinə qarşı mübarizə mərkəzi (bundan sonra – Milli CERT) – ölkə üzrə kibertəhlükəsizlik sahəsində məlumat mübadiləsini, informasiya infrastrukturu subyektlərinin (kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektləri, mühafizə olunan şəxslər, qorunan və strateji obyektlər istisna olmaqla) və CERT-lərin fəaliyyətinin (kritik informasiya infrastrukturuna münasibətdə səlahiyyətli orqan vasitəsilə), dövlət orqanlarına (qurumlarına), habelə Azərbaycan Respublikasının Mərkəzi Bankına və maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərə (bank, sığortaçı, təkrarsığortaçı, qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər, səhmdar investisiya fondu və investisiya fondunun idarəçisi, ödəniş xidmət təchizatçıları və s.) məxsus informasiya infrastrukturlarına, eləcə də onlarla bağlı aidiyyəti üzrə müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) və Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən yaradılmış CERT-lər üzrə digər fəaliyyət istiqamətləri istisna olmaqla, yalnız kibertəhdid, kiberhücum və kiberinsidentlər üzrə məlumat mübadiləsi (kritik informasiya infrastrukturuna münasibətdə səlahiyyətli orqan vasitəsilə) koordinasiyasını, o cümlədən kibertəhlükəsizliyin pozulması hallarının, hadisələrinin və faktlarının aşkarlanmasını, səbəblərinin araşdırılmasını (dövlət orqanlarında (qurumlarında) (mühafizə olunan şəxslərin, qorunan və strateji

obyektlərin informasiya infrastrukturu istisna olmaqla) informasiya infrastrukturuna kibertəhdidlərin, kiberhücumların və kiberinsidentlərin səbəblərinin Dövlət CERT-i ilə birgə araşdırılması), habelə kibertəhdidlər üzrə qabaqlayıcı tədbirlərin həyata keçirilməsini təmin edən müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum);

Dövlət kompüter insidentlərinə qarşı mübarizə mərkəzi (bundan sonra – Dövlət CERT/GOV CERT) – kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektlərinin, Azərbaycan Respublikası Mərkəzi Bankının informasiya infrastrukturu istisna olmaqla, sahəvi CERT olaraq dövlət orqanlarının (qurumlarının) fəaliyyətini təmin edən informasiya infrastrukturlarının (kritik informasiya infrastrukturu obyektlərinə münasibətdə səlahiyyətli orqanla birlikdə), o cümlədən ali kateqoriya dövlət orqanlarının, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturunun kibertəhlükəsizlik sahəsində məlumat mübadiləsini, o cümlədən kibertəhlükəsizliyinin pozulması hallarının, hadisələrinin və faktlarının aşkarlanması, səbəblərinin araşdırılması (mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturu istisna olmaqla, kibertəhdidlərin, kiberhücumların və kiberinsidentlərin səbəblərinin Milli CERT-lə birlikdə araşdırılması), qarşısının alınması üçün kibertəhdidlər üzrə öz səlahiyyətləri çərçivəsində qabaqlayıcı tədbirlərin həyata keçirilməsini, eləcə də onların təhlükəsiz internet şəbəkəsi ilə təmin edilməsini və fasiləsiz qaydada Təhlükəsizlik əməliyyatları mərkəzi vasitəsilə təhlükəsizliyinin nəzarətdə saxlanılmasını, kibertəhdid, kiberhücum və kiberinsidentlə bağlı Milli CERT-lə qarşılıqlı məlumat mübadiləsini (kritik informasiya infrastrukturu obyektlərinə münasibətdə səlahiyyətli orqan vasitəsilə) həyata keçirən, Milli CERT-dən daxil olmuş məlumatlar əsasında insidentlərin fəsadlarının aradan qaldırılmasını, proaktiv kibertəhlükəsizlik tədqiqatının aparılması və “gov.az” domen zonasına bənzədilmiş saxta domenlərin aşkarlanması üzrə monitorinqi həyata keçirən, sahə üzrə məlumat mübadiləsində iştirak edən müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum);

kibermәkan – bilavasitə və ya dolayısı ilə informasiya-telekommunikasiya şəbəkələrinə, habelə elektron rabitə və ya kompüter şəbəkələrinə qoşulmuş informasiya infrastrukturu obyektlərindən ibarət rəqəmsal mühit;

kibergigiyena – informasiya infrastrukturlarının və istifadəçilərin kibertəhlükəsizliyini təmin etmək, riskləri azaltmaq, kiberhücumların və kibertəhdidlərin qarşısını almaq məqsədilə dövlət hakimiyyəti və yerli özünüidarəetmə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar, həmçinin fiziki şəxslər tərəfindən müntəzəm tətbiq edilməli olan davranış qaydalarının, texniki və təşkilati tədbirlərin məcmusu;

rəqəmsal dəlil – kiberinsidentlər üzrə hüquqi əhəmiyyət kəsb edən hadisələrlə bağlı halların və faktların müəyyən edilməsi üçün istifadə olunan, rəqəmsal texnologiyalar vasitəsilə yaradılan, emal edilən və ya saxlanılan, bütövlüyü və etibarlılığı təmin edilməklə əldə edilən və ilkin texniki ekspertiza tələb edən məlumatlar və ya məlumat daşıyıcıları;

rəqəmsal inkişaf – rəqəmsal texnologiyaların və innovativ həllərin tətbiqi yolu ilə dövlət idarəçiliyinin, iqtisadi fəaliyyətin və xidmətlərin səmərəliliyinin, əlçatanlığının və keyfiyyətinin artırılmasına, habelə məlumatlara əsaslanan

qərarvermənin, rəqəmsal bacarıqların və innovasiya ekosisteminin inkişafına yönəlmiş sistemli və davamlı fəaliyyətin məcmusu;

rəqəmsal tədqiqat – informasiya infrastrukturunda baş vermiş kiberinsidentlərin araşdırılması, rəqəmsal dəlillərin müəyyən edilməsi məqsədilə həyata keçirilən, informasiya infrastrukturu obyektlərində məlumatların identifikasiyası, toplanılması, surətinin çıxarılması, qorunub-saxlanılması, bütövlüyünün təmin edilməsi, texniki təhlili və nəticələrin sənədləşdirilməsi proseslərinin məcmusu;

Rəqəmsal tədqiqat mərkəzi – rəqəmsal tədqiqat fəaliyyətini həyata keçirən müvafiq icra hakimiyyəti orqanının (qurumunun) müəyyən etdiyi orqan (qurum);

Təhlükəsizlik əməliyyatları mərkəzi (bundan sonra – SOC) – informasiya infrastrukturunun kibertəhlükəsizliyinin təmin edilməsi məqsədilə kibertəhdidlərin, kiberhücumların və kiberinsidentlərin real vaxt rejimində monitorinqini, aşkarlanmasını, eyniləşdirilmiş təhlilini və ilkin texniki cavab tədbirlərini həyata keçirən, ixtisaslaşmış işçi heyətinə, texnoloji vasitələrə və təhlükəsizlik prosedurlarına malik olan qurum və ya struktur;

Milli təhlükəsizlik əməliyyatları mərkəzi (bundan sonra – Milli SOC) – ölkə üzrə fəaliyyət göstərən SOC-lardan və digər mənbələrdən daxil olan məlumatların (mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturu istisna olmaqla) toplanmasını və təhlilini təmin edən, qarşılıqlı məlumat mübadiləsindən irəli gələrək topladığı və təhlil etdiyi həmin məlumatlar əsasında kibertəhlükəsizlik vəziyyətinin mərkəzləşdirilmiş qaydada monitorinqini aparan müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum);

rəqəmsal həll – fəaliyyətin şəffaflığının, effektivliyinin, səmərəliliyinin artırılması, həmçinin göstərilən xidmətlərinin keyfiyyətinin və istifadəçi məmnunluğunun yüksəldilməsi məqsədilə tətbiq edilən proqram təminatı və texnoloji avadanlıqların məcmusu;

tənzimləyici test mühiti – rəqəmsal həllərin sahə üzrə effektivliyinin test rejimində qiymətləndirilməsinin məhdud çərçivədə (ərazi, müddət, əməliyyatların sayı, həcmi, iştirakçıların və istifadəçilərin sayı (dairəsi) ilə bağlı və ya digər məhdudiyyətlər) və müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) tənzimləməsi ilə həyata keçirilməsinə imkan verən alət.”.

3. 3-cü maddənin birinci hissəsinin səkkizinci abzasına “təhlükəsizliyin” sözündən sonra “, habelə informasiya təhlükəsizliyinin və kibertəhlükəsizliyin” sözləri əlavə edilsin.

4. 14-cü maddəyə aşağıdakı məzmunda səkkizinci hissə əlavə edilsin:

“Dövlət informasiya ehtiyatları və sistemlərinin (kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektlərinə məxsus informasiya ehtiyatları və sistemləri, eləcə də kritik informasiya infrastrukturu, Azərbaycan Respublikası Mərkəzi Bankının və maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərin (dövlət mülkiyyətində olan və paylarının (səhmlərinin) nəzarət zərfi dövlətə məxsus olan hüquqi şəxslərin) informasiya infrastrukturu istisna olmaqla) təhlükəsizlik meyarları üzrə monitorinqinin və auditinin aparılması, habelə informasiya təhlükəsizliyi üzrə rəy verilməsi qaydaları müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilir.”.

5. aşağıdakı məzmunda 14-3-cü, 14-4-cü maddələr və V-II fəsil əlavə edilsin:

“**Maddə 14-3. Rəqəmsal inkişaf üzrə layihələrin maliyyələşdirilməsi**

14-3.1. Ali kateqoriya dövlət orqanları, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin təhlükəsizliyini təmin edən dövlət orqanları, kəşfiyyat və əks-kəşfiyyat fəaliyyətinin subyektləri, eləcə də Azərbaycan Respublikasının Mərkəzi Bankı istisna olmaqla, dövlət orqanları (qurumları) tərəfindən hər növbəti il ərzində həyata keçirilməsi nəzərdə tutulan rəqəmsal inkişaf üzrə layihələrə dair təkliflər, tələb olunan maliyyə vəsaitinin məbləği və maliyyələşdirmə mənbəyi qeyd edilməklə, cari il yanvarın 20-dək müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) təqdim edilir. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) həmin təkliflərə 2 ay müddətində baxaraq texniki və səmərəlilik baxımından məqsədəuyğunluq haqqında rəyini aidiyyəti dövlət orqanına (qurumuna) təqdim edir.

14-3.2. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) dövlət investisiyası çərçivəsində həyata keçirilən rəqəmsal inkişaf üzrə layihələrə dair müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) rəyini alır. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) rəy alınması üçün müraciətə 14 iş günü müddətində baxmalı və cavablandırmalıdır. Bu müddət ərzində müraciət cavablandırılmadıqda, rəy müsbət hesab olunur.

14-3.3. Dövlət proqramlarında, strategiyalarda, milli fəaliyyət planlarında, konsepsiyalarda və bu kimi digər sənədlərdə nəzərdə tutulan strateji hədəflərə və məqsədlərə, ölkənin rəqəmsal inkişaf üzrə vahid arxitekturasına uyğun olmayan, dövlət investisiyası çərçivəsində maliyyələşdirilməsi nəzərdə tutulmayan, habelə təkrar (dublikat) layihələrə müsbət rəy verilmir. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) özünün və müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) müsbət rəy verdiyi layihələrə dair sənədləri həmin rəylə birlikdə cari il aprelin 1-dək müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) təqdim edir.

14-3.4. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) bu Qanunun 14-3.3-cü maddəsində qeyd edilən sənədləri aldığı vaxtdan 2 ay müddətində maliyyə ekspertizasını apararaq rəyini müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) və aidiyyəti dövlət orqanına (qurumuna) təqdim edir.

14-3.5. Bu Qanunun 14-3.1-ci, 14-3.2-ci və 14-3.4-cü maddələrində qeyd edilən rəylər müsbət olduqda aidiyyəti dövlət orqanı (qurumu) rəqəmsal inkişaf üzrə layihələrin maliyyələşdirilməsi üzrə təkliflərini “Büdcə sistemi haqqında” Azərbaycan Respublikası Qanununun tələblərinə uyğun olaraq cari il iyulun 1-dək müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) təqdim edir.

14-3.6. Bu Qanunun 14-3.5-ci maddəsində nəzərdə tutulan layihələrin maliyyələşdirilməsi üçün vəsaitin müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən aidiyyəti dövlət qurumuna hər bir layihə üzrə ayrılması müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanla (qurumla) razılaşdırılmaqla həyata keçirilir.

14-3.7. Rəqəmsal inkişaf üzrə layihələrin maliyyələşdirilməsi üzrə dövlət qurumları tərəfindən təkliflərin, eləcə də həmin təkliflərə dair bu Qanunun 14-3.1-ci, 14-3.2-ci və 14-3.4-cü maddələrində qeyd edilən rəylərin verilməsi müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) informasiya sistemi üzərindən həyata keçirilir.

Maddə 14-4. Tənzimləyici test mühiti

14-4.1. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) rəqəmsal həllərin tətbiq olunacağı sahə üzrə tənzimləmə və nəzarət funksiyalarını həyata keçirən aidiyyəti dövlət orqanları (qurumları) ilə birlikdə fiziki və hüquqi şəxslərin (dövlətə məxsus olan kommersiya hüquqi şəxslər və publik hüquqi şəxslər istisna olmaqla) müraciəti əsasında onlar tərəfindən tətbiqi (istifadəsi) təklif olunan rəqəmsal həllərin (o cümlədən süni intellekt texnologiyalarının) sınaqdan keçirilməsi məqsədilə tənzimləyici test mühitini tətbiq edir.

14-4.2. Tənzimləyici test mühitinin həyata keçirilməsi qaydaları, o cümlədən onda iştirak edən şəxslərin fəaliyyətinə nəzarət edilməsi, tənzimləyici test mühitinin maksimum müddəti və normativ hüquqi aktların tələblərindən istisnaların tətbiqi qaydası müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən olunur.

14-4.3. Bu Qanunun maddələri maliyyə bazarlarında rəqəmsal həllərin (o cümlədən süni intellekt texnologiyalarının) sınaqdan keçirilməsinə şamil edilmir. Maliyyə bazarlarında rəqəmsal həllərin (o cümlədən süni intellekt texnologiyalarının) sınaqdan keçirilməsi “Azərbaycan Respublikasının Mərkəzi Bankı haqqında” Azərbaycan Respublikası Qanununun 50-ci maddəsinə uyğun olaraq həyata keçirilir. Azərbaycan Respublikası Mərkəzi Bankının nəzarəti altında həyata keçirilən tənzimləyici test mühiti üzrə sınaqlarda iştirak edən subyektlərin sayına və sınaqların nəticələrinə dair Azərbaycan Respublikası Mərkəzi Bankının rəsmi internet informasiya ehtiyatındakı müvafiq reyestrdə əks olunan açıq məlumatları altı ayda bir dəfə - yanvar və iyul aylarının 10-dək müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) təqdim edir.”;

“V-II fəsil

İnformasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyi

Maddə 20-7. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyinin təmin edilməsi

20-7.1. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturlarında kibertəhlükəsizlik üzrə fəaliyyət həmin infrastrukturun mövcud olduğu sahə üzrə dövlət siyasətini, tənzimləməsini və nəzarətini həyata keçirən dövlət orqanının (qurumunun) müvafiq strukturu və ya həmin orqan (qurum) tərəfindən müqavilə əsasında müəyyən edilən rezident hüquqi şəxs olan CERT-lər vasitəsilə təmin edilir.

20-7.2. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturu obyektinə qarşı yönəlmiş kibertəhdid və kiberhücumların, həmçinin baş vermiş kiberinsidentlərin real vaxt rejimində fasiləsiz monitorinqi və onlara qarşı ilkin texniki cavab tədbirlərinin görülməsi SOC-lar tərəfindən həyata keçirilir.

20-7.3. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturu subyektlərinin siyahısı (dövlət orqanlarına (qurumlarına) məxsus, informasiya infrastrukturu Dövlət CERT-i isitisna olmaqla) həmin infrastrukturun

mövcud olduğu sahə üzrə dövlət siyasətini, tənzimləməsini və nəzarətini həyata keçirən dövlət orqanı (qurumu) tərəfindən müəyyən edilərək Milli CERT-ə təqdim edilir.

20-7.4. CERT-lər tərəfindən mütəmadi olaraq, lakin ildə bir dəfədən az olmayaraq ictimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturlarının siyahısı nəzərdən keçirilməli və həmin siyahının yenilənməsi təmin edilməlidir. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturlarının yenilənmiş siyahısı bu Qanunun 20-7.3-cü maddəsində nəzərdə tutulan dövlət orqanı (qurumu) tərəfindən yeniləndiyi tarixdən 10 iş günü ərzində Milli CERT-ə təqdim edilməlidir.

20-7.5. İctimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturunun kibertəhlükəsizliyi üzrə ümumi tələblər müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum), xüsusi tələblər isə həmin infrastrukturun mövcud olduğu sahə üzrə dövlət siyasətini, tənzimləməsini və nəzarətini həyata keçirən dövlət orqanı (qurumu) tərəfindən (bu maddənin ikinci cümləsinin tələbi nəzərə alınmaqla, dövlət orqanlarının (qurumlarının) infrastrukturuna münasibətdə müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanla (qurumla) razılaşdırmaqla) müəyyən edilir. Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya infrastrukturunun kibertəhlükəsizliyi üzrə ümumi və xüsusi tələblər Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən müəyyən edilir.

20-7.6. Hər bir informasiya infrastrukturu subyekti tərəfindən CERT və ya SOC struktur bölmə kimi yaradıla və ya müqavilə əsasında rezident hüquqi şəxslər müəyyən edilə bilər.

20-7.7. Milli CERT və Dövlət CERT-i arasında kibertəhdid, kiberhücum və kiberinsidentlər üzrə qarşılıqlı məlumat (mühafizə olunan şəxslər, qorunan və strateji obyektlərin informasiya infrastrukturuna dair məlumatlar istisna olmaqla) mübadiləsi Milli CERT və Dövlət CERT-i tərəfindən birgə müəyyən edilmiş formada həyata keçirilir.

20-7.8. Bu Qanunun V-II fəslinin yalnız 20-8.2-ci maddəsinin üçüncü cümləsi, 20-9.3-cü, 20-10.1-ci və 20-10.6-cı maddələrinin tələbləri kritik informasiya infrastrukturu obyektlərinə, dövlət orqanlarına (qurumlarına) məxsus, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturuna, onlarla bağlı müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) yaratdığı CERT-lərə və SOC-lara şamil edilir.

20-7.9. Dövlət orqanlarında (qurumlarında) (mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturu istisna olmaqla) kibertəhdidlərin, kiberhücumların və kiberinsidentlərin səbəblərinin araşdırılması Dövlət CERT-i tərəfindən Milli CERT-lə birgə həyata keçirilir. Dövlət orqanları (qurumları) tərəfindən yaradılan (müqavilə əsasında müəyyən edilən) CERT-lər Milli CERT-lə yanaşı, Dövlət CERT-i ilə də məlumat mübadiləsi aparırlar.

20-7.10. Dövlət CERT-inin fəaliyyəti, hüquqları və vəzifələri müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) təsdiq etdiyi əsasnamə ilə tənzimlənir. Dövlət orqanlarına (qurumlarına) məxsus (kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektləri istisna olmaqla), habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyinin təmin edilməsi qaydaları müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilir.

20-7.11. Reyestrin aparılmasına və sorğuların verilməsinə münasibətdə bu Qanunun 20-8.4 – 20-8.16-cı və 20-9.1.2-ci maddələrinin tələbləri kritik informasiya infrastrukturu üzrə CERT-lərə, Dövlət CERT-inə və Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən yaradılmış CERT-ə və həmin CERT-lər üzrə SOC-lara, habelə maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlər tərəfindən yaradılan SOC-lara şamil edilmir.

20-7.12. Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən yaradılan CERT-lərə və SOC-lara, habelə maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə yaradılan SOC-lara münasibətdə bu Qanunun V-II fəslinin yalnız 20-8.2-ci maddəsinin üçüncü cümləsi, 20-9.3-cü, 20-10.1-ci və 20-10.6-cı maddələri, eləcə də maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərin domen adı “az” ölkə kodlu yüksək səviyyəli domen zonasında olan internet informasiya ehtiyatlarının monitorinqi və auditi üzrə 20-10-4.7-ci və 20-10.5-ci maddələr şamil edilir.

20-7.13. Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərin informasiya infrastrukturlarında kibertəhlükəsizlik üzrə fəaliyyəti Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən təmin edilir. Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlər tərəfindən SOC-ların yaradılmasının və fəaliyyətinin tənzimlənməsi, monitorinqi və bu fəaliyyətə nəzarət edilməsi Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən həyata keçirilir.

Maddə 20-8. CERT-lərin və SOC-ların fəaliyyətinin təşkili

20-8.1. CERT-lər və SOC-lar tərəfindən göstərilən xidmətlərin dairəsi bu Qanunun tələbləri nəzərə alınmaqla, onların əsasnaməsi (nizamnaməsi) və ya bu Qanunun 20-7.1-ci və 20-7.6-cı maddələrində qeyd edilən müqavilə ilə müəyyən olunur.

20-8.2. Qurumlar müvafiq CERT-i və SOC-u yaratdıqdan və ya müəyyən etdikdən sonra 10 (on) iş günü ərzində onların reyestrə daxil edilməsi üçün müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) elektron qaydada müraciət etməlidir. CERT-lər və SOC-lar reyestrə daxil edilmədən fəaliyyət göstərə bilməzlər. Bu Qanunun 20-7.8-ci və 20-7.12-ci maddələrində nəzərdə tutulan CERT-lər və SOC-lar onların elektron müraciəti əsasında hər hansı bir icraat aparılmadan reyestrə daxil edilmiş hesab olunurlar.

20-8.3. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən CERT-lərin və SOC-ların reyestri elektron formada aparılır.

20-8.4 CERT-lər reyestrə daxil edilməsi üçün aşağıdakı minimal tələblərə cavab verməlidir:

20-8.4.1. işçi heyəti kibertəhlükəsizlik sahəsində ixtisasa və peşə hazırlığına malik olmalı;

20-8.4.2. kiberinsidentlərin və kiberhücumların real vaxt rejimində fasiləsiz monitorinqi və onlara qarşı operativ cavab tədbirlərinin həyata keçirilməsi üçün SOC-a, həmçinin kiberhücumların və kibertəhdidlərin aşkarlanması, aidiyyəti qurumlarla koordinasiya fəaliyyətinin, kiberinsidentlərə yol açа biləcək halların erkən mərhələdə müəyyən edilməsinin təmin edilməsi üzrə texnoloji infrastruktura malik olmalı;

20-8.4.3. kiberinsidentlərin qeydiyyatı və identifikasiyası, onların prioritetləşdirilməsi və təsnifatı, cavab tədbirlərinin planlaşdırılması və icrasının

izlənilməsi, həyata keçirilən fəaliyyətin sənədləşdirilməsi, hesabatlılığın və statistik məlumatların formalaşdırılması, habelə Milli CERT tərəfindən müəyyən edilmiş sistemlərə inteqrasiya funksiyalarına malik mərkəzləşdirilmiş insident idarəetmə sistemi və insident idarəetmə təlimatı mövcud olmalı;

20-8.4.4. kibertəhdidlərin aşkarlanmasını təmin edən proaktiv kibertəhlükəsizlik tədqiqatının aparılması, bu fəaliyyət çərçivəsində zərərli fəaliyyət göstəricilərinin toplanması və təhlili, milli və beynəlxalq mənbələrdən məlumatların əldə edilməsi və emalı, potensial təhdidlər üzrə erkən xəbərdarlıq mexanizmlərinin tətbiqi və əldə edilmiş məlumatların aidiyyəti üzrə paylaşılması üçün texniki infrastruktura malik olmalı;

20-8.4.5. kibertəhlükəsizlik, məlumat mübadiləsi və məlumatların mühafizəsi üzrə siyasət sənədlərinə malik olmalı.

20-8.5. SOC-lar reyestrə daxil edilməsi üçün aşağıdakı minimal tələblərə cavab verməlidir:

20-8.5.1. kiberinsidentlərin və kiberhücumların real vaxt rejimində fasiləsiz monitorinqinin və onlara qarşı ilkin texniki cavab tədbirlərinin həyata keçirilməsi, eləcə də belə fəaliyyətlər nəticəsində əldə edilən məlumatların dərhal Milli SOC-a ötürülməsi üçün texniki infrastruktura malik olmalı;

20-8.5.2. işçi heyəti kibertəhlükəsizlik sahəsində ixtisasa və peşə hazırlığına malik olmalı;

20-8.5.3. fasiləsiz monitorinq zamanı fasiləsiz rejimində fəaliyyət göstərməli, fəaliyyət göstərdiyi sahə üzrə informasiya ehtiyatlarından və sistemlərindən məlumatların (loqların) toplanması, sistemləşdirilməsi və real vaxt rejimində təhlili üçün zəruri texniki və proqram təminatına malik olmalı;

20-8.5.4. kiberinsidentlərin qeydiyyatı və identifikasiyası, onların prioritetləşdirilməsi və təsnifatı, cavab tədbirlərinin planlaşdırılması və icrasının izlənilməsi, həyata keçirilən fəaliyyətin sənədləşdirilməsi, hesabatlılığın və statistik məlumatların formalaşdırılması, habelə Milli CERT tərəfindən müəyyən edilmiş sistemlərə inteqrasiya funksiyalarına malik mərkəzləşdirilmiş insident idarəetmə sistemi və insident idarəetmə təlimatı mövcud olmalı;

20-8.5.5. kibertəhlükəsizlik, məlumat mübadiləsi və məlumatların mühafizəsi üzrə siyasət sənədlərinə malik olmalı.

20-8.6. Bu Qanunun 20-8.2-ci maddəsində qeyd edilən müraciətə aşağıdakı sənədlər və məlumatlar əlavə edilməlidir:

20-8.6.1. CERT-in və ya SOC-un hüquqi şəxslərin dövlət reyestrindən çıxarışının surəti (rezident hüquqi şəxs olduqda);

20-8.6.2. CERT-in və ya SOC-un əsasnaməsinin və ya nizamnaməsinin surəti;

20-8.6.3. CERT-in və ya SOC-un infrastrukturunun yerləşdiyi ünvan və əlaqə məlumatları (telefon nömrəsi, elektron poçt);

20-8.6.4. CERT-in və ya SOC-un kibertəhlükəsizlik, məlumat mübadiləsi və məlumatların mühafizəsi üzrə siyasət sənədləri, habelə insident idarəetmə təlimatı;

20-8.6.5. CERT-in və ya SOC-un işçilərinin kibertəhlükəsizlik sahəsində peşə hazırlığına və ixtisasa malik olduğunu təsdiq edən sənədlərin surəti (təhsil haqqında sənəd və ya beynəlxalq səviyyədə tanınan sertifikat);

20-8.6.6. texniki-texnoloji infrastrukturu barədə məlumatlar.

20-8.7. Bu Qanunun 20-8.6-cı maddəsinə əsasən tələb olunan sənədlərin və məlumatların Elektron Hökumət İnformasiya Sistemi vasitəsilə müvafiq dövlət qurumundan əldə edilməsi mümkün olduqda, həmin sənədlər və məlumatlar qurumdan tələb edilmir. Belə sənədlərin və məlumatların Elektron Hökumət İnformasiya Sistemi vasitəsilə əldə edilməsi mümkün olmadığı hallarda onların təqdim edilməsi qurumun razılığı ilə sorğu əsasında müvafiq dövlət qurumundan tələb olunur və ya qurum tərəfindən təmin edilir.

20-8.8. Qurumun bu Qanunun 20-8.6-cı maddəsinə uyğun təqdim etdiyi sənədlər və məlumatlar müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən 15 (on beş) iş günü müddətində yoxlanılır. Həmin sənədlərdə və məlumatlarda aradan qaldırılması mümkün olan çatışmazlıqlar (bu Qanunun 20-8.7-ci maddəsinin tələbi nəzərə alınmaqla) aşkar edildikdə, müraciətin qeydiyyata alındığı tarixdən 20 (iyirmi) iş günündən gec olmayaraq onların aradan qaldırılması barədə məlumat quruma təqdim edilir, habelə formal tələblərə əməl olunmamasının hüquqi nəticələri ona izah edilir. Bütün çatışmazlıqlar quruma eyni zamanda bildirilməlidir.

20-8.9. Qurum həmin çatışmazlıqları məlumatı aldığı vaxtdan ən geci 20 iş günü müddətində aradan qaldırmalıdır.

20-8.10. Qurum müraciətə əlavə edilmiş sənədlərdə və məlumatlarda aşkar olunmuş çatışmazlıqları bu Qanunun 20-8.9-cu maddəsində nəzərdə tutulmuş müddətdə aradan qaldırmadıqda müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) müraciəti baxılmamış saxlayır və bu barədə qərarı 5 iş günü müddətində onlara təqdim edir.

20-8.11. Müraciətə əlavə edilmiş sənədlərdə və məlumatlarda çatışmazlıqlar aşkar edilmədikdə və ya aşkar olunmuş çatışmazlıqlar aradan qaldırıldıqdan sonra müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən CERT və ya SOC barədə məlumatlar 10 iş günü müddətində reyestrə daxil edilir və bu barədə məlumat 2 iş günü müddətində aidiyyəti quruma təqdim edilir.

20-8.12. Reyestrə daxil edilən məlumatlarda dəyişikliklər baş verdikdə və ya CERT və SOC ləğv edildikdə, müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqana (quruma) 5 iş günü müddətində elektron qaydada məlumat verilir. Məlumat daxil olduqdan sonra 5 iş günündən gec olmayaraq, müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən reyestrdə müvafiq dəyişikliklər edilir (ləğv edilən CERT-ə və ya SOC-a dair məlumatlar reyestrdə arxivləşdirilir).

20-8.13. CERT-lərin və SOC-ların fəaliyyətinin bu Qanunun 20-8.4-cü və 20-8.5-ci maddələrində qeyd edilən tələblərə uyğunluğunun yoxlanılması məqsədilə Milli CERT tərəfindən ildə bir dəfədən az olmayaraq monitorinqlər həyata keçirilir. Monitorinqlər CERT və ya SOC-un fəaliyyət göstərdiyi yerlərə getməklə və ya getmədən (hesabatlar, sorğular və digər məlumatlar əsasında) aparılır. Monitorinqin keçirilməsinə ən geci 5 iş günü qalanadək aidiyyəti CERT-ə və ya SOC-a bu barədə məlumat verilir. Monitorinq nəticəsində aşkar edilən çatışmazlıqlar Milli CERT tərəfindən müəyyən edilən müddətlərdə aradan qaldırılmalıdır.

20-8.14. Bu Qanunun 20-8.4-cü və 20-8.5-ci maddələrində qeyd edilən tələblərə sahibkarlıq subyekti olan CERT və ya SOC tərəfindən riayət olunmasının monitorinqi həmin sahibkarlıq fəaliyyətinin həyata keçirildiyi obyektlərə gəlmədən aparılır. Milli CERT-in və Milli SOC mütəxəssisləri informasiya infrastrukturunun kibertəhlükəsizliyi ilə bağlı metodiki köməklik göstərilməsi, məsləhət verilməsi və

vəziyyətin qiymətləndirilməsi üçün həmin CERT-in və ya SOC-un dəvəti ilə onun informasiya infrastrukturu obyektlərinə gələ bilərlər.

20-8.15. CERT-lərin və SOC-ların işçi heyəti fəaliyyəti zamanı informasiya infrastrukturu subyekti, onun texnoloji infrasrtukturu, informasiya ehtiyatları və onlarda olan informasiya barədə əldə olunmuş məlumatların konfidensiallığını təmin etməlidir.

20-8.16. CERT və SOC-un işçi heyəti kibertəhlükəsizlik sahəsində bilik və bacarıqlarının artırılması üçün davamlı təlimlərə cəlb edilməli, eləcə də onların bilik və bacarıqlarının artırılması, habelə sertifikatlaşdırılması təmin edilməlidir.

20-8.17. Milli SOC tərəfindən aparılan monitorinq kritik informasiya infrastrukturuna, dövlət orqanlarına (qurumlarına) məxsus, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturuna, Azərbaycan Respublikasının Mərkəzi Bankına və maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərə, eləcə də aidiyyəti üzrə müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) və Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən yaradılmış SOC-ların fəaliyyətinə şamil olunmur. Kritik informasiya infrastrukturu obyektlərinə münasibətdə fəaliyyət göstərən SOC-ların Milli SOC-la əlaqələndirilməsi və məlumat mübadiləsi kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi üzrə səlahiyyətli orqan, maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə SOC-ların Milli SOC-la əlaqələndirilməsi və məlumat mübadiləsi Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən həyata keçirilir.

Maddə 20-9. CERT-lərin vəzifələri və hüquqları

20-9.1. CERT-lərin (Dövlət CERT-i istisna olmaqla) vəzifələri aşağıdakılardır:

20-9.1.1. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturuna qarşı yönəlmiş kibertəhdidləri, kiberhücumları və kiberinsidentləri vaxtında aşkarlamaq, onların qeydiyyatını və risklərin qiymətləndirilməsini aparmaq, ilkin araşdırmaq və təhlil etmək, qarşısını almaq;

20-9.1.2. fəaliyyət göstərdiyi sahə üzrə Milli CERT tərəfindən informasiya infrastrukturunun kibertəhlükəsizlik vəziyyətinin öyrənilməsi və proaktiv kibertəhlükəsizlik tədqiqatının aparılması ilə bağlı göndərilmiş sorğuları 24 saat, rəqəmsal tədqiqatın aparılması ilə bağlı sorğuları isə 5 iş günü ərzində cavablandırmaq və tələb olunan məlumatları təqdim etmək;

20-9.1.3. ictimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturu obyektlərinin sahə üzrə fəaliyyət göstərən SOC-a inteqrasiyasını təmin etmək;

20-9.1.4. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturu obyektlərində kibertəhlükəsizlik vəziyyətinin SOC vasitəsilə fasiləsiz monitorinqini və ilkin texniki cavab tədbirlərini həyata keçirmək;

20-9.1.5. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturu subyektlərini kibertəhdidlər, kiberhücumlar, kiberinsidentlər və kibertəhlükəsizlik riskləri, habelə onların təhlilinin nəticələri barədə operativ məlumatlandırmaq;

20-9.1.6. kiberinsidentlərin idarə olunması və aradan qaldırılması üzrə operativ tədbirlər görmək, kiberinsidentlərin lokallaşdırılması və təsirlərinin minimuma endirilməsi üçün müvafiq texniki və təşkilati tədbirlər görmək;

20-9.1.7. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturu subyektləri ilə kibertəhdidlərə, kiberhücumlara və kiberinsidentlərə qarşı operativ koordinasiyanı təmin etmək;

20-9.1.8. kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə məlumatları dərhal Milli CERT-ə ötürmək, eləcə də onların statistik uçotunu aparmaq, analitik hesabatlar hazırlamaq və rüblük əsasla Milli CERT-ə təqdim etmək;

20-9.1.9. kibertəhlükəsizlik sahəsində risklərin azaldılması və kibertəhlükəsizliyin təmin edilməsi məqsədilə sahə üzrə informasiya infrastrukturu subyektlərinə tövsiyələr vermək, habelə metodiki və təşkilati dəstək göstərmək;

20-9.1.10. kibertəhlükəsizlik üzrə məlumat mübadiləsini və erkən xəbərdarlıq mexanizmlərini təşkil etmək;

20-9.1.11. kibergigiyenanın təmin edilməsi istiqamətində mütəmadi tədbirlər görmək, sahə üzrə informasiya infrastrukturu subyektlərinin kibertəhlükəsizlik üzrə hazırlıq səviyyəsinin artırılması məqsədilə təlimlər, simulyasiya məşqləri və maarifləndirici tədbirlər təşkil etmək;

20-9.1.12. kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə məlumatları bir ildən az olmayan müddətdə, araşdırmaların nəticəsinə dair məlumatları isə üç ildən az olmayan müddətdə saxlamaq;

20-9.1.13. kibertəhlükəsizlik risklərinin qiymətləndirilməsi və zəifliklərin müəyyən olunması məqsədilə informasiya infrastrukturu obyektlərinin ildə bir dəfədən az olmayaraq kibertəhlükəsizlik auditlərinin keçirilməsi ilə bağlı tədbirlər görmək;

20-9.1.14. sahə üzrə informasiya infrastrukturunun kibertəhlükəsizliyi üzrə bu Qanunun 20-7.5-ci maddəsi ilə müəyyən edilmiş ümumi və xüsusi tələbləri pozmuş şəxslərin məsuliyyətə cəlb edilməsi üçün aidiyyəti dövlət orqanlarına müraciət etmək;

20-9.1.15. bu Qanun və Azərbaycan Respublikasının digər normativ hüquqi aktları ilə müəyyən edilmiş digər vəzifələri həyata keçirmək.

20-9.2. CERT-lərin (Dövlət CERT-i istisna olmaqla) bu Qanunla müəyyən olunmuş vəzifələrini həyata keçirmək üçün aşağıdakı hüquqları vardır:

20-9.2.1. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturu obyektlərinin təhlükəsizliyində boşluqların, zəifliklərin və digər uyğunsuzluqların müəyyən edilməsi məqsədilə təsdiq edilmiş illik və ya cari planlar üzrə müdaxilə sınaqlarını və digər texniki təhlükəsizlik testlərini həyata keçirmək;

20-9.2.2. kibertəhlükəsizlik sahəsində normativ hüquqi aktların təkmilləşdirilməsi ilə bağlı Milli CERT-ə təkliflər vermək;

20-9.2.3. fəaliyyət göstərdiyi sahə üzrə informasiya infrastrukturu obyektlərinin kibertəhlükəsizlik vəziyyəti ilə bağlı məlumat və texniki göstəricilərin təqdim edilməsini informasiya infrastrukturu subyektlərindən tələb etmək;

20-9.2.4. kiberhücumların, kiberinsidentlərin və kibertəhdidlərin araşdırılması və qarşısının alınması məqsədilə sahə üzrə informasiya infrastrukturu subyektləri ilə birgə texniki tədbirlər həyata keçirmək;

20-9.2.5. digər sahələr üzrə fəaliyyət göstərən CERT-lər və Milli CERT-i məlumatlandırmaqla beynəlxalq təşkilatlarla əməkdaşlıq etmək və məlumat mübadiləsi aparmaq;

20-9.2.6. fəaliyyət istiqamətləri üzrə yerli və beynəlxalq təcrübəni öyrənmək və uyğun təcrübənin tətbiqi ilə bağlı tədbirlər görmək, o cümlədən Milli CERT-ə təkliflər vermək;

20-9.2.7. kibertəhlükəsizlik üzrə yeni texnologiyaların və həllərin tətbiqi ilə bağlı pilot layihələr həyata keçirmək;

20-9.2.8. bu Qanun və Azərbaycan Respublikasının digər normativ hüquqi aktları ilə müəyyən edilmiş digər hüquqları həyata keçirmək.

20-9.3. Bu Qanunun 20-7.8-ci və 20-7.12-ci maddələrində nəzərdə tutulan CERT-lər Milli CERT-lə yalnız qarşılıqlı məlumat mübadiləsi (kritik informasiya infrastrukturuna münasibətdə səlahiyyətli orqan vasitəsilə) həyata keçirirlər. Bu zaman məlumat mübadiləsi Milli CERT-in həmin CERT-lərlə birgə müəyyən etdiyi formada aparılır.

20-9.4. Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə yaradılan CERT-lərin və SOC-ların fəaliyyətinin təşkili və Milli CERT-lə əlaqələndirilməsi Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən həyata keçirilir.

Maddə 20-10. İnformasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyi üzrə fəaliyyətinin təşkili

20-10.1. İnformasiya infrastrukturunun kibertəhlükəsizliyinin təmin edilməsi ilə bağlı fəaliyyətin koordinasiyası (kritik informasiya infrastrukturu, dövlət orqanlarına (qurumlarına) məxsus, habelə mühafizə olunan şəxslərin, qorunan və strateji obyektlərin informasiya infrastrukturu, Azərbaycan Respublikasının Mərkəzi Bankı və maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlər, eləcə də onlarla bağlı aidiyyəti üzrə müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) və Azərbaycan Respublikasının Mərkəzi Bankı tərəfindən yaradılmış CERT-lərlə bağlı yalnız kibertəhdid, kiberhücum və kiberinsidentlər üzrə məlumat mübadiləsi) Milli CERT tərəfindən həyata keçirilir. Milli CERT kritik informasiya infrastrukturu obyektlərinin kibertəhlükəsizliyinə münasibətdə məlumat mübadiləsini səlahiyyətli orqan vasitəsilə həyata keçirir.

20-10.2. Kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektlərinə məxsus olan informasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyi həmin orqanlar tərəfindən təmin edilir. Bu orqanların informasiya infrastrukturunun informasiya təhlükəsizliyinə və kibertəhlükəsizliyinə qarşı mövcud və yarana biləcək kibertəhdidlər, kiberhücumlar və kiberinsidentlər, onların qarşısının alınması və nəticələrinin aradan qaldırılması üzrə görülən tədbirlər barədə məlumatlar açıqlanmır və digər dövlət orqanları (qurumları), o cümlədən Milli CERT-lə və Milli SOC-la mübadilə edilmir. Kəşfiyyat və əks-kəşfiyyat fəaliyyəti subyektlərinə məxsus olan informasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyinin təmin edilməsi qaydaları həmin orqanların normativ hüquqi aktları ilə müəyyən edilir.

20-10.3. Milli CERT-in vəzifələri aşağıdakılardır:

20-10.3.1. ölkə üzrə kibertəhlükəsizlik vəziyyətinin mütəmadi monitorinqini aparmaq, kibertəhdidlər, kiberhücumlar, kiberinsidentlər və zərərverici proqram təminatı barədə məlumatları toplamaq, mübadilə etmək, sistemləşdirmək və təhlil etmək, habelə həmin məlumatların potensial təsirlərini qiymətləndirmək, məlumat mübadiləsini həyata keçirmək;

20-10.3.2. ölkənin kibertəhlükəsizliyinə yönələn kibertəhdidlərə, kiberhücumlara və kiberinsidentlərə qarşı əlaqələndirilmiş tədbirlərin görülməsini təşkil etmək;

20-10.3.3. proaktiv kibertəhlükəsizlik tədqiqatını həyata keçirmək və erkən xəbərdarlıq mexanizmlərini təşkil etmək;

20-10.3.4. kibertəhlükəsizliyin təmini üzrə CERT-lərə və informasiya infrastrukturu subyektlərinə metodiki və təşkilati köməklik göstərmək;

20-10.3.5. CERT-lərdən, digər ölkələrin analoji qurumlarından və digər mənbələrdən daxil olan məlumatlar əsasında kibertəhdidlərin qabaqlanması, qarşısının alınması və kiberinsidentlərə reaksiya üzrə koordinasiyalı fəaliyyəti təşkil etmək və zəruri texniki dəstək göstərmək;

20-10.3.6. kibertəhdidlər, kiberhücumlar, kiberinsidentlər və zərərverici proqram təminatı barədə informasiya infrastrukturu subyektlərini və CERT-ləri operativ məlumatlandırmaq, müvafiq tövsiyələr vermək;

20-10.3.7. kibertəhlükəsizliyin təmin edilməsi məqsədilə aidiyyəti dövlət orqanları (qurumları) ilə birgə standartlar, metodiki sənədlər və təlimatlar hazırlamaq, habelə onların tətbiqi ilə bağlı tədbirlər görmək;

20-10.3.8. xarici mənbəli kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə xarici dövlətlərin müvafiq qurumları və beynəlxalq təşkilatlarla məlumat mübadiləsini həyata keçirmək;

20-10.3.9. kibertəhdidlərin, kiberhücumların və kiberinsidentlərin vahid qeydiyyatını və statistik uçotunu aparmaq, analitik hesabatlar hazırlamaq;

20-10.3.10. kibertəhlükəsizlik sahəsində təlimlərin, simulyasiya məşqlərinin və sınaqların keçirilməsini təşkil etmək və əlaqələndirmək;

20-10.3.11. informasiya infrastrukturu subyektləri və CERT-lər tərəfindən kibertəhlükəsizlik sahəsində beynəlxalq standartların və ən yaxşı təcrübələrin tətbiqinə dəstək göstərmək;

20-10.3.12. kibertəhlükəsizlik sahəsində normativ hüquqi aktların təkmilləşdirilməsi ilə bağlı təkliflər hazırlamaq və aidiyyəti üzrə təqdim etmək;

20-10.3.13. dövlət orqanları (qurumları), informasiya infrastrukturu subyektləri və CERT-lər arasında kibertəhlükəsizlik sahəsində əməkdaşlığı və qarşılıqlı məlumat mübadiləsini təşkil etmək.

20-10.4. Milli CERT bu Qanunla müəyyən olunmuş vəzifələrini yerinə yetirmək məqsədilə aşağıdakı hüquqlara malikdir:

20-10.4.1. informasiya infrastrukturu subyektlərindən kibertəhlükəsizlik vəziyyəti, kibertəhdidlər, kiberhücumlar və kiberinsidentlər, habelə təhlükəsizlik riskləri barədə məlumatları bu Qanunun 1-ci maddəsinin üçüncü hissəsinin, 20-7.8-ci, 20-7.12-ci, 20-9.3-cü, 20-9.4-cü və 20-10.6-cı maddələrinin tələbləri nəzərə alınmaqla əldə etmək;

20-10.4.2. kiberinsidentlərin araşdırılması və aradan qaldırılması məqsədilə CERT-lərin, informasiya infrastrukturu subyektlərinin fəaliyyətini bu Qanunun 20-7.8-ci, 20-7.12-ci, 20-9.3-cü, 20-9.4-cü və 20-10.6-cı maddələrinin tələbləri nəzərə alınmaqla əlaqələndirmək;

20-10.4.3. kibertəhlükəsizlik sahəsində dövlət orqanları (qurumları) və digər aidiyyəti qurumlarla birgə tədbirlər həyata keçirmək;

20-10.4.4. beynəlxalq təşkilatlar və xarici ölkələrin CERT strukturları ilə əməkdaşlıq etmək, təcrübə və məlumat mübadiləsi aparmaq;

20-10.4.5. kibertəhlükəsizliyin təmin edilməsi (kibertəhdidlər, kiberhücumlar və kiberinsidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması) ilə əlaqədar informasiya infrastrukturu subyektlərinə, CERT-lərə, SOC-lara, internet provayderlərə və host provaydelərə göstərişlər vermək;

20-10.4.6. kibertəhlükəsizlik sahəsində yeni texnologiyaların və həllərin tətbiqi üzrə pilot layihələr həyata keçirmək;

20-10.4.7. kibertəhlükəsizlik risklərinin qiymətləndirilməsi və zəifliklərin müəyyən olunması məqsədilə informasiya infrastrukturu subyektini məlumatlandırmaqla informasiya infrastrukturu obyektlərinin, o cümlədən internet informasiya ehtiyatlarının kibertəhlükəsizlik üzrə monitorinqini və auditini həyata keçirmək.

20-10.5. Həyata keçirilmiş monitorinqlər və auditlər nəticəsində aşkar edilmiş zəifliklərin, boşluqların və digər uyğunsuzluqların aradan qaldırılması ilə əlaqədar Milli CERT tərəfindən müəyyən edilmiş müddət ərzində CERT-lər, informasiya infrastrukturunun subyektləri, o cümlədən internet informasiya ehtiyatlarının sahibləri tərəfindən tədbirlər görülərək nəticəsi barədə Milli CERT-ə məlumat verilməlidir.

20-10.6. Bu Qanunun 20.9-3-cü maddəsinin tələbləri nəzərə alınmaqla, CERT-lər arasındakı, həmçinin CERT-lərlə və informasiya infrastrukturu subyektləri ilə Milli CERT arasındakı fəaliyyətin əlaqələndirilməsi və fasiləsiz məlumat mübadiləsi müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqanın (qurumun) vahid kibertəhlükəsizlik platforması vasitəsilə təmin edilir.

20-10.7. CERT-lər və informasiya infrastrukturu subyektləri informasiya infrastrukturuna yönəlmiş kiberhücumlara qarşı cavab tədbirlərinin görülməsi, habelə kibertəhdidlərin və kiberinsidentlərin qarşısının alınması ilə bağlı Milli CERT-in həyata keçirdiyi fəaliyyətə zəruri şərait yaratmalı və dəstək verməlidirlər.

20-10.8. Ölkəni hədəf alan kibertəhdidlər və kiberhücumlar barədə məlumatların digər dövlətlərin bu sahədə səlahiyyətli qurumlarından əldə edilməsi, həmçinin digər ölkələri hədəf alan hücumlar barədə məlumatların ötürülməsi Milli CERT vasitəsilə və ya Milli CERT-i məlumatlandırmaqla həyata keçirilir.

20-10.9. CERT-lər, informasiya infrastrukturunun subyektləri, həmçinin ictimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturu subyektləri, o cümlədən internet provayderlər, host provayderlər və internet informasiya ehtiyatının sahibləri Milli CERT tərəfindən kibertəhlükəsizlik vəziyyətinin öyrənilməsi, proaktiv kibertəhlükəsizlik tədqiqatının aparılması məqsədilə göndərilən sorğuları 24 saat, rəqəmsal tədqiqatın aparılması ilə bağlı göndərilən sorğuları isə 5 iş günü ərzində cavablandırmalıdır.

Maddə 20-11. İnformasiya infrastrukturunun informasiya təhlükəsizliyi və kibertəhlükəsizliyi

20-11.1. İnformasiya infrastrukturunun kibertəhlükəsizliyi informasiya infrastrukturu subyekti tərəfindən informasiya infrastrukturu obyektinin kibertəhlükəsizliyində zəifliklərin, boşluqların və digər uyğunsuzluqların aşkar olunması məqsədilə risklərin qiymətləndirilməsi, təhlükəsizlik auditlərinin keçirilməsi və onların nəticələrinin aradan qaldırılması üzrə tədbirlərin görülməsi yolu ilə təmin edilir.

20-11.2. İnformasiya infrastrukturu subyekti bu Qanunun 20-7.8-ci, 20-7.12-ci, 20-9.3-cü, 20-9.4-cü, 20-10.2-ci və 20-10.6-cı maddələrinin tələbləri nəzərə alınmaqla, informasiya infrastrukturu obyektlərinə qarşı yönəlmiş kiberinsident və kiberhücumlar barədə məlumatın onların aşkarlandığı andan dərhal sonra Milli CERT-ə təqdim olunmasını təmin etməlidir.

20-11.3. İnformasiya infrastrukturu subyektinin müraciəti əsasında kibertəhlükəsizlik və proaktiv kibertəhlükəsizlik tədqiqatı üzrə xidmətlər Milli CERT tərəfindən ödənişli əsaslarla həyata keçirilir. Ödənişin məbləği tərəflər arasında bağlanılan müqavilə əsasında müəyyən edilir.

20-11.4. Müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən kiberinsidentləri aşkarlama, ölçmə meyarları və indikatorları müəyyənləşdirilərək həmin orqanın (qurumun) rəsmi internet informasiya ehtiyatında yerləşdirilir və mütəmadi yenilənməsi təmin edilir.

20-11.5. CERT-lər, SOC-lar, həmçinin informasiya infrastrukturu subyektləri, o cümlədən internet informasiya ehtiyatlarının sahibləri, internet provayderlər və host provayderlər tərəfindən Milli CERT-in kibertəhlükəsizliyin təmin edilməsi (kibertəhdidlərin, kiberhücumların və kiberinsidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması) ilə əlaqədar göstərişlərinin yerinə yetirilməməsi, informasiya infrastrukturuna yönəlmiş kibertəhdidlər, kiberhücumlar və kiberinsidentlər barədə məlumatların dərhal Milli CERT-ə təqdim edilməməsi, eləcə də Milli CERT-in informasiya infrastrukturunun kibertəhlükəsizlik vəziyyətinin öyrənilməsi və proaktiv kibertəhlükəsizlik tədqiqatının aparılması məqsədilə göndərdiyi sorğuların 24 saat, rəqəmsal tədqiqatın aparılması ilə bağlı göndərdiyi sorğuların isə 5 iş günü ərzində cavablandırılmaması, kiberinsidentlərin və kiberhücumların real vaxt rejimində fasiləsiz monitorinqinin və onlara qarşı ilkin texniki cavab tədbirlərinin həyata keçirilməməsi, eləcə də belə fəaliyyətlər nəticəsində əldə edilən məlumatların dərhal Milli SOC-a ötürülməməsi, rəqəmsal tədqiqatın və proaktiv kibertəhlükəsizlik tədqiqatına şəraitin yaradılmaması və reyestrə daxil edilmədən CERT və SOC kimi fəaliyyətin göstərilməsi, ictimai əhəmiyyətli funksiyaları yerinə yetirən informasiya infrastrukturunun kibertəhlükəsizliyi üzrə ümumi və xüsusi tələblərin (informasiya infrastrukturunun subyektləri, o cümlədən internet provayderlər, host provayderlər və internet informasiya ehtiyatının sahibləri tərəfindən) yerinə yetirilməməsi qanunla müəyyən edilmiş məsuliyyətə səbəb olur.

20-11.6. Domen adı “az” (“gov.az” istisna olmaqla) ölkə kodlu yüksək səviyyəli domen zonasında yerləşən internet informasiya ehtiyatlarının sahibləri tərəfindən Milli CERT-in kibertəhlükəsizliyin təmin edilməsi (kibertəhdidlər, kiberhücumlar və kiberinsidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması) ilə əlaqədar göstərişlərinin yerinə yetirilməməsi domen adının “az” ölkə kodlu yüksək səviyyəli domen zonasında olan qeydiyyatının xitamı, domen adına texniki xidmətin dayandırılması üçün əsasdır. Bu halda Milli CERT domen adının qeydiyyatını aparan orqandan domen adının qeydiyyatına xitam verilməsini, ona texniki xidmətin dayandırılmasını (o cümlədən məhkəmə qaydasında) tələb edə, maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərə münasibətdə isə həmin tədbirlərin görülməsi üçün Azərbaycan Respublikasının Mərkəzi Bankına müraciət edir.

Maddə 20-12. Rəqəmsal tədqiqatın aparılması

20-12.1. İnformasiya infrastrukturu obyektlərində baş vermiş kiberinsidentlər barədə əldə edilən məlumatlar əsasında Rəqəmsal tədqiqat mərkəzi tərəfindən onların risk əsaslı qiymətləndirilməsi aparılır. Qiymətləndirilmənin nəticəsinə uyğun olaraq Rəqəmsal tədqiqat mərkəzi rəqəmsal tədqiqatı aparılmalı olan kiberinsidentləri müəyyən edir.

20-12.2. Rəqəmsal tədqiqat mərkəzi tərəfindən sahə üzrə fəaliyyət göstərən CERT-lər kiberinsidentlərin rəqəmsal tədqiqatının aparılmasına cəlb edilə bilərlər.

20-12.3. Rəqəmsal tədqiqat zamanı CERT-lər və ya Rəqəmsal tədqiqat mərkəzi tərəfindən əldə olunan məlumatların bütövlüyü qorunmalı, onların dəyişdirilməsinə, silinməsinə və ya saxtalaşdırılmasına yol verilməməli, rəqəmsal tədqiqat zamanı beynəlxalq kibertəhlükəsizlik standartlarına uyğun metod və vasitələrdən istifadə olunmalıdır.

20-12.4. Rəqəmsal tədqiqat prosesi CERT-lər və ya Rəqəmsal tədqiqat mərkəzi tərəfindən sənədləşdirilməli, rəqəmsal dəlillərin əldə edilməsi, saxlanılması, ötürülməsi, təhlili mərhələləri həmin sənəddə ardıcıl və izlənilə bilən formada əks olunmalıdır.

20-12.5. Rəqəmsal tədqiqat nəticəsində əldə olunan rəqəmsal dəlillər və rəqəmsal tədqiqata dair sənədlər Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində, “Əməliyyat-axtarış fəaliyyəti haqqında”, “Kəşfiyyat və əks-kəşfiyyat fəaliyyəti haqqında” qanunlarında və digər normativ hüquqi aktlarında müəyyən edilmiş tədbirlərin görülməsi üçün müvafiq dövlət orqanına (qurumuna) təqdim edilir.

20-12.6. Rəqəmsal tədqiqatın rəsmiləşdirilməsi və nəticəsinə dair məlumatlar və sənədlər Rəqəmsal tədqiqat mərkəzi tərəfindən 3 ildən az olmayan müddətdə saxlanılmalıdır.”.

İlham Əliyev
Azərbaycan Respublikasının Prezidenti

Bakı şəhəri, 14 iyul 2026-cı il
№ 454-VIIQD