

## Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli Sərəncamı ilə təsdiq edilmişdir

# Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası

### 1. Qısa xülasə

Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin əsas istiqamətlərindədir. Ölkənin sosial-iqtisadi tərəqqisinin aparıcı qüvvəsi olan informasiya-kommunikasiya texnologiyalarının (bundan sonra - İKT) dinamik inkişafı bu sahədə mövcud olan və yeni yaranan risklərin təhlilinin aparılmasını, mühafizə obyektlərinin dəqiqləşdirilməsini, onların aid olduğu informasiya infrastrukturalarının funksional dayanıqlılığını, bu infrastrukturardan istifadə edən subyektlərin hüquq və qanuni maraqlarını, fəaliyyətin davamlılığını təmin etmək üçün qabaqalıcı və bərpəedic tədbirlərin müəyyənəndirilmiş səviyyədə görülməsini, informasiya təhlükəsizliyini idarəetmə alətlərinin davamlı təkmilləşdirilməsini şərtləndirir.

Qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması istər milli, istərsə də beynəlxalq səviyyədə əsas məsələyə çevrilmişdir. Bu fəaliyyətdə insan, cəmiyyət və dövlət maraqlarının qorunması başlıca məqsəddir. Son zamanlar Azərbaycanın informasiya məkanına, o cümlədən onun tərkib hissələrinə (dövlət, özəl və qeyri-hökumət qurumlarının, fiziki şəxslərin sahib olduğu informasiya ehtiyatlarına və infrastrukturalarına, bu ehtiyatlarda olan məlumatların həyat boyu proseslərinə, həmin proseslər üçün istifadə olunan maddi və qeyri-maddi obyektlərə və onlar arasında əlaqələrə) qarşı texnoloji cəhətdən çoxşaxəli hücumlar genişlənməkdədir.

İnformasiya təhlükəsizliyi informasiya sahəsində milli təhlükəsizliyə təhdidləri müəyyən etmək, bu təhdidlərin istifadə edə biləcəyi zəifliklərin, boşluqların və təhdid nəticəsində yarana bilən fəsadların aradan qaldırılması və ya övvəldən təyin edilmiş hədlərə qədər azaldılması üçün hüquqi, təşkilati,

əməliyyat-axtarış, kəşfiyyat və əks-kəşfiyyat, elmi-texniki və təhsil, informasiya-təhlil, kommunikasiya, kədr təminatı, iqtisadi və digər sahələr üzrə tədbirləri əlaqələndirilmiş qaydada təşkil, icra, nəzarət və davamlı təkmilləşdirmək üçün qanunvericiliklə müəyyən edilən mühafizə üsulları və vasitələri ilə təmin edilir.

Kibertəhlükəsizlik sahəsində milli ekosistemin formalaşdırılması və inkişafı istiqamətində aparılmış əməli fəaliyyət ölkəmizin beynəlxalq reytinglərdə mövqeyinin ciddi şəkildə yaxşılaşdırılması ilə nəticələnmişdir. Azərbaycan Beynəlxalq Telekomunikasiya İttifaqının tərtib etdiyi "Qlobal kibertəhlükəsizlik indeksi 2020" (Global Cybersecurity Index, GCI) reytingində mövqeyini 15 pillə yaxşılaşdıraraq, 194 ölkə arasında 89.31 xal ilə 40-cı yerdə qərarlaşmışdır.

"Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası" (bundan sonra - Strategiya) dövlətin, cəmiyyətin və insanların müasir İKT-dən təhlükəsiz istifadəsinin təmin edilməsi üçün milli informasiya təhlükəsizliyi səviyyəsinin yüksəldilməsinə, dövlət və özəl şəbəkələrin, kritik informasiya infrastrukturalarının təhlükəsizliyinin təmin olunmasına aid tədbirlərin müəyyənəndirilməsinin və həyata keçirilməsinin təşkilinə, həmçinin fərdi məlumatların mühafizəsinə, Azərbaycan Respublikasının Konstitusiyası ilə təsbit edilmiş insan hüquq və azadlıqlarına riayət edilməsinə daha əlverişli şəraitin yaradılmasına xidmət edir.

Strategiya Azərbaycan Respublikasının Konstitusiyasına və digər normativ hüquqi aktlarına, o cümlədən "Milli təhlükəsizlik haqqında", "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının qanunlarına, Azərbaycan Respublikası Prezidentinin 2007-ci il 23 may tarixli 2198 nömrəli Sərəncamı ilə təsdiq edil-

miş "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası"na, habelə informasiya təhlükəsizliyi üzrə Azərbaycan Respublikasının tərəfdar çıxdığı beynəlxalq müqavilələrə əsaslanır.

Strategiya informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində Azərbaycan Respublikasında ilk strategiya olmaqla, ölkədə informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə dövlət siyasətinin tərkib hissəsidir və bu sahədə fəaliyyətin əsas məqsədlərini, prinsiplərini, istiqamətlərini və prioritet vəzifələrini müəyyən edir.

Strategiyada qeyd olunan məsələlər həm milli, həm də ümumbəşəri xarakter daşıyır, insanların, cəmiyyətin və dövlətin maraqlarını nəzərə alaraq, dövlət, özəl və qeyri-hökumət təşkilatlarına, fiziki şəxslərə şamil edilir. İnsanların, cəmiyyətin və dövlətin həyatı əhəmiyyətli bütün maraqlarının daha yüksək və təkmil səviyyədə qorunması hazırda həm də ölkənin informasiya təhlükəsizliyi və kibertəhlükəsizlik siyasətinin əsas məqsədi kimi müəyyənəndirilir və onun dinamik inkişaf tələblərinə cavab verməsi nəzərdə tutulur.

Strategiyada informasiya, informasiyalaşdırma və informasiyanın mühafizəsi sahəsində münasibətləri tənzimləyən Azərbaycan Respublikasının qanunlarında, digər müvafiq normativ hüquqi aktlarda, həmçinin texniki normativ hüquqi aktlarda müəyyən olunmuş anlayışlardan istifadə edilir.

### 2. Qlobal trendlər

2.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində fəaliyyət üçün aşağıda göstərilən müasir və yeni çağırışlar nəzərə alınır, qabaqcıl təcrübələrdən istifadə edilir:

2.1.1. informasiya təhlükəsizliyini real vaxt rejimində ("online") qiymətləndirmə və mühafizənin səmərəliliyini mütəmadi qiymətləndirmə texnologiyaları;

2.1.2. kibercinayətkarlığın xidmət kimi ("cyber-crime as a service") beynəlxalq səviyyədə yayılmasına əks-cavab olaraq kibertəhlükəsizlik xidmətlərini milli və beynəlxalq səviyyələrdə şəbəkələşdirmə və bununla daha da gücləndirmə, kibertəhlükəsizlik toru ("cybersecurity mesh") arxitekturası;

2.1.3. informasiya təhlükəsizliyi ilə əlaqəli olan sahələrlə idarəetmə sistemləri arasında harmonizasiya, qurumdaxili və qurumlararası koordinasiya, beynəlxalq əməkdaşlıq, informasiya təhlükəsizliyini istiqamətləndirmə şuraları ("cyber-savvy boards"), informasiya təhlükəsizliyi ekosistemi;

2.1.4. informasiya təhlükəsizliyi ilə əlaqəli olan təchizat zəncirlərini standartlaşdırma tədbirləri;

2.1.5. identifikasiya - çoxfaktorlu autentifikasiya və texniki vasitələrin identifikasiyası - konfidensiallığı gücləndirmək üçün kritik texnologiyalar;

2.1.6. "məsafədən iş" in geniş yayılması və bundan yaranan kibertəhlükəsizlik riskləri, mobil kibertəhlükəsizlik texnologiyaları;

2.1.7. qurumların texniki xidmətlərində və informasiya təhlükəsizliyində hiperavtomatlaşdırma və burada informasiya təhlükəsizliyi tələblərinin pozulma hallarından yaranan zəiflikləri, riskləri idarəetmə texnologiyaları;

2.1.8. süni intellekt mühəndisliyi, idarəetmə üzrə qərarvermədə, riskləri, insidentləri müəyyən etmədə, o cümlədən funksionallıqda anomaliyaları və konfigurasiyada sanksiyasız dəyişiklikləri dərhal aşkar etmədə, qabaqalıcı (preventiv) və bərpəedic (korrektiv) əks-tədbirləri hazırlamaqda süni intellekt, rəqəmsal etimad ("digital trust") texnologiyaları;

2.1.9. "bulud" xidmətlərinin inkişafı, genişlənməsi və həm də onlara təhdidlərin artması, "paylanmış bulud" ("distributed cloud") texnologiyaları;

2.1.10. informasiya təhlükəsizliyi sahəsində risk-yönümlü modelləşdirmə, simulyasiya və kiberpoliqonlar texnologiyaları;

2.1.11. internetdə davranış mədəniyyəti, sosial mühəndislik "hücumlar"ın və onlara əks-tədbirlərin daha da "ağıllı" olması, maarifləndirmə işinin genişləndirilməsi;

2.1.12. kibercinayətkarlığının çoxalması, o cümlədən pandemiya kontekstində sürətlə artan kibertəhdidlər;

2.1.13. kibertəhdidlərə qarşı mübarizədə daha mükəmməl texnoloji həllərin tətbiqi zərurəti;

2.1.14. kibercinayətkarlığın törədilmə üsul və vasitələrinin sürətli diversifikasiyası, o cümlədən kriptovalyutaların geniş vüsət alması və müxtəlif cinayətkar məqsədlərlə istifadə olunması;

2.1.15. "ransomware" hücumlarının artması və bu hücumlara qarşı intensiv maarifləndirmə təşəbbüslərinin icra olunması;

2.1.16. "insayder" təhdidlərinin artması və bu təhdidlərə qarşı mübarizənin gücləndirilməsi;

2.1.17. kibertəhdidlərlə mübarizə aparılması üçün "çoxfaktorlu autentifikasiya" metodlarından geniş istifadə zərurətinin yaranması;

2.1.18. insanların, proqram təminatı vasitələrinin internetdə (və digər qlobal şəbəkədə) ona qoşulmuş texniki təminat vasitələri ilə qarşılıqlı fəaliyyəti üçün yaranmış virtual mühitdə - kiberməkanda mühafizəsi tələb olunan rəqəmsallaşdırılmış məlumatların sürətlə çoxalması ilə əlaqədar təkmilləşdirilmiş mühafizə mexanizmlərindən istifadəyə dair ehtiyacın artması.

### 3. Mövcud vəziyyətin təhlili

Son illər ölkəmizdə kiberməkanda dövlət müstəqilliyinin, milli maraqların qorunması, informasiya

təhlükəsizliyi sahəsində vahid dövlət siyasətinin təkmilləşdirilməsi və informasiya təhlükəsizliyinin texnoloji infrastruktur komponentlərinin yaradılması istiqamətində məqsədyönlü işlər aparılır.

Vətən müharibəsinin ilk günlərindən kiberməkanda mümkün təxribatların və döyüş əməliyyatları ilə bağlı məlumatların sızmasının qarşısını almaq məqsədilə Azərbaycanın internet seqmentinin, həmçinin sosial şəbəkələr, mesencerlər və digər elektron kommunikasiya platformaları vasitəsilə aparılan məlumat mübadiləsinin təhlükəsizliyinin təmin olunması istiqamətində kompleks tədbirlər həyata keçirilmişdir. İşğaldan azad olunmuş ərazilərdə müasir informasiya texnologiyalarına əsaslanan infrastrukturun yaradılması, "Ağıllı şəhər" və "Ağıllı kənd" konsepsiyalarının reallaşması regional sabitliyi və inkişafı şərtləndirən amillərdən biridir. Bu ərazilərdə dövlət və ictimai təhlükəsizliyin təmin olunması üçün mümkün terror-təxribat və digər nöqtələrin müəyyən edilməsi, çevik əks-tədbirlərin hazırlanması məqsədilə "big data", "cloud", "machine learning" texnologiyaları əsasında yaradılmış müvafiq həllərin tətbiqi nəzərdə tutulur.

Qlobal pandemiya şəraitində insanların, biznes dairələrinin, dövlət orqanlarının (qurumlarının) fəaliyyətinin əsas hissəsi kiberməkana keçmiş, məhsus və təşkilatların bir qismi işçilərini məsafədən işə cəlb etmişdir. Əksər hallarda bu keçid sürətlə baş vermiş və istifadə olunan texnologiyaların və proqram təminatının təhlükəsizlik baxımından qiymətləndirilməsi lazımı qaydada aparılmamışdır. Məsafədən iş üçün tətbiq olunmuş proqram təminatının müxtəlifliyini və çoxsaylı istehsalçılara məxsus olduğunu nəzərə alaraq, fərdi məlumatların, kommuniya sirlərinin və digər qorunan informasiyanın sızması təhlükəsi ötən illərlə müqayisədə dəfələrlə artmışdır.

*Ardı 11-ci səh.*



## Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyi dair 2023-2027-ci illər üçün Strategiyası

### Əvvəli 10-cu səh.

Bununla bağlı, qorunan informasiyanın mühafizəsi istiqamətində əlavə tədbirlər həyata keçirilməsi zərurəti yaranmışdır.

Ünvanı, ölkədə kibercinayətlərlə mübarizə imkanlarının genişləndirilməsi üçün bir sıra mühüm hüquqi və təşkilati tədbirlər görülmüşdür. İnformasiya təhlükəsizliyi, habelə kibertəhlükəsizlik üzrə hüquqi bazanın möhkəmləndirilməsi məqsədilə Azərbaycan Respublikası aidiyyəti beynəlxalq konvensiya və proqramlara qoşulmuş, milli qanunvericilik bazası inkişaf etdirilmişdir.

2001-ci il noyabrın 23-də Budapeşt şəhərində imzalanmış "Kibercinayətkarlıq haqqında" Konvensiyanın müvafiq bəyanatlarla və qeyd-şərtlərlə Azərbaycan Respublikasının 2009-cu il 30 sentyabr tarixli Qanunu ilə təsdiq edilmiş kibercinayətkarlıqla mübarizə sahəsində atılan mühüm addımlardan biridir. Həmin Konvensiyanın müddəalarından irəli gələrək, Azərbaycan Respublikasının Cinayət Məcələsinə müvafiq dəyişikliklər edilmişdir.

Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyində fəaliyyət göstərən standartlaşdırma üzrə "İnformasiya-kommunikasiya texnologiyaları" Texniki Komitəsi (TK05) tərəfindən informasiya təhlükəsizliyi üzrə beynəlxalq standartların əsasında 18 identik milli standart hazırlanmış və müvafiq qaydada dövlət qeydiyyatına alınmışdır.

Azərbaycan Respublikasında informasiya təhlükəsizliyi sahəsindəki əsas vəzifələrin yerinə yetirilməsi, milli informasiya resurslarının qorunması və təhdidlərin qarşısının alınması və bu sahədə effektiv tədbirlərin gücləndirilməsi məqsədilə informasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikası Prezidentinin 2012-ci il 26 sentyabr tarixli 708 nömrüli Fərmanı ilə müəyyən edilmişdir. Bu Fərmanla informasiya təhlükəsizliyi məsələlərinə məsul olan qurumlar - Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi və Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzi yaradılmışdır. "Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin 2013-cü il 5 mart tarixli 833 nömrüli Fərmanında dəyişiklik edilmişdir" Azərbaycan Respublikası Prezidentinin 2018-ci il 19 sentyabr tarixli 276 nömrüli Fərmanı ilə qeyd olunan mərkəzə xidmət statusu verilmişdir. Bununla yanaşı, "Xüsusi dövlət mühafizəsi sahəsində idarəetmənin təkmilləşdirilməsi haqqında" Azərbaycan Respublikası Prezidentinin 2020-ci il 16 mart tarixli 957 nömrüli Fərmanı ilə Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi Dövlət Agentliyinin bazasında müstəqil olaraq Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti yaradılmışdır.

Azərbaycan Respublikası Prezidentinin 2014-cü il 2 aprel tarixli 359 nömrüli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"da müxtəlif sahələrin inkişafı kimi, informasiya təhlükəsizliyinin təmin edilməsi də öz əksini tapmışdır. Həmin Milli Strategiyanın əsas istiqamətlərindən biri olan "İnformasiya təhlükəsizliyinin təmin edilməsi"nin məqsədlərinə çatmaq üçün ölkənin milli informasiya məkanının və kritik infrastrukturlarının, o cümlədən informasiya infrastrukturunun informasiya təhlükəsizliyini təmin edən sistemlərin inkişaf etdirilməsi nəzərdə tutulmuşdur. Bundan irəli gələrək, global informasiya məkanında Azərbaycan Respublikasının milli maraqlarının qorunması, informasiya təhlükəsizliyi sisteminin inkişaf etdirilməsi və İKT-dən təhlükəsiz istifadə mədəniyyətinin yüksəldilməsi həlli vacib olan əsas məsələlərdən biri kimi müəyyənləşdirilmişdir.

Ölkədə informasiya məkanının təhlükəsizliyinin təmin edilməsi, dövlət və cəmiyyət üçün xüsusi əhəmiyyət kəsb edən infrastruktur obyektlərinin informasiya sistemləri və ehtiyatlarının kibercinayətlərdən qorunması, belə təhdidlərin qabaqlanması, qarşısının alınması və aradan qaldırılması sahəsində fəaliyyət göstərən dövlət qurumlarının işinin əlaqələndirilməsini təmin etmək üçün Azərbaycan Respublikası Prezidentinin 2018-ci il 29 mart tarixli 3851 nömrüli Sərəncamı ilə İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyası yaradılmışdır.

Bundan başqa, Azərbaycanda TIER III səviyyəli, ISO/IEC 20000 və ISO/IEC 27001 standartlarına uyğun Data Markəzı yaradılmış və fəaliyyəti təmin edilmiş, "Elektron hökumət" in inkişafı, "Rəqəmsal hökumət"ə keçidin təmin edilməsi, dövlət qurumlarının informasiya texnologiyalarına, elektron xidmətlərinin yaradılmasına və göstərilməsinə tələb olunan dövlət xərclərinin optimallaşdırılması, informasiya sistemlərinin fəaliyyətinin daha müasir standartlar əsasında keyfiyyəti, dayanıqlı və təhlükəsiz infrastrukturda təhlükəsiz təmin edilməsi, vətəndaşların bu imkanlardan sərbəst istifadəsi məqsədilə "bulud texnologiyası"nın tətbiqi məqsədilə "Hökumət buludu"nun ("G-cloud") yaradılmasına başlanılmışdır.

"Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin 2021-ci il 17 aprel tarixli 1315 nömrüli Fərmanına

əsasən, Azərbaycan Respublikasında kritik informasiya infrastrukturunun və onun tərkibinə daxil olan informasiya sistemlərinin, informasiya-kommunikasiya şəbəkələrinin və avtomatlaşdırılmış idarəetmə sistemlərinin təhlükəsizliyinin gücləndirilməsi məqsədilə ardıcıl tədbirlər həyata keçirilir.

Azərbaycanda informasiya təhlükəsizliyinin təmin olunması məsələləri yuxarıda qeyd edilən hüquqi aktlarla yanaşı, "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda və Azərbaycan Respublikası Prezidentinin 2007-ci il 23 may tarixli 2198 nömrüli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası"nda öz əksini tapmışdır.

Azərbaycan Respublikasının qanunvericiliyinə əsasən, ölkədə informasiya təhlükəsizliyinin, həmçinin kibertəhlükəsizliyinin təmin edilməsi sahəsində səlahiyyət və məsuliyyət bölgüsü müəyyənləşdirilmişdir. Dövlət orqanları səlahiyyətlərinə uyğun olaraq informasiya təhlükəsizliyinin müxtəlif məsələləri ilə məşğulduqları, informasiya sistemlərinin mükiyyətləri və ya sahibləri olan dövlət qurumları və özəl müəssisələr, həmçinin fiziki şəxslər onların fəaliyyətinin kibertəhlükəsizliyinə məsuliyyət daşıyırlar.

Beynəlxalq təcrübəyə uyğun olaraq ölkədə kibertəhlükəsizlik insidentlərinə cavabvermə qrupları (CERT) fəaliyyət göstərir. Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidməti - Milli CERT (www.cert.az) ölkə üzrə kibertəhlükəsizliyin pozulmasına yönəlmis hərəkətlərin aşkarlanmasını, qarşısının alınması üçün preventiv tədbirlər həyata keçirməsini təmin edən əlaqələndirici qurum kimi çıxış edir. Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi (www.cert.gov.az) dövlət qurumlarının kibertəhlükəsizliyinin pozulmasına yönəlmis hərəkətlərin aşkarlanmasını, qarşısının alınması üçün preventiv tədbirlərin görülməsini, eləcə də onların təhlükəsiz internet şəbəkəsi ilə təmin edilməsini və 24/7 Təhlükəsizlik Əməliyyatları Mərkəzi (SOC) vasitəsilə təhlükəsizliyinin nəzərdə saxlanılmasını həyata keçirir. Milli Elmlər Akademiyasının Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi "AZScienceCERT" (www.sciencecert.az) elm-kompüter şəbəkəsinin təhlükəsizliyinə məsuldur.

Sürətlə qloballaşan dünyada milli informasiya məkanına təhdidlər də global xarakter daşıyır. Buna görə də kibertəhlükəsizliyin təminatının mühüm şərtlərindən biri beynəlxalq əməkdaşlığın mövcudluğudur.

Azərbaycan Respublikası informasiya təhlükəsizliyi və kibercinayətkarlıqla mübarizə məsələlərinin beynəlxalq təşkilatlarla qarşılıqlı əlaqədə qurur və əməkdaşlıq edir. Həmçinin Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidməti tərəfindən "Kibercinayətkarlıq haqqında" Konvensiyaya uyğun olaraq, kiberməkanda törədilən cinayətlərin aradan qaldırılması məqsədilə xarici həmkarlarla təcili köməyin (verilənlərin mühafizəsi) təmin olunması ilə bağlı fəaliyyət həyata keçirilir.

Azərbaycan Respublikasının hətərövləli inkişafı, dövlət idarəçiliyində, iqtisadi və sosial sahələrdə, insanlarn gündülik tələbatlarının ödənilməsində informasiya texnologiyalarının və vasitələrinin geniş tətbiqi və əhəmiyyətinin artması təhlükəsizliyin təmin edilməsi baxımından bu sahədə mühafizə tədbirlərinin gücləndirilməsini zəruri edir. Bu məqsədlə beynəlxalq təcrübəyə əsaslanaraq, informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə dövlət siyasətinin prioritet istiqamətlərinin müəyyənləşdirilməsi, təhdidlərin və real şəraitin, o cümlədən problemlərin diaqnoz, obyektiv, elmi baxımdan düzgün təhlil olunması, qiymətləndirilməsi və informasiya təhlükəsizliyi sahəsində səmərəli fəaliyyətin təşkili Strategiyada öz əksini tapmışdır.

Milli informasiya təhlükəsizliyinə və kibertəhlükəsizliyə təsir edən amillər GZİT (Güclü Tərəflər, Zəif tərəflər, İmkanlar, Təhdidlər) analiz metoduna uyğun olaraq mütləmədi qiymətləndirilir. Bu amillər Strategiyada nəzərə alınmışdır və prioritet istiqamətlər, vəzifələr, müvafiq həll yolları, eləcə də kompleks tədbirlər planı müəyyənləşdirilmişdir.

Strategiyamızın hazırlanması zamanı qabaqcıl beynəlxalq təcrübə, region və Avropa dövlətlərinin müvafiq strategiyaların araşdırılması və ölkəmizdə tətbiqi baxımında təhlil edilmişdir.

Hazırda Avropa İttifaqına daxil olan 27 ölkənin, Beynəlxalq Telekomunikasiya İttifaqına üzv olan 193 ölkənin isə 108-nin müəyyən dövrüli əhatə edən informasiya təhlükəsizliyi və kibertəhlükəsizlik strategiyaları mövcuddur.

Beynəlxalq təşkilatların hesabatlarına ölkələrin kibertəhlükəsizlik üzrə reytinginə təsir edən əsas meyarlardan biri bu sahədə informasiya təhlükəsizliyi və ya kibertəhlükəsizlik strategiyasının olmasıdır.

### 4. Hədəf göstəricilər

4.1. Strategiyanın əhatə etdiyi dövr ərzində aşağıda qeyd olunan hədəflərə nail olunması nəzərdə tutulur.

4.1.1. informasiya təhlükəsizliyi və kibertəhlükəsizlik riskləri reystrinin formalaşdırılmasının və aparılmasının təşkili;

4.1.2. informasiya təvacüvünə və həqiqətlərin təhrif edilməsinə, milli dəyərlərin pozulmasına aid təhdidlərin qarşısını ala bilən müasir texnologiyaların (o cümlədən süni intellektə əsaslanan texnologiyaların) işlənilməsi üçün fəaliyyətin gücləndirilməsi;

4.1.3. informasiya təhlükəsizliyi hadisələrinin monitorinqinin, insidentləri və kritik halları aşkarlama meyarlarının müəyyən edilməsinin və tətbiqinin təmin olunması;

4.1.4. informasiya mühafizəsinin texniki, kriptotrafik, proqram və digər vasitələr üzrə təminatın təkmilləşdirilməsi, bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi;

4.1.5. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində startapların fəaliyyətinin gücləndirilməsi;

4.1.6. informasiyalaşdırma obyektlərində, texniki xidmət və informasiya xidməti subyektlərində informasiya təhlükəsizliyini idarəetmə sistemlərinin (İTİS-lərin) formalaşdırılmasının, onların səmərəlilik səviyyələrinin ölçülməsinin təmin edilməsi;

4.1.7. fərdi məlumatların mühafizəsinin gücləndirilməsi;

4.1.8. İKT-xidmət subyektlərində fəaliyyətin təkmilləşdirilməsi;

4.1.9. "ağıllı" sistemlərin təhlükəsizliyinin təkmilləşdirilməsi;

4.1.10. mediada, o cümlədən milli rəqəmsal efir məkanında informasiya təhlükəsizliyi və kibertəhlükəsizliyin davamlı təkmilləşdirilməsi;

4.1.11. kritik informasiya infrastrukturunu obyektlərinin təhlükəsizliyinin təmini;

4.1.12. fəvqəladə hallarda, müharibə şəraitində kritik informasiya infrastrukturlarının təhlükəsizliyini və idarə edilməsini təmin etmək üçün təşkilatı əsasları yaradılması;

4.1.13. kibercinayətkarlığa qarşı mübarizə, o cümlədən kibercriminalistika sahəsində fəaliyyətin gücləndirilməsi;

4.1.14. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin real təbiiqatı nəticəsində rəqəbatdə davamlı məhsulların işlənməsi və hazırlanması;

4.1.15. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində fəaliyyət üçün kompetensiya (bilik, bacarıq və səriştə) tələbatları, tədris və təlim proqramları, maarifləndirmə materialları bazasının formalaşdırılması və aktuallığının davamlı təmin olunması;

4.1.16. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində kadr hazırlığının və informasiya təhlükəsizliyi üzrə ixtisaslaşmış struktur bölmələrinin müvafiq kadrlarla təminatının gücləndirilməsinin təmin olunması;

4.1.17. informasiya təhlükəsizliyi sahəsində ali təhsil almış məzunların ixtisası üzrə məşğulluq səviyyəsinin yüksəldilməsi;

4.1.18. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə ixtisaslaşan yeniyetmə və gənclərin təhdidlərdən mühafizəsinin təşkili;

4.1.19. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində qabaqcıl beynəlxalq hüquqi və texniki normativ aktların öyrənilməsi, informasiya təhlükəsizliyi və əlaqəli sahələrə aid beynəlxalq mənbələrin praktiki tövsiyələrinin tətbiqi;

4.1.20. cəmiyyətdə geniş maarifləndirmə və məlumatlandırma nəticəsində informasiya təhlükəsizliyi və kibertəhlükəsizliyi mədəniyyətinin yüksəldilməsinin təmin edilməsi;

4.1.21. internetdən gələn global təhdidlərdən, zərərli informasiyalardan və yaranan fəsadlardan uşaqların mühafizəsi;

4.1.22. informasiya təhlükəsizliyi və kibertəhlükəsizlik ekosisteminin formalaşdırılması;

4.1.23. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə idarəetmə sahəsində beynəlxalq təşkilatlarla əməkdaşlığın inkişaf etdirilməsi;

4.1.24. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə beynəlxalq reytinglərdə ölkəmizin mövqeyinin yaxşılaşdırılması;

4.1.25. informasiya təhlükəsizliyi üzrə beynəlxalq standartların ölkədə tətbiqinin genişləndirilməsi, o cümlədən müxtəlif standartlaşdırma təşkilatlarının məhsullarında ölkəmizdə vahid yanaşma ilə uyğunlaşdırılması formada istifadənin təmin olunması və İnformasiya Təhlükəsizliyi üzrə Milli Standartların davamlı təkmilləşdirilməsi;

4.1.26. informasiya təhlükəsizliyi sahəsində kadr hazırlığını təmin edən təhsil müəssisələrinin səmərəliliyinin artırılması, yeni təhsil mərkəzlərinin formalaşdırılması;

4.1.27. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə beynəlxalq şirkətlərlə birgə laboratoriyaların formalaşdırılması.

### 5. Məqsədlər

5.1. İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmini üzrə aşağıdakı məqsədlər hədəflərə nail olunmasına xidmət edən:

5.1.1. informasiya məkanında, xüsusən də kritik informasiya infrastrukturlarında təhlükəsizlik risklərinin müəyyənləşdirilməsi;

5.1.2. informasiya təvacüvünə və həqiqətlərin təhrif edilməsinə, milli dəyərlərin pozulmasına aid təhdidlərə qarşı hazırlığın gücləndirilməsi;

5.1.3. informasiya məkanında və kritik informasiya infrastrukturlarında informasiya təhlükəsizliyi struktur vahidlərinin, "CERT" şəbəkələrinin və onlar arasında qarşılıqlı fəaliyyətin davamlı təkmilləşdirilməsi;

5.1.4. informasiya təhlükəsizliyi, həmçinin kibertəhlükəsizlik sənayesinin formalaşdırılması, informasiya mühafizəsi texnologiyaları sahəsində xərçədən birbaşa əsliğin minimalaşdırılması, nəzərdə saxlanılması, proqram mühəndisliyinin və rəqəmsal iqtisadiyyatın inkişaf etdirilməsi;

5.1.5. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində innovativ həllərin və startapların təşviqi, onların dəstəklənməsi, yeni məhsul və xidmətlərin yaradılması;

5.1.6. ölkənin informasiya infrastrukturlarında risklərin, xidmətlərin, insidentlərin idarə edilməsi üçün tələb olunan əsas tədbirlərin müəyyən edilməsində sistemliyin təmin olunması, standartların və qabaqcıl təcrübənin tətbiqi, təhlükəsizlik səviyyəsinin yüksəldilməsi və bu səviyyənin ölçmə modelinin müəyyənləşdirilməsi;

5.1.7. informasiya sızması, o cümlədən fərdi məlumatların mühafizəsi üzrə təhlükəsizlik səviyyəsinin yüksəldilməsi;

5.1.8. İKT-məhsulların həyat təsiklinin optimal idarə edilməsinin, izafilyivinin minimalaşdırılmasının və adekvatlığının obyektiv qiymətləndirilməsinin təmin olunması;

5.1.9. "ağıllı" sistemlərin yaradılmasına, tətbiqinə və istifadəsinə metodiki və təhlükəsizlik dəstəyi göstərilməsi;

5.1.10. milli rəqəmsal efir məkanının kibertəhlükəsizliyinin təmin edilməsi;

5.1.11. kritik informasiya infrastrukturları obyektlərinin təhlükəsizliyinə dövlət nəzarətinin həyata keçirilməsi;

5.1.12. kritik informasiya infrastrukturlarının təhlükəsizliyinin, onların idarəetmə səviyyələrinin risklərə adekvat yüksəldilməsi;

5.1.13. kibercinayətkarlığa qarşı mübarizənin və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin aparılmasına davamlı təşkilatı dəstək verilməsinin təmin olunması;

5.1.14. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin aparılmasına davamlı təşkilatı dəstək verilməsinin təmin olunması;

5.1.15. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət sahəsi bərədə məlumatların təhlükəsizlik xassələrinin təmin olunması, müvafiq kadrların hazırlanması üçün obyektiv informasiya ilə təmin edilməsi;

5.1.16. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində kadrların hazırlanmasına və idarə olunmasına aid planlaşdırma, icra və nəzarət işlərinin optimallığının təmin olunması;

5.1.17. təhsil müəssisələri ilə dövlət və özəl sektor arasında informasiya təhlükəsizliyi üzrə kadr hazırlığına dair əməkdaşlığın genişləndirilməsinin təşkili;

5.1.18. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində milli kadr ehtiyatının təkmilləşdirilməsi və mühafizəsi, ölkə xaricinə "beyin axını"nın qarşısının alınması;

5.1.19. informasiya təhlükəsizliyinin və kibertəhlükəsizliyin normativ əsasının aktuallığının təşkili;

5.1.20. İKT-məhsulları və xidmətləri bazarında informasiya təhlükəsizliyinin və kibertəhlükəsizliyinin təmin olunması, həmçinin sifariş, isehsal, təchizat tərəflərinin qanuni maraqlarını qorumaq üçün tədbirlər görülməsi;

5.1.21. cəmiyyətdə informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinə dair zəruri biliklərin, bacarıqların artırılmasına və təbliğinə dəstək verilməsi;

5.1.22. uşaqların internetdən təhlükəsiz istifadə imkanlarını möhkəmləndirilməsinə, tövsiyələrin işlənilməsinə təşkilatı dəstək verilməsi;

5.1.23. dövlət, özəl və vətəndaş cəmiyyəti institutları və bu institutların subyektləri arasında əməkdaşlığın inkişaf etdirilməsi;

5.1.24. milli informasiya təhlükəsizliyi və kibertəhlükəsizlik ilə beynəlxalq informasiya təhlükəsizliyi arasında inteqrasiya əlaqələrinin təmin olunması;

5.1.25. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində beynəlxalq təşkilatlarla əməkdaşlığın inkişaf etdirilməsi, sahə üzrə hüquqi bazanın təkmilləşdirilməsi;

5.1.26. informasiya təhlükəsizliyi üzrə beynəlxalq standartların ölkədə geniş tətbiq olunmasına təşkilatı və metodiki dəstək verilməsi, o cümlədən müxtəlif standartlaşdırma təşkilatlarının ölkəmizdə istifadə olunan məhsulların uyğunluq baxımından vahid yanaşma ilə icmallaşdırılması və İnformasiya Təhlükəsizliyi üzrə Milli Standartların formalaşdırılması;

5.1.27. informasiya təhlükəsizliyi üzrə kadr hazırlığı üçün müasir təhsil müəssisələrinin və laboratoriyalarının formalaşdırılması.

### 6. Prioritet istiqamətlər

Azərbaycan Respublikasında informasiya təhlükəsizliyinin və kibertəhlükəsizliyinin təmin edilməsi sahəsində fəaliyyətin strateji planlaşdırılması və mərhələli olaraq həyata keçirilməsi nəzərdə tutulur.

#### 6.1. Təhdidlərin müəyyənləşdirilməsi və risklərin idarəedilməsi

Təşkilatların, insanların fəaliyyətində İKT-nin rolunun daim artdığı müasir dövrdə informasiya mühafizəsinin obyektlərinə mümkün təhdidlərin baş verə bilməsinin, bu zaman zəifliklərdən (boşluqlardan və digər uyğunsuzluqlardan) istifadənin mümkünlüyünün və fəsadların yaranma bəhdəsinin qiymətləndirilməsi zəruridir. Milli informasiya məkanında risklərin qiymətləndirilməsi Strategiyanın əsas elementlərindən biridir.

İnformasiya təhlükəsizliyinin təmin olunması üçün riskləri, xidmətləri və insidentləri idarəetmə sistemləri, o cümlədən bu sistemlərə tələb olunan əsas tədbirlər toplusu, təhlükəsizlik səviyyəsinin ölç-

mə modeli və həmin sistemləri davamlı təkmilləşdirmə mexanizmi formalaşdırılır.

Bu baxımdan müvafiq sahəyə aid təhdidlərin müəyyənləşdirilməsi və risklərin idarə edilməsi ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində həmin təhdidlərin qarşısını ala bilən müasir texnologiyalar hazırlanacaq, mühafizə qabiliyyəti yüksəldiləcəkdir.

#### 6.2. İnformasiya təhlükəsizliyi hadisələrinin aşkarlanması tədbirlərinin və mühafizə texnologiyalarının gücləndirilməsi

İnformasiya təhlükəsizliyinin təmin edilməsi risklərə adekvat olan üsul və vasitələrin (informasiya təhlükəsizliyini idarəetmə alətlərinin) seçilməsindən, onlara qoyulan mükəmməllik və etimad tələblərinə uyğun olmasından, onların imkanlarının və istifadəsinin səmərəlilik göstəricilərindən asılıdır.

Bu baxımdan informasiya təhlükəsizliyi hadisələrinin aşkarlanması tədbirlərinin və mühafizə texnologiyalarının gücləndirilməsinə dair bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində informasiya mühafizəsinin təminatı təkmilləşdiriləcək, bu sahədə yerli istehsal və yerli istehsalçılar, innovativ fəaliyyət inkişaf edəcəkdir.

#### 6.3. İnformasiya məkanının informasiya təhlükəsizliyinin təmin olunması səviyyəsinin yüksəldilməsi

İnformasiya təhlükəsizliyinin təmin edilməsi, informasiya təhlükəsizliyi risklərinin idarə olunması informasiya təhlükəsizliyinə təhdidlərin təsir ünvanı olan obyektlərin (informasiya prosesləri üçün lazım olan, mühafizəsinə tələblər qoyulan və ya zərurət olan aktivlərin), bu obyektlərin təyinatı üzrə yətərli və yararlı olmasın, bu obyektlərdə olan zəifliklərin, boşluqların və digər uyğunsuzluqların müəyyən edilməsindən və həmin obyektlərin davamlı təkmilləşdirilməsindən, həmçinin bu Strategiyada qeyd olunan vəzifələrin icrasından asılıdır.

Bu baxımdan informasiya məkanının informasiya təhlükəsizliyinin təmin olunması səviyyəsinin yüksəldilməsi ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində İKT xidmət subyektlərində fəaliyyət, həmçinin milli rəqəmsal efir məkanında kibertəhlükəsizlik davamlı təkmilləşdiriləcəkdir.

#### 6.4. Kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin edilməsi

Cəmiyyətin mühüm həyatı funksiyalarını təmin etmək üçün böyük rol malik olan, fəaliyyətindəki nasazlıqların və ya sradan çıxmasının əhəlinin sağlamlığına, təhlükəsizliyinə, iqtisadi və sosial rifahına, həmçinin dövlət qurumlarının fəaliyyətində davamlılığınə ciddi təsir göstərən infrastrukturların və ya onların əhəmiyyəti hissələrinin informasiya təhlükəsizliyinin təmin olunması xüsusilə vacibdir. Bununla yanaşı, hər hansı bir sahədə baş vermiş hadisə digər sahələrdə də zəncivari hadisələrə səbəb ola bilər. Qeyd edilən səbəblərdən kritik informasiya infrastrukturlarının təhlükəsizliyinin təmini mükiyyətə növləndirən əsas amiyaraq daim diqqət mərkəzində olmalı və bu məqsədlə müvafiq tədbirlər görülməlidir.

Bu baxımd

## Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli Sərəncamı ilə təsdiq edilmişdir

## Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası

Əvvəlki 11-ci səh.

## 8. "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün strategiyası"nın həyata keçirilməsi ilə bağlı tədbirlər planı

Tədbirlər	Əsas icraçı orqan (qurum)	Digər icraçılar	İcra müddəti	Nəticə indikatorları		
				İlkin nəticələr	Araşq nəticələr	Yekun nəticələr
<b>8.1. Prioritet 1. Təhdidlərin müəyyənəndirilməsi və risklərin idarəedilməsi</b>						
<b>8.1.1. Informasiya təhlükəsizliyi və kibertəhlükəsizlik riskləri reyestrinin formalaşdırılmasının və aparılmasının təşkili</b>						
8.1.1.1. Informasiya məkanında informasiya təhlükəsizliyinə və kibertəhlükəsizliyə təhdidlərin kateqoriyalarını müəyyən etmək və təsnifatlaşdırmaq	XRİTDX	DTX, RİNN, DİN, MN	2023 – 2024	Təhdidlərin analiz olunması	Kateqoriyaların təyin olunması	Təhdidlərin təsnifatlaşdırılması
8.1.1.2. Informasiya məkanında informasiya təhlükəsizliyinə və kibertəhlükəsizliyə təhdidlərin qarşısının alınması fəaliyyətinin səmərəli təşkili məqsədilə informasiya təhlükəsizliyi riskləri reyestrinin aparılma qaydasını müəyyən etmək	NK	XRİTDX, RİNN, DTX	2023 – 2024	İnformasiya təhlükəsizliyi riskləri reyestrinin aparılma qaydasının hazırlanması	İnformasiya təhlükəsizliyi riskləri reyestrinin aparılma qaydasının razılaşdırılması	İnformasiya təhlükəsizliyi riskləri reyestrinin aparılma qaydasının təsdiq edilməsi
8.1.1.3. Informasiya təhlükəsizliyi üzrə yaranan biləcək təhdidlərin və risklərin əvvəlcədən müəyyən edilməsi və görülməli tədbirləri proqnozlaşdırmaq məqsədilə süni intellekt əsaslı həllərin işlənilib hazırlanmasını və tətbiqini təşkil etmək	XRİTDX	DTX, RİNN, ETN	2023 – 2027	Səhə üzrə müasir texnologiya və həllərin tətbiqi	Təbii sahələrinin öyrənilməsi	Süni intellekt əsaslı həllərin işlənilib hazırlanması və tətbiq edilməsi
<b>8.1.2. Informasiya təvəüzünə və həqiqətlərin təhrif edilməsinə, milli dəyərlərin pozulmasına aid təhdidlərin (bu bənd üzrə bundan sonra – müvafiq sahələrə aid təhdidlər) qarşısını ala bilən müasir texnologiyaların (o cümlədən süni intellektə əsaslanan texnologiyaların) hazırlanması ilə bağlı fəaliyyətin gücləndirilməsi</b>						
8.1.2.1. Müvafiq sahələrə aid təhdidlərdə istifadəsi ehtimal olunan, belə təhdidlərin qarşısını ala bilən müasir texnologiyaların (xüsusən süni intellekt, qeyri-salis məntiqə və s.) hazırlanmasını, tətbiq və tədris olunmasını, təlimlərin keçirilməsini təşkil etmək	XRİTDX	RİNN, DTX, DİN, MİN	mütləmadi	Müvafiq sahə üzrə müasir texnologiya və həllərin tətbiqi	Təbii sahələrinin öyrənilməsi	Müasir texnologiyaların vasitəsilə təhlükəsizliyin tədris olunması, təlimlərin keçirilməsi
8.1.2.2. Kiberməkanda informasiya-psixoloji ekspansiyaların, radikal dini təşkilatların fərdi və ictimai təfəkkürə destruktiv informasiya təsirlərinin qarşısının alınması və qabaqlayıcı tədbirlər üzrə hüquqi, təşkilati və texnoloji mexanizmlərin müasir texnologiyalar vasitəsilə təkmilləşdirilməsi üçün təkliflər vermək və tətbiqini təşkil etmək	DTX	DİN, RİNN	mütləmadi	Müvafiq sahə üzrə müasir texnologiya və həllərin tətbiqi	Praktik adaptasiya imkanlarının araşdırılması	Müasir texnologiyalar vasitəsilə təkmilləşdirilmiş mexanizmlərin tətbiqi ilə bağlı tədbirlər görülməsi
<b>8.2. Prioritet 2. Informasiya təhlükəsizliyi hadisələrinin aşkarlanması tədbirlərinin və mühafizə texnologiyalarının gücləndirilməsi</b>						
<b>8.2.1. Informasiya təhlükəsizliyi hadisələrinin monitorinqinin, insidentləri və kritik halları aşkarlama meyarlarının müəyyən edilməsi və tətbiqinin təmin olunması</b>						
8.2.1.1. Informasiya təhlükəsizliyi hadisələrinin monitorinqi üçün insidentləri və kritik halları aşkarlama, ölçmə meyarlarını və indikatorlarını müəyyən etmək	RİNN	DTX, XRİTDX, DİN, MN, ETN, VXSİDA	2023 – 2024	Səhə üzrə beynəlxalq təcrübənin öyrənilməsi	Yerli ekosistmə uyğun təcrübənin tətbiqi imkanlarının araşdırılması	Aşkarlama, ölçmə meyarları və indikatorların müəyyən edilməsi
8.2.1.2. Kritik informasiya infrastrukturlarında informasiya təhlükəsizliyi üzrə əməliyyat mərkəzləri üçün fəaliyyətin təşkili üzrə metodiki sənədləri hazırlamaq, informasiya təhlükəsizliyi hadisələrinin monitorinqinə dair xidmətlərin tətbiqinə, informasiya təhlükəsizliyi üzrə əməliyyat mərkəzinin (informasiya təhlükəsizliyi struktur vahidinin) formalaşdırılmasına təşkilati dəstək vermək	DTX	XRİTDX	mütləmadi	Aşkar edilən insidentlərin kateqoriyalar üzrə analiz edilməsi	Fəaliyyətin təşkili üzrə metodiki sənədlərə dair meyarların müəyyənəndirilməsi	Fəaliyyətin təşkili üzrə metodiki sənədlərin hazırlanması və informasiya təhlükəsizliyi hadisələrinin monitorinqinə dair xidmətlərin tətbiqinə və müvafiq informasiya təhlükəsizliyi struktur vahidinin formalaşdırılmasına təşkilati dəstək verilməsi
8.2.1.3. Milli CERT-in potensialının gücləndirilməsi üçün tədbirlər görmək, bunlarla əlaqədar təhlükəsizlik üzrə əməliyyat mərkəzinin yaradılmasını təmin etmək	RİNN	XRİTDX, DTX, DİN, MN	2023 – 2025	Milli CERT-in fəaliyyət istiqamətlərinə uyğun təhlükəsizlik üzrə əməliyyat mərkəzi üçün texniki imkanların və tələblərin müəyyənəndirilməsi	Təhlükəsizlik üzrə əməliyyat mərkəzinin fəaliyyəti üçün təşkilati tədbirlər görülməsi	Təhlükəsizlik üzrə əməliyyat mərkəzinin yaradılması və fəaliyyətə başlaması
8.2.1.4. Milli CERT və digər CERT-lər arasında vahid məlumatlandırma mexanizmlərini müəyyən etmək və tətbiqinə dəstək vermək	RİNN	XRİTDX, DTX	2023 – 2024	Qabaqçıl təcrübənin öyrənilməsi	Vahid məlumatlandırma mexanizminin müəyyənəndirilməsi	Vahid məlumatlandırma mexanizminin tətbiqi
<b>8.2.2. Informasiya mühafizəsinin texniki, kriptografik, proqram və digər vasitələri üzrə təminatın təkmilləşdirilməsi və bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi</b>						
8.2.2.1. Informasiya mühafizəsi təminatının təkmilləşdirilməsi və bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi məqsədilə informasiya mühafizəsi vasitələrinin təchizatı və istehsalı ilə bağlı prioritet fəaliyyət sahələrini müəyyən etmək	İN	XRİTDX, RİNN, DTX	mütləmadi	Ehtiyac meyarlarının müəyyənəndirilməsi	Prioritet sahələrin müəyyənəndirilməsi	İnformasiya mühafizəsi təminatının təkmilləşdirilməsi və bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi
8.2.2.2. Informasiya mühafizəsi vasitələrinin yerli istehsalçıların stimullaşdırılması məqsədilə təkliflər hazırlamaq	NK	İN, XRİTDX, RİNN, DTX	mütləmadi	Ehtiyac sahələrinin müəyyənəndirilməsi	Prioritet sahələrin seçilməsi	Seçilmiş prioritet sahələr üzrə layihələrin həyata keçirilməsi ilə bağlı təkliflər hazırlanması
8.2.2.3. Informasiya mühafizəsi vasitələri istehsalının, milli rəqəmsal iqtisadiyyatın, xüsusilə proqram mühafizəsinin inkişafına təşkilati və elmi dəstək vermək	DTX	ETN, XRİTDX, RİNN, ASK	mütləmadi	Ehtiyac sahələrinin müəyyənəndirilməsi	Prioritet sahələrin seçilməsi	Layihələrin həyata keçirilməsinə təşkilati və elmi dəstək verilməsi
8.2.2.4. Informasiya mühafizəsi sahəsində yerli istehsalın inkişafı məqsədilə kriptografik mühafizə sahəsində milli resursların hazırlanması üçün tədbirlər görmək	DTX	XRİTDX, AMEA	2023 – 2024	Ehtiyac sahələrinin müəyyənəndirilməsi	Səhə üzrə qabaqçıl təcrübələrin öyrənilməsi	Müvafiq sahədə milli resursların hazırlanması
<b>8.2.3. Informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində startapların fəaliyyətinin genişləndirilməsi</b>						
8.2.3.1. Informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində innovativ həllərin tətbiqinin və startapların fəaliyyətinin təşviqi, yeni məhsulların və xidmətlərin yaradılmasına, işlənilməsinə və bazara çıxarılmasına dəstək vermək	RİNN	İN, ETN, XKX, DTX, VXSİDA	mütləmadi	Startapların fəaliyyətinin təşviqi üçün təkliflər hazırlanması, dəstək imkanları və vasitələrinin müəyyən olunması	Akselərasiya proqramlarının işlənilməsi, dəstək imkanları və vasitələrinin açıqlanması	Təklif və proqramların həyata keçirilməsi, seçilmiş həll və startap fəaliyyətinin dəstəklənməsi

8.2.3.2. Informasiya təhlükəsizliyi üzrə texnologiyaların hazırlanması, həmçinin istehsalı üçün vergi və digər icbari ödənişlərə dair güzəştlərin müəyyən edilməsi ilə bağlı təkliflər vermək	NK	İN, RİNN, DGK, ƏƏSMN, ƏN	2024	Beynəlxalq təcrübənin öyrənilməsi	Müvafiq fəaliyyət üzrə vergi və digər icbari ödənişlərə əlaqədar güzəştlərin müəyyən edilməsi ilə bağlı təkliflərin hazırlanması	Müvafiq fəaliyyət üzrə vergi və digər icbari ödənişlərə əlaqədar güzəştlərin müəyyən edilməsi ilə bağlı təkliflərin təqdim olunması
<b>8.3. Prioritet 3. Informasiya məkanının informasiya təhlükəsizliyinin təmin olunması səviyyəsinin yüksəldilməsi</b>						
<b>8.3.1. İKT xidmət subyektlərində fəaliyyətin təkmilləşdirilməsi</b>						
8.3.1.1. Informasiya xidməti, elektron xidmət və texniki xidmət subyektlərində və onların fəaliyyəti üzrə müvafiq obyektlərdə informasiya təhlükəsizliyinin təmin edilməsi fəaliyyətinin standartlara və qabaqçıl təcrübəyə uyğun formalaşdırılmasını təşvil etmək	RİNN	XRİTDX, İN, ASİ, VXSİDA	mütləmadi	Müvafiq sahə üzrə standartların və qabaqçıl təcrübənin öyrənilməsi	Müvafiq sahə üzrə standartların və qabaqçıl təcrübənin öyrənilməsi	Təşvilat materiallarının hazırlanması və təşvilat işlərinin həyata keçirilməsi
8.3.1.2. Informasiya məkanının və onun ayrı-ayrı seçmələrinin, xüsusən də fərdi məlumatlar üzrə seçmələrinin informasiya təhlükəsizliyinin təmin olunması səviyyəsinin ölçülməsinə, qiymətləndirilməsinə və təhlilənin aid mexanizmlərin hazırlanması və tətbiq edilməsi	RİNN	XRİTDX, VXSİDA, DTX	mütləmadi	Müvafiq sahədə informasiya təhlükəsizliyinin təmin olunması səviyyəsinin mövcud vəziyyətinin öyrənilməsi	Müvafiq sahədə informasiya təhlükəsizliyinin təmin olunması səviyyəsinin mövcud vəziyyətinin öyrənilməsi	İnformasiya təhlükəsizliyinin ölçülməsinə, qiymətləndirilməsinə və təhlilənin aid mexanizmlərin hazırlanması
8.3.2. "Ağıllı" sistemlərin təhlükəsizliyinin təkmilləşdirilməsi	RİNN	XRİTDX, DTX, ETN	2023 – 2025	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Məsələ ilə əlaqədar təkliflərin hazırlanması	Təhlükəsizlik tələblərinin müəyyən edilməsi
8.3.2.1. "Ağıllı" sistemlərin (dronlar, pilotsuz aparatlar, humanoidlar, robotlar və s.) yaradılmasına, tətbiqinə və utilziyasına aid təhlükəsizlik tələblərini müəyyən etmək	RİNN	XRİTDX, DTX, ETN	2023 – 2025	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Məsələ ilə əlaqədar təkliflərin hazırlanması	Təhlükəsizlik tələblərinin müəyyən edilməsi
8.3.2.2. "Ağıllı" sistemlərin yaradılmasına, tətbiqinə və utilziyasına aid elmi, texnoloji, hüquqi və s. məsələlərin kompleks həlli üçün təkliflər vermək	RİNN	XRİTDX, DTX, ETN	2024 – 2027	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Müxtəlif həllərin tətbiqi imkanlarının tədqiqi	"Ağıllı" sistemlərin yaradılması, tətbiqi və utilziyasına əlaqədar fəaliyyətin səmərəli təşkilinin təmin edilməsi
<b>8.3.3. Mediada, o cümlədən milli rəqəmsal efir məkanında informasiya təhlükəsizliyi və kibertəhlükəsizliyin davamlı təkmilləşdirilməsi</b>						
8.3.3.1. Milli rəqəmsal efir məkanının (simsiz şəbəkə və yeni nəsil rabitə texnologiyaları və s.) kibertəhlükəsizliyinə təşkilati və texnoloji dəstək vermək	RİNN	AŞ, ETN, DTX, XRİTDX	mütləmadi	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Rəqəmsal efir məkanında təhdidlərin qiymətləndirilməsi	Milli rəqəmsal efir məkanının kibertəhlükəsizliyinin gücləndirilməsi
8.3.3.2. Audiovizual və onlayn media vasitələrinin informasiya təhlükəsizliyinə təşkilati və texnoloji dəstək vermək	RİNN	AŞ, ETN, DTX, XRİTDX	mütləmadi	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Təhdidlərin qiymətləndirilməsi	Audiovizual və onlayn media vasitələrinin informasiya təhlükəsizliyinin gücləndirilməsi
8.3.3.3. Milli rəqəmsal efir məkanı üçün minimal kibertəhlükəsizlik tələblərini müəyyən etmək və onların icrasına nəzarət mexanizmlərini yaratmaq	RİNN	AŞ, ETN, DTX, XRİTDX	2023	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Tələblərin müəyyənəndirilməsi	Tələblərin icrasına nəzarət mexanizminin yaradılması
<b>8.4. Prioritet 4. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi</b>						
8.4.1. Fövqəladə hallarda, müharibə şəraitində kritik informasiya infrastrukturunun təhlükəsizliyini, kritik informasiya infrastrukturunun idarə olunmasını təmin etmək üçün təşkilati əsasların yaradılması, risklərin qiymətləndirilməsi və idarə olunması planının hazırlanması	DTX	XRİTDX	2024 – 2025	Risklərin reyestrində toplanmış məlumatların qiymətləndirilməsi	Qiymətləndirmənin aparılması	Risklərin idarə olunması üzrə planın hazırlanması
8.4.2. Kritik informasiya infrastrukturunun insidentlər zamanı bərpa planlarının hazırlanması	DTX	XRİTDX, İnfrastruktur subyektləri	mütləmadi	Təhdidlər və risklərin qiymətləndirilməsi	Müvafiq bərpa planlarının hazırlanmasının təşkil olunması	Bərpa planlarının hazırlanması və təsdiq edilməsi
<b>8.5. Prioritet 5. Kibercinayətə qarşı mübarizə, o cümlədən kiberkriminalistika sahəsində fəaliyyətin gücləndirilməsi</b>						
8.5.1. "Kibercinayətlər" elektron informasiya sistemini formalaşdırmaq və bu sistmə səlahiyyətli qurumların çıxışının təmin edilməsi ilə bağlı təkliflər hazırlamaq	NK	DİN, DTX, BP (tövsiyə olunur), XRİTDX, RİNN, VXSİDA	2023 – 2024	İnformasiya sisteminin operatoru müəyyən olunması, texniki şərtin hazırlanması	İnformasiya sisteminin texniki şərti və səlahiyyətli qurumlarla razılaşdırılması	Sistem operatoru tərəfindən sistem yaradılması və fəaliyyətinin təşkili
8.5.2. Kibercinayətə qarşı və ona qarşı mübarizə sahəsində müvafiq ölçmə mexanizmlərini formalaşdırmaq və bu sahədə mütləmadi qiymətləndirməni həyata keçirmək	DTX	DİN, XRİTDX, BP (tövsiyə olunur), ƏN	mütləmadi	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Ölçmə mexanizmlərinin formalaşdırılması	Qiymətləndirmənin aparılması
8.5.3. Informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində cinayətlərin aşkarlanması, sübutların toplanması, cinayət işlərinin istintaqının aparılması üçün texniki imkanların genişləndirilməsini təşkil etmək	DTX	DİN, XRİTDX, BP (tövsiyə olunur), ƏN	mütləmadi	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Texniki imkanların tətbiqi və araşdırılması	Texniki imkanların genişləndirilməsi
8.5.4. Hüquq-mühafizə orqanlarının aidiyyəti əməkdaşları, mütəxəssisləri üçün kibercinayətlərin aşkar olunması və istintaqı üzrə təlimlərin keçirilməsini təşkil etmək	DTX	DİN, BP (tövsiyə olunur), ƏN, XRİTDX	mütləmadi	Səhə üzrə qabaqçıl təcrübənin öyrənilməsi	Təlimçilər üçün təlimlərin təşkil edilməsi	Təlimçilər vasitəsilə davamlı təlimlər keçirilməsi
8.5.5. Hüquq-mühafizə orqanları ilə informasiya sistemlərinin operatorları, telekommunikasiya operatorları və provayderlər arasında kibertəhlükəsizlik sahəsində əməkdaşlığı gücləndirmək	RİNN	DİN, DTX, BP (tövsiyə olunur), XRİTDX	mütləmadi	Hüquq-mühafizə orqanları ilə əməkdaşlığa ehtiyacı olan informasiya sistemləri operatorlarının, telekommunikasiya operatorlarının və provayderlərin müəyyənəndirilməsi	Səhə üzrə əlaqədar cavabdeh şəxslərin müəyyənəndirilməsi	Əməkdaşlıq və koordinasiyanın təmin edilməsi

Ardı 13-cü səh.

Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli Sərəncamı ilə təsdiq edilmişdir

## Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası

Əvvəli 12-ci səh.

8.6. Prioritet 6. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialın gücləndirilməsi, institusional bazanın inkişaf etdirilməsi						
<b>8.6.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin aparılmasına təşkilati dəstək verilməsi</b>						
8.6.1.1. İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin edilməsi üçün tələbat olan sahələrdə yeni laboratoriyaların yaradılmasına, mövcud olanların təkmilləşdirilməsinə təşkilati dəstək vermək	XRİTDX	ETN, RİNN, DTX	mütəmadi	Prioritet olan sahələrin müəyyən-ləşdirilməsi	Müvafiq sahələrdə yeni laboratoriyaların yaradılması, mövcud olanların təkmilləşdirilməsi üzrə ehtiyacların qiymətləndirilməsi	Yeni laboratoriyaların yaradılması və mövcud olanların təkmilləşdirilməsi
8.6.1.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi-tədqiqat və layihə-təcrübə işlərinin prioritet mövzuların təbiiqi üçün seçilməsini təşkil etmək	ETN	RİNN, XRİTDX, DTX	mütəmadi	Prioritet mövzuların müəyyən-ləşdirilməsi	Həmin mövzular üzrə elmi tədqiqat və layihə-təcrübə işlərinin keyfiyyətinin artırılması	İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialın gücləndirilməsi
8.6.1.3. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində xarici ölkələrin elmi mərkəzləri ilə əməkdaşlığın genişləndirilməsinə, birgə elmi-tədqiqat layihələrinin həyata keçirilməsinə, beynəlxalq seminar və konfranslarda iştirakın təmin edilməsinə təşkilati dəstək vermək	ETN	DTX, XİN, XRİTDX, RİNN	mütəmadi	İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində xarici ölkələrin qabaqcıl elmi mərkəzlərinin müəyyən-ləşdirilməsi	Birgə elmi tədqiqat layihələrinin başlanılması	Müvafiq sahədə xarici ölkələrin elmi mərkəzləri ilə əməkdaşlığın genişləndirilməsi
8.6.1.4. Kriptografiyanın əsaslarının dərinləşdirilməsini, bu sahədə elmi tədqiqatların aparılmasını, milli kriptografik alqoritmin təbiiqi oluğunu informasiyanın kriptografik mühafizə vasitələrinin layihələndirilməsini və təkmilləşdirilməsini təmin edəcək yüksəkixtisaslı kadrların və sənədlərin müəyyən-ləşdirilməsini təşkil etmək	DTX	XRİTDX, ETN	2023 – 2024	Sahə üzrə siyasət və prioritetlərin müəyyən-ləşdirilməsi	Faaliyyət planının hazırlanması	Yüksəkixtisaslı və sənədlərin hazırlanması
<b>8.6.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət üçün kompetensiyaya (bilik, bacarıq və sənədlər) tələbatları, tədris və təlim proqramları, maarifləndirmə materialları bazasının formalaşdırılması və aktuallığının davamlı təmin olunması</b>						
8.6.2.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət üçün zəruri olan kompetensiyalara (bilik, bacarıq və sənədlər) tələbatların mütəmadi öyrənilməsinə, adekvat perspektivli ixtisasların müəyyən olunmasını təşkil etmək	ETN	RİNN, XRİTDX, DTX, ƏƏSMN	mütəmadi	Sahə üzrə daim artan tələbatların müəyyən-ləşdirilməsi	Yeni kompetensiyaların (bilik, bacarıq və sənədlər) sənədlərinin və mövcud çatışmazlıqlar üzrə prioritetlərin müəyyən-ləşdirilməsi	Yeni kompetensiyalara (bilik, bacarıq və sənədlər) uyğun ixtisasların müəyyən edilməsi və təkliflərin verilməsi
8.6.2.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə kompetensiyalar (bilik, bacarıq və sənədlər) və ixtisaslar üçün zəruri olan kvalifikasiyaya aid tələbatların, ixtisas növləri, təhsil pillələri üzrə müvafiq tədris və təlim, habelə ixtisasartırma proqramlarının müəyyən edilməsi, bu proqramların texnologiyaların inkişaf istiqamətlərinə uyğun perspektivli olması və sənədlərinin davamlı yüksəldilməsi üçün tövsiyə, təklif və təşkilati dəstək vermək	NK	ETN, RİNN, XRİTDX, DTX, ƏƏSMN	mütəmadi	Sahə üzrə tədris texnologiyaların yeniliklərə və tələblərə uyğunluğunun ölçülməsi	Ölçü nəticəsində müəyyən edilən çatışmazlıqlar üzrə prioritetlərin müəyyən-ləşdirilməsi	Tədris texnologiyaların yeniliklərə və tələblərə uyğunluğunun davamlı təmin edilməsi üçün təkliflərin hazırlanması
<b>8.6.3. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə kadr hazırlığının və ixtisaslaşmış struktur bölmələrin müvafiq kadrlarla təminatının gücləndirilməsi</b>						
8.6.3.1. Dövlət orqanlarında (qurumlarında) informasiya təhlükəsizliyi üzrə ixtisaslaşmış struktur bölmələrin yaradılması və onların müvafiq kadrlarla təminatının planlaşdırılması ilə bağlı təkliflərin hazırlanması	DTX	XRİTDX, ƏƏSMN, DİM, RİNN, ETN, MN	2024	Qurumlar-dan sahə üzrə kadr ehtiyacları haqqında məlumatların toplanması	Kadr təminatı üçün planlı yanaşmanın tətbiqinin araşdırılması	İxtisaslaşmış struktur bölmələrin yaradılması və onların müvafiq kadrlarla təminatı ilə bağlı təkliflərin hazırlanması
8.6.3.2. İnformasiya təhlükəsizliyi üzrə mütəxəssislərin əməyinin stimullaşdırılması üçün təkliflər vermək	XRİTDX	RİNN, MN, ƏƏSMN, DTX, ETN	2023 – 2024	Sahə üzrə əməyin qiymətləndirilməsinin ödənilməsi və dövlət qurumlarında müqayisəli təhlilinin aparılması	Qurumlarda sahə üzrə əməyin stimullaşdırılması üçün müvafiq mexanizmlərin hazırlanması	İxtisaslı kadrların əməyinin stimullaşdırılması
<b>8.6.4. İnformasiya təhlükəsizliyi üzrə kadr hazırlığında təhsil müəssisələri ilə dövlət və özəl sektor arasında əməkdaşlığın genişləndirilməsi</b>						
8.6.4.1. İnformasiya təhlükəsizliyi üzrə mütəxəssislərin tədris prosesinə cəlb olunması və tələblərin təcrübə keçmələrinə şərait yaradılmasını təmin etmək	ETN	RİNN, DTX, XRİTDX, MN	mütəmadi	Sahə üzrə təcrübə imkanlarının araşdırılması	Təcrübə proqramları üçün əməkdaşlığın qurulması	Mütəxəssislərin tədris prosesinə cəlb və təcrübə imkanlarının genişləndirilməsi
8.6.4.2. Xarici ölkələrin qabaqcıl universitetlərində, elmi mərkəzlərində informasiya texnologiyaları və informasiya təhlükəsizliyi üzrə ölkə üçün mütəxəssis hazırlığına dəstək vermək	ETN	RİNN, DTX	mütəmadi	Xaricdə təhsil müvafiq sahələrinin araşdırılması	Mütəxəssis hazırlığı ilə bağlı müvafiq proqramların seçilərək təşviq edilməsi	Xaricdə sahə üzrə mütəxəssis hazırlığına dəstək verilməsi
8.6.4.3. İnformasiya təhlükəsizliyi sahəsində kadr hazırlığını təmin edən təhsil müəssisələri ilə, eləcə də informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə beynəlxalq və yerli şirkətlərlə birgə laboratoriyalar formalaşdırmaq	İN	DTX, ETN, RİNN, XRİTDX, XİN	2023 – 2027	Sahə üzrə tələblər nəzərə alınaraq təkliflərin hazırlanması	Beynəlxalq və yerli şirkətlərin təkliflərinin uyğun laboratoriyaların formalaşdırılmasına cəlb edilməsi	Müvafiq laboratoriyaların formalaşdırılması
8.6.4.4. İnformasiya təhlükəsizliyi üzrə ixtisaslaşan yeniyetmə və gənclərə hüquqi və texniki yardım göstərilməsi, istedadlı şəxslərə dəstək verilməsi ilə bağlı tədbirlər görmək	RİNN	DTX, ETN, XRİTDX	mütəmadi	Sahə üzrə biliklərin bazasının toplanması	Prioritetlərin seçilməsi	Müvafiq onlayn maarifləndirmə, məsləhət xidmətlərinin formalaşdırılması, dəstək verilməsi işlərinin həyata keçirilməsi
<b>8.7. Prioritet 7. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində normativ bazanın təkmilləşdirilməsi</b>						
8.7.1. Fərdi məlumatların işlənməsi və mühafizəsi sahəsində normativ hüquqi bazanın beynəlxalq təcrübə əsas götürülməklə təkmilləşdirilməsi	NK	RİNN, DTX, XRİTDX, DİN, ƏN	mütəmadi	Sahə üzrə beynəlxalq təcrübənin öyrənilməsi	Müvafiq təkliflərin təqdim olunması	Müvafiq sahədə normativ hüquqi bazanın təkmilləşdirilməsi

8.7.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində qabaqcıl beynəlxalq hüquqi və texniki normativ aktları, praktik tövsiyələri təşviq etmək, milli standartların davamlı təkmilləşdirilməsinə dəstək vermək	RİNN	DTX, XRİTDX, ETN, İN	mütəmadi	Ölkədə beynəlxalq standartların tətbiqi olumması, milli standartların aktuallığı vəziyyətlərinin, problemlərin və tələbatların mütəmadi araşdırılması	Ölkədə beynəlxalq standartların tətbiqinə, milli standartların genişləndirilməsinə aid təkliflərin verilməsi	Təşkilati və metodiki tövsiyələrin verilməsi, icmalın dərc olunması
<b>8.8. Prioritet 8. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin yüksəldilməsi</b>						
<b>8.8.1. Cəmiyyətdə informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyəti üzrə zəruri biliklərin, bacarıqların artırılmasına və təbliğinə dəstək verilməsi</b>						
8.8.1.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə maarifləndirmə tədbirlərinin keçirilməsini təşkil etmək, o cümlədən bu barədə televiziya proqramları, videoçarxlar hazırlamaq və nümayiş etdirmək, informasiya təhlükəsizliyi və kibertəhlükəsizlikə qarşı ictimai mübarizə üsulları və bu üsullarda istifadə barədə cəmiyyətin, fərdlərin bilik səviyyəsini yüksəltmək	RİNN	ETN, DTX, XRİTDX	mütəmadi	Maarifləndirmə tədbirlərinin qiymətləndirilməsi	Maarifləndirmə tədbirlərinin intensivləşdirilməsi	Müvafiq sahədə zəruri bilik və bacarıqların səviyyəsinin yüksəldilməsi
8.8.1.2. Dövlət orqanlarında (qurumlarında) əzəl təşkilatlarda informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətini formalaşdırmaq – kibergigiyəni təmin etmək məqsədilə tədbirlər görmək	XRİTDX	RİNN, DİM, VXSİDA	2023 – 2027	Nümunəvi kibergigiyə pilot layihəsinin həyata keçirilməsi	Kibergigiyənin pilot layihəsinin təşviq olunması	Dövlət orqanlarında (qurumlarında) əzəl sektorda informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması və kibergigiyənin təmin edilməsi
<b>8.8.2. Uşaqların internetdən təhlükəsiz istifadə imkanlarının möhkəmləndirilməsinə təşkilati dəstək verilməsi</b>						
8.8.2.1. Ailələrin, valideynlərin və uşaqların internetdəki təhlükələr barədə məlumatlandırılması üçün tədbirlər təşkil etmək	AQUPDK	RİNN, ETN, DİN, DTX	mütəmadi	Maarifləndirmə tədbirlərinin hazırlanması	Maarifləndirmə tədbirlərinin həyata keçirilməsi	Maarifləndirmə tədbirlərinin intensivləşdirilməsi
8.8.2.2. "Uşaqların zərərli informasiyadan qorunması haqqında" Azərbaycan Respublikası Qanununun tələblərindən irəli gələn vəzifələrin həyata keçirilməsi məqsədilə milli onlayn məlumatlandırma mərkəzinin yaradılması, həmin mərkəzin beynəlxalq şəbəkələrə inteqrasiyasını təmin etmək	AQUPDK	RİNN, ETN	mütəmadi	Milli onlayn məlumatlandırma mərkəzinin yaradılması	Milli onlayn məlumatlandırma mərkəzinin təşviq olunması, beynəlxalq şəbəkələrə inteqrasiyasının təmin edilməsi	Uşaqların zərərli informasiyadan qorunmasını təmin edilməsi
8.8.2.3. Təhsilin bütün səviyyələrində kibertəhlükəsizlik üzrə təhsil modulunu hazırlamaq, eləcə də internetdə təhlükələr barədə materialları tədris resurslarına daxil etmək	ETN	RİNN, DTX	mütəmadi	Təhsilin bütün səviyyələrində uyğun sahə üzrə materialların yaradılması	Yaradılmış materialların tədris resurslarına daxil edilməsi	Bu materialların mütəmadi yenilənməsini həyata keçirməsi
<b>8.9. Prioritet 9. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə ölkədaxili və beynəlxalq əməkdaşlığın inkişaf etdirilməsi</b>						
<b>8.9.1. Dövlət orqanları (qurumları), özəl sektor və vətəndaş cəmiyyəti institutları arasında əməkdaşlığın inkişaf etdirilməsi</b>						
8.9.1.1. İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyinin təmin olunması, o cümlədən insidentlərə qarşı tədbirlər görülməsi üçün dövlət orqanları (qurumları), özəl sektor və vətəndaş cəmiyyəti institutları arasında əməkdaşlıq formalarının müəyyən etmək və onların hüquqi əsasını yaratmaq	XRİTDX	RİNN, DTX, DİN	2023 – 2024	Əməkdaşlıq müxtəlif formalarının effektivliyinin araşdırılması	Uyğun əməkdaşlıq formalarının seçilməsi	Əməkdaşlıq hüquqi əsasının yaradılması
8.9.1.2. Təhdidləri qiymətləndirmə və həlli yollarını müəyyən etmə sahəsində dövlət koordinasiya və məsləhətləşmə platformalarını yaratmaq və onların inkişafına dəstək vermək	RİNN	DTX, DİN	2023 – 2024	Sahə üzrə müxtəlif koordinasiya və məsləhətləşmə platformalarının yaradılması	Müxtəlif mövzuların bu platformalarda müzakirələrə çıxarılması	Platformaların effektivliyinin ölçülməsi, inkişafına dəstək verilməsi
8.9.1.3. Ölkə səviyyəsində kibertəhlükəsizliklə bağlı (təhdidlər, boşluqlar, risklər və s. barədə) informasiya mübadiləsi və qarşılıqlı əməkdaşlıq sahəsində əlaqələndirməni həyata keçirmək, təhdidlərə və hücumlara qarşı erkən xəbərdarlıq, cavabvermə imkanlarını formalaşdırmaq	RİNN	DTX, DİN, XRİTDX	mütəmadi	Təhdidlər, boşluqlar, risklər və s. məlumatların əldə edilməsi və toplanmasının təşkil	Əldə edilən məlumatların bölüşdürülməsi və erkən xəbərdarlıq mexanizmlərinin yaradılması	Mexanizmlərin avtomatlaşdırılması imkanlarının genişləndirilməsi
8.9.1.4. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində fəaliyyət göstərən qabaqcıl onlayn təlim-tədris platformaları ilə əməkdaşlıq əlaqələri qurmaq	RİNN	XRİTDX, ETN, DİM	mütəmadi	Əməkdaşlıq müxtəlif formalarının effektivliyinin araşdırılması	Pilot layihələrin həyata keçirilməsi	Uğurlu layihələr üzrə əməkdaşlığın davam etdirilməsi
<b>8.9.2. İnformasiya təhlükəsizliyini idarəetmə sahəsində beynəlxalq təşkilatlarla əməkdaşlığın inkişaf etdirilməsi</b>						
8.9.2.1. Kibercinayətkarlığa qarşı mübarizə üzrə beynəlxalq əməkdaşlığı genişləndirmək, qabaqcıl təcrübənin mənimsənilməsinə və bölüşdürülməsinə təmin etmək	DTX	DİN, ƏN, RİNN, XRİTDX	mütəmadi	Qabaqcıl təcrübənin və yeniliklərin mənimsənilməsi	Kibercinayətkarlığa qarşı mübarizə təcrübəsinin bölüşdürülməsi	Beynəlxalq əməkdaşlığın genişləndirilməsi
8.9.2.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə beynəlxalq təlimlərdə, ekspert görüşlərində və müxtəlif tədbirlərdə mütəxəssislərin iştirakına təşkilati dəstək vermək	RİNN	XRİTDX, MN, DTX, ETN, MB, KXX	mütəmadi	İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə mütəxəssislərlə davamlı əlaqə yaradılması	Qabaqcıl təcrübəyə əsaslanan təlimlərin və görüşlərin kataloqunun yaradılması	Sahə üzrə mütəxəssislərin iştirakına təşkilati dəstək verilməsi
8.9.2.3. İnformasiya təhlükəsizliyi subyektləri, o cümlədən Milli CERT və digər CERT-lər səviyyəsində beynəlxalq əməkdaşlığın inkişaf etdirilməsini, kibertəhlükəsizlik sahəsində beynəlxalq təcrübənin öyrənilməsinə təşkilati dəstək vermək	RİNN	XRİTDX, ETN, DTX, MB	mütəmadi	Beynəlxalq CERT mərkəzləri ilə əməkdaşlığın inkişaf etdirilməsi	Beynəlxalq CERT mərkəzlərinə üzvlüyün təmin edilməsi	Beynəlxalq fəaliyyətdə qarşılıqlı fəaliyyət və təcrübə mübadiləsinin gücləndirilməsi
8.9.2.4. Əhəlinin fərdi məlumatlar sahəsində hüquqlarının qorunması üçün beynəlxalq miqyaslı operatorlarla (kontentdaşıyıcılarla) əlaqələr yaratmaq	RİNN	XİN	mütəmadi	Əhəlinin fərdi məlumatlar sahəsində hüquqlarının qorunması üçün cavabdeh operatorların müəyyən-ləşdirilməsi	Bu sistemlər üzrə cavabdeh operatorların müəyyən-ləşdirilməsi	Beynəlxalq miqyaslı operatorlarla əlaqələrin yaradılması

## Akronimlər

AQUPDK - Azərbaycan Respublikasının Ailo, Qadın və Uşaq Problemləri üzrə Dövlət Komitəsi  
 ASİ - Azərbaycan Standartlaşdırma İnstitutu  
 AMEA - Azərbaycan Milli Elmlər Akademiyası  
 AŞ - Azərbaycan Respublikasının Audiovizual Şurası  
 ASK - Azərbaycan Respublikasının Sahibkarlar (İşgötürənlər) Təşkilatları Milli Konfederasiyası  
 BP - Azərbaycan Respublikasının Baş Prokurorluğu  
 DIM - Azərbaycan Respublikasının Dövlət İmtahan Mərkəzi  
 DİN - Azərbaycan Respublikasının Daxili İşlər Nazirliyi  
 DTX - Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti  
 DGK - Azərbaycan Respublikasının Dövlət Gömrük Komitəsi  
 ƏƏSMN - Azərbaycan Respublikasının Əmək və Əhəlinin Sosial Müdafiəsi Nazirliyi

ƏN - Azərbaycan Respublikasının Ədliyyə Nazirliyi  
 XRİTDX - Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti  
 XİN - Azərbaycan Respublikasının Xarici İşlər Nazirliyi  
 KXX - Azərbaycan Respublikasının Xarici Kəşfiyyat Xidməti  
 İN - Azərbaycan Respublikasının İqtisadiyyat Nazirliyi  
 MB - Azərbaycan Respublikasının Mərkəzi Bankı  
 MN - Azərbaycan Respublikasının Müdafiə Nazirliyi  
 MİN - Azərbaycan Respublikasının Mədəniyyət Nazirliyi  
 NK - Azərbaycan Respublikasının Nazirlər Kabineti  
 RİNN - Azərbaycan Respublikasının Rəqəmsal İnkişaf və Noqiyat Nazirliyi  
 ETN - Azərbaycan Respublikasının Elm və Təhsil Nazirliyi  
 VXSİDA - Azərbaycan Respublikasının Prezidenti yanında Vətəndaşlara Xidmət və Sosial İnnovasiyalar üzrə Dövlət Agentliyi