Azərbaycan Respublikası Prezidentinin
2023-cü il 28 avqust tarixli
nömrəli 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 istiqamətlərindəndir. 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 infrastrukturlarının funksional dayanıqlığını, bu infrastrukturlardan istifadə edən subyektlərin hüquq və qanuni maraqlarını, fəaliyyətin davamlılığını təmin etmək üçün qabaqlayıcı və bərpaedici tədbirlərin müəyyənləşdirilmiş 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 infrastrukturlarına, 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 əvvəldən təyin edilmiş hədlərə qədər azaldılması üçün hüquqi, təşkilati, əməliyyat-axtarış, kəşfiyyat və əks-kəşfiyyat, elmi-texniki və təhsil, informasiya-təhlil, kommunikasiya, kadr 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 reytinqlərdə mövqeyinin ciddi şəkildə yaxşılaşdırılması ilə nəticələnmişdir. Azərbaycan Beynəlxalq Telekommunikasiya İttifaqının tərtib etdiyi “Qlobal kibertəhlükəsizlik indeksi 2020” (Global Cybersecurity Index, GCI) reytinqində 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 infrastrukturlarının təhlükəsizliyinin təmin olunmasına aid tədbirlərin müəyyənləşdirilməsinin 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 edilmiş “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 həyati əhəmiyyətli bütün maraqlarının daha yüksək və təkmil səviyyədə qorunması hazırda həm də ölkənin informasiya təhlükəsizliyi və kibertəhlükəsizlik siyasətinin əsas məqsədi kimi müəyyənləşdirilir 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 (“cybercrime 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 zəifliklər, riskləri idarəetmə texnologiyaları;

2.1.8. süni intellekt mühəndisliyi, idarəetmə üzrə qərarvermədə, riskləri, insidentləri müəyyənetmədə, o cümlədən funksionallıqda anomaliyaları və konfiqurasiyada sanksiyasız dəyişiklikləri dərhal aşkaretmədə, qabaqlayıcı (preventiv) və bərpaedici (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 riskyönümlü modelləşdirmə, simulyasiya və kiberpoliqonlar texnologiyaları;

2.1.11. internetdə davranış mədəniyyəti, sosial mühəndislik “hücumları”nın və onlara əks-tədbirlərin daha da “ağıllı” olması, maarifləndirmə işinin genişləndirilməsi;

2.1.12. kiberhücum vektorlarının 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, müəssisə 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 lazımi qaydada aparılmamışdır. Məsafədən iş üçün tətbiq olunmuş proqram təminatının müxtəlifliyini və çoxsaylı istehsalçılara məxsus olduğunu nəzərə alaraq, fərdi məlumatların, kommersiya sirrinin və digər qorunan informasiyanın sızması təhlükəsi ötən illərlə müqayisədə dəfələrlə artmışdır. Bununla bağlı, qorunan informasiyanın mühafizəsi istiqamətində əlavə tədbirlərin həyata keçirilməsi zərurəti yaranmışdır.

Ümumiyyətlə, ölkədə kibercinayətlərlə mübarizə imkanlarının genişləndirilməsi üçün bir sıra mühüm hüquqi və təşkilati tədbirlər görülmüşdür. İnformasiya təhlükəsizliyi, habelə kibertəhlükəsizlik üzrə hüquqi bazanın təkmilləşdirilməsi 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 edilməsi kibercinayətkarlıqla mübarizə sahəsində atılan

mühüm addımlardan biridir. Həmin Konvensiyanın müddəalarından irəli gələrək, Azərbaycan Respublikasının Cinayət Məcəlləsinə 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 nömrəli 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 nömrəli Fərmanında dəyişiklik edilməsi barədə" Azərbaycan Respublikası Prezidentinin 2018-ci il 19 sentyabr tarixli 276 nömrəli 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 nömrəli Fərmanı ilə Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi 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 nömrəli 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 sistemin inkişaf etdirilməsi nəzərdə tutulmuşdur. Bundan irəli gələrək, qlobal 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 kiberhücumlardan qorunması, belə təhdidlərin qabaqlanması, qarşısının alınması və araşdırılması sahəsində fəaliyyət göstərən dövlət qurumlarının işinin əlaqələndirilməsini təmin etmək üçün Azərbaycan Respublikası Prezidentinin 2018-ci il 29 mart tarixli 3851 nömrəli Sərəncamı ilə İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyası yaradılmışdır.

Bundan başqa, Azərbaycanda TIER III səviyyəli, ISO/IEC 20000 və ISO/IEC 27001 standartlarına uyğun Data Mərkəzi yaradılmış və fəaliyyəti təmin edilmiş, "Elektron hökumət"in inkişafı, "Rəqəmsal hökumət"ə keçidin təmin edilməsi, dövlət qurumlarının informasiya texnologiyalarına, elektron xidmətlərin yaradılmasına və göstərilməsinə tələb olunan dövlət xərclərinin optimallaşdırılması, informasiya sistemlərinin fəaliyyətinin daha müasir standartlar əsasında keyfiyyətli, dayanıqlı və təhlükəsiz infrastrukturda təşkilinin 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 nömrəli 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 nömrəli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası"nda öz əksini tapmışdır.

Azərbaycan Respublikasının qanunvericiliyinə əsasən, ölkədə informasiya təhlükəsizliyinin, həmçinin kibertəhlükəsizliyin təmin edilməsi sahəsində səlahiyyət və məsuliyyət bölgüsü müəyyənləşdirilmişdir. Dövlət orqanları səlahiyyətlərinə uyğun olaraq informasiya təhlükəsizliyinin müxtəlif məsələləri ilə məşğuldurlar, informasiya sistemlərinin mülkiyyətçiləri 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 yönəlmiş hərəkətlərin aşkarlanmasını, qarşısının alınması üçün preventiv tədbirlərin həyata keçirilməsini 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 yönəlmiş 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 nəzarətdə 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 qlobal xarakter daşıyır. Buna görə də kibertəhlükəsizliyin təminatının mühüm şərtlərindən biri beynəlxalq əməkdaşlığın mövcudluğudur.

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

Azərbaycan Respublikasının hərtərəfli inkişafı, dövlət idarəçiliyində, iqtisadi və sosial sahələrdə, insanların gündəlik 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 dəqiq, 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 (**G**üclü tərəflər, **Z**əif tərəflər, **İ**mkanlar, **T**əhdidlər) analiz metoduna uyğun olaraq mütəmadi qiymətləndirilir. Bu amillər Strategiyada nəzərə alınmışdır və prioritet istiqamətlər, vəzifələr, müvafiq həll yolları, eləcə də kompleks tədbirlər planı müəyyənləşdirilmişdir.

Strategiyanın hazırlanması zamanı qabaqcıl beynəlxalq təcrübə, region və Avropa dövlətlərinin müvafiq strategiyaları araşdırılmış və ölkəmizdə tətbiqi baxımından təhlil edilmişdir.

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

Beynəlxalq təşkilatların hesabatlarında ölkələrin kibertəhlükəsizlik üzrə reytinqinə 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 reyestrinin formalaşdırılmasının və aparılmasının təşkili;

4.1.2. informasiya təcavüzünə və həqiqətlərin təhrif edilməsinə, milli dəyərlərin pozulmasına aid təhdidlərin qarşısını ala bilən müasir texnologiyaların (o cümlədən süni intellektə əsaslanan texnologiyaların) işlənib hazırlanması 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, kriptoqrafik, proqram və digər vasitələr üzrə təminatının təkmilləşdirilməsi, bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi;

4.1.5. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində startapların fəaliyyətinin genişləndirilməsi;

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 təhlükəsizliyinin və kibertəhlükəsizliyin davamlı təkmilləşdirilməsi;

4.1.11. kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmini;

4.1.12. fövqəladə hallarda, müharibə şəraitində kritik informasiya infrastrukturlarının təhlükəsizliyini və onun idarə edilməsini təmin etmək üçün təşkilati əsasların yaradılması;

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

4.1.14. informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin real tətbiqləri nəticəsində rəqabətədavamlı 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 bölmələrin 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 alətlərin öyrənilməsi, informasiya təhlükəsizliyi və əlaqəli sahələrə aid beynəlxalq mənbələrin praktiki tövsiyələrinin təşviqi;

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

4.1.21. internetdən gələn qlobal 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 reytinqlərdə ölkəmizin mövqeyinin yaxşılaşdırılması;

4.1.25. informasiya təhlükəsizliyi üzrə beynəlxalq standartların ölkədə tətbiqinin genişləndirilməsi, o cümlədən müxtəlif standartlaşdırma təşkilatlarının məhsullarından ölkəmizdə vahid yanaşma ilə uyğunlaşdırılmış 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 edir:

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

5.1.2. informasiya təcavüzünə 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 xaricdən birbaşa asılılığın minimallaşdırılması, nəzarətdə 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 sistemliliyin 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 tsiklinin optimal idarə edilməsinin, izafiliyinin minimallaşdırılmasının və adekvatlığının obyektiv qiymətləndirilməsinin təmin olunması;

5.1.9. “ağıllı” sistemlərin yaradılmasına, tətbiqinə və utilizasiyasına 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 mübarizə səviyyəsinin mütəmadi qiymətləndirilməsinin adekvatlığının təmin edilməsi;

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

5.1.15. informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət sahəsi barədə 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 tükənməzliyi və mühafizəsi, ölkə xaricinə "beyin axını"nın qarşısının alınması;

5.1.19. informasiya təhlükəsizliyinin və kibertəhlükəsizliyin normativ əsasının aktuallığının təmin edilməsi;

5.1.20. İKT-məhsulları və xidmətləri bazarında informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması, həmçinin sifariş, istehsal, 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 imkanlarının möhkəmləndirilməsinə, tövsiyələrin işlənilməsinə təşkilati 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 təşkilati və metodiki dəstək verilməsi, o cümlədən müxtəlif standartlaşdırma təşkilatlarının ölkəmizdə istifadə olunan məhsullarının uyğunluq baxımından vahid yanaşma ilə icmallaşdırılması və İnformasiya Təhlükəsizliyi üzrə Milli Standartların formalaşdırılması;

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

## 6. Prioritet istiqamətlər

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

### 6.1. Təhdidlərin müəyyənləşdirilməsi və risklərin idarə edilməsi

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 yarana bilməsinin 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 səviyyəsini ölçmə 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 yetərli və yararlı olmasının, 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 həyati funksiyalarını təmin etmək üçün böyük rola malik olan, fəaliyyətindəki nasazlıqların və ya sıradan çıxmasının əhalinin sağlamlığına, təhlükəsizliyinə, iqtisadi və sosial rifahına, həmçinin dövlət qurumlarının fəaliyyətinin davamlılığına ciddi təsir göstərən infrastrukturların və ya onların əhəmiyyətli hissələrinin informasiya təhlükəsizliyinin təmin olunması xüsusilə vacibdir. Bununla yanaşı, hər hansı bir sahədə baş vermiş hadisə digər sahələrdə də zəncirvari hadisələrə səbəb ola bilər. Qeyd edilən səbəblərdən kritik informasiya infrastrukturlarının təhlükəsizliyinin təmini mülkiyyət növündən asılı olmayaraq daim diqqət mərkəzində olmalı və bu məqsədlə müvafiq tədbirlər görülməlidir.

Bu baxımdan kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin edilməsi ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində kritik informasiya infrastrukturları obyektlərinin təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət təkmilləşəcək, bu sahədə risklərin qiymətləndirilməsi və idarə olunmasının keyfiyyəti yaxşılaşacaqdır.

### 6.5. Kibercinayətkarlığa qarşı mübarizə, o cümlədən kiberkriminalistika sahəsində fəaliyyətin gücləndirilməsi

Kibercinayətkarlıq bütün dünyada artır və bəzən mütəşəkkil beynəlxalq qruplaşmalar vasitəsilə həyata keçirilərək, inkişaf etmiş İKT infrastrukturuna malik ölkələrin demək olar ki, hamısını əhatə edir. Azərbaycan Respublikasında da müasir texnoloji vasitələrdən istifadənin genişlənməsi kibercinayətlərin başvermə təhdidi ilə müşayiət olunur. Kibercinayətlər böyük həcmli və miqyaslı ola, həmçinin kritik infrastrukturların, informasiya sistemlərinin işinin pozulması, fərdi məlumatların oğurlanması, insanların şəxsi həyatına təhlükə törətməsi və onlara mənəvi zərər vurulması ilə nəticələnə bilir. Kiberməkanın fiziki sərhədlərinin olmaması kibercinayətkarlara beynəlxalq problem olan terror, təxribat, casusluq, transmilli mütəşəkkil cinayətkarlıq kimi təhlükəli fəaliyyətləri bu məkanın imkanlarından istifadə etməklə həyata keçirmək üçün geniş şərait yaradır.

Bu baxımdan kibercinayətkarlığa qarşı mübarizə, o cümlədən kiberkriminalistika üzrə fəaliyyətin gücləndirilməsi ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində cinayətlərin aşkarlanması, sübutların toplanılması, cinayət işlərinin istintaqının aparılmasına dair fəaliyyətin səmərəli təşkili sahəsində imkanlar genişləndiriləcəkdir.

### 6.6. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialın gücləndirilməsi, institusional bazanın inkişaf etdirilməsi

İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunmasının kompleks təşkili və həyata keçirilməsi bu sahədə aparılan elmi tədqiqatlardan və onların nəticələrinin praktikaya tətbiqindən, təhsilin mövcud və perspektiv tələbata uyğun olmasından asılıdır.

Bu baxımdan informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialı gücləndirmə, institusional bazanı inkişaf etdirmə ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində aparılan elmi tədqiqat və layihə-təcrübə işlərinin keyfiyyəti yüksəldiləcək, müvafiq sahələrdə kadr hazırlığı, kadrların təkmilləşdirilməsi və ixtisaslaşmış struktur bölmələrin keyfiyyətli kadrlarla təminatı təmin ediləcəkdir.

### 6.7. İnformasiya təhlükəsizliyi və kibertəhlükəsizliyə dair normativ bazanın təkmilləşdirilməsi

İnformasiya təhlükəsizliyi və kibertəhlükəsizliyə dair normativ hüquqi bazanın müasir çağırışlara uyğun olaraq təkmilləşdirilməsi davamlı təmin edilməlidir.

Bu baxımdan informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair normativ bazanın təkmilləşdirilməsi ilə bağlı bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində qabaqcıl beynəlxalq təcrübəyə uyğun olan və müvafiq sahənin bu Strategiya ilə müəyyən edilən məqsədlərə, prioritet istiqamətlərə uyğun tənzimlənməsinə imkan verən hüquqi baza formalaşacaqdır.

### 6.8. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin yüksəldilməsi

İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması təşkilati məsələlərin həlli, insidentlərin qarşısının alınması və onlar baş verdiyi halda müvafiq fəaliyyətin həyata keçirilməsi, həmçinin fərdi təhlükəsizliyin təmin olunması üçün lazımi bilik və bacarıqların aşılanması ilə bağlı kompleks fəaliyyətdir. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşmasında maarifləndirmə mühüm rol oynayır.

İnformasiya texnologiyalarının yüksək sürətlə inkişafı və dəyişməsi ona bağlı informasiya təhlükəsizliyi tələblərinin daim təkmilləşdirilməsinə ehtiyac yaradır. Qeyd edilən səbəblərdən də intensiv inkişaf və yeniliklər nəzərə alınmaqla, maarifləndirmə tədbirləri mütəmadi olaraq, günün tələblərinə uyğun aparılmalıdır.

Bu baxımdan informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin yüksəldilməsinə dair bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində cəmiyyətdə informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyəti üzrə zəruri biliklər, bacarıqlar artırılacaq, informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyəti təmin ediləcəkdir.

### 6.9. İnformasiya təhlükəsizliyi və kibertəhlükəsizliklə bağlı ölkədaxili və beynəlxalq əməkdaşlığın inkişaf etdirilməsi

İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması üçün milli və beynəlxalq səviyyədə əməkdaşlıq mühüm rol oynayır. Ölkədə informasiya təhlükəsizliyinə və kibertəhlükəsizliyə məsul olan dövlət orqanlarının (qurumların) və maraqlı tərəflərin bütün məsələlər, o cümlədən hüquqi-təşkilati, texniki-texnoloji, maarifləndirmə və məlumatlandırılma, baş verən hadisələrə qarşı əlaqəli fəaliyyət kimi məsələlər üzrə əməkdaşlığının təşkili informasiya təhlükəsizliyinin təmin edilməsində vacib amillərdəndir. Həmçinin, kibertəhlükəsizlik məsələlərinin qlobal xarakterini nəzərə alaraq, bu məsələlər üzrə beynəlxalq səviyyədə də əməkdaşlıq günün tələbidir. Ölkədaxili və beynəlxalq əməkdaşlıq informasiya təhlükəsizliyinin, həmçinin kibertəhlükəsizliyin təmin edilməsinə ciddi zəmin yaradır.

İnformasiya təhlükəsizliyi üzrə əməkdaşlıq informasiya təhlükəsizliyinin subyektləri olan səlahiyyətli orqanlar (qurumlar), CERT-lər, özəl sektor və digər maraqlı tərəflər, o cümlədən fərdi istifadəçilər arasında təşkil edilir. Özəl sektor bir sıra kritik infrastrukturun sahibləri olmaqla yanaşı, həm milli informasiya təhlükəsizliyinin təmin olunmasına məsuliyyət daşıyır, həm də bu sahədə mühüm hüquq və vəzifələrə malikdir. Qeyd edilən səbəblərdən özəl sektor öz fəaliyyətinin təşkilində, dövlət qurumlarına və insanlara müxtəlif İKT xidmətlərinin göstərilməsində, İKT məhsulların təchizatında, İKT ilə əlaqəli digər işlərin görülməsində informasiya təhlükəsizliyi tələblərinə riayət etməlidir.

Bu baxımdan informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə ölkədaxili və beynəlxalq əməkdaşlığın inkişaf etdirilməsinə dair bu Strategiyada nəzərdə tutulan tədbirlərin həyata keçirilməsi nəticəsində dövlət orqanları (qurumları), özəl sektor və vətəndaş cəmiyyəti institutları arasında, habelə informasiya təhlükəsizliyini idarəetmə sahəsində beynəlxalq təşkilatlarla əməkdaşlıq inkişaf edəcəkdir.

## 7. Maliyyələşdirmə mexanizmləri

Strategiyada nəzərdə tutulan tədbirlərin maliyyələşdirilməsi büdcə təşkilatları üçün onların saxlanılması məqsədilə Azərbaycan Respublikasının dövlət büdcəsində nəzərdə tutulan vəsaitdən və qanunla qadağan edilməyən digər mənbələrdən həyata keçirilir.

Təsərrüfathesablı qurumların, özəl qurumların Strategiyada nəzərdə tutulan tədbirlərdə iştirakı həmin qurumların vəsaiti hesabına və qanunla qadağan edilməyən digər mənbələrdən maliyyələşir.

## 8. “AZƏRBAYCAN RESPUBLİKASININ İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ KİBERTƏHLÜKƏSİZLİYƏ DAİR 2023 – 2027-Cİ İLLƏR ÜÇÜN STRATEGİYASI”NIN HƏYATA KEÇİRİLMƏSİ İLƏ BAĞLI TƏDBİRLƏR PLANI

| Tədbirlər | Əsas icraçı orqan (qurum) | Digər icraçılar | İcra müd-dəti | Nəticə indikatorları | | |
|---|---|---|---|---|---|---|
| | | | | ilkin nəticələr | aralıq nəticələr | yekun nəticələr |
| **8.1. Prioritet 1. Təhdidlərin müəyyənləşdirilməsi və risklərin idarə edilməsi** | | | | | | |
| **8.1.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik riskləri reyestrinin formalaşdırılmasının və aparılmasının təşkili** | | | | | | |
| 8.1.1.1. İnformasiya 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 təsnifatlaşdırıl-ması |
| 8.1.1.2. İnformasiya 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. İnformasiya təhlükəsizliyi üzrə yarana biləcək təhdidlərin və risklərin əvvəlcədən müəyyən edilməsi və görülməli tədbirləri proqnozlaşdırmaq məqsədilə süni intellekt əsaslı həllərin işlənib hazırlanmasını və tətbiqini təşkil etmək | XRİTDX | DTX, RİNN, ETN | 2023 – 2027 | Sahə üzrə müasir texnologiya və həllərin tədqiq edilməsi | Tətbiq sahələrinin öyrənilməsi | Süni intellekt əsaslı həllərin işlənib hazırlanması və tətbiq edilməsi |
| **8.1.2. İnformasiya təcavüzünə 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** | | | | | | |
| 8.1.2.1. Müvafiq sahələrə aid təhdidlərdə istifadəsi ehtimal olunan, belə təhdidlərin qarşısını ala bilən müasir texnologiyaların (xüsusən süni intellekt, qeyri-səlis məntiq və s.) hazırlanmasını, tədqiq və tədris olunmasını, təlimlərin keçirilməsini təşkil etmək | XRİTDX | RİNN, DTX, DİN, MdN | müntəzəm | Müvafiq sahə üzrə müasir texnologiya və həllərin tədqiqi | Tətbiq sahələrinin öyrənilməsi | Müasir texnologiyaların hazırlanması, tədqiq və 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 təklifər vermək və tətbiqini təşkil etmək | DTX | DİN, RİNN | mütəmadi | Müvafiq sahə üzrə müasir texnologiya və həllərin tədqiqi | Praktik adaptasiya imkanları-nın araşdırıl-ması | Müasir texnologiyalar vasitəsilə təkmilləşdirilmiş mexanizmlərin tətbiqi ilə bağlı tədbirlər görülməsi |
| **8.2. Prioritet 2. İnformasiya təhlükəsizliyi hadisələrinin aşkarlanması tədbirlərinin və mühafizə texnologiyalarının gücləndirilməsi** | | | | | | |
| **8.2.1. İnformasiya təhlükəsizliyi hadisələrinin monitorinqinin, insidentləri və kritik halları aşkarlama meyarlarının müəyyən edilməsi və tətbiqinin təmin olunması** | | | | | | |
| 8.2.1.1. İnformasiya təhlükəsizliyi hadisələrinin monitorinqi üçün insidentləri və kritik halları aşkarlama, ölçmə meyarlarını və indikatorlarını müəyyən etmək | RİNN | DTX, XRİTDX, DİN, MN, ETN, VXSİDA | 2023 – 2024 | Sahə üzrə beynəlxalq təcrübənin öyrənilməsi | Yerli ekosistemə uyğun təcrübənin tətbiqi imkanları-nın araşdırıl-ması | Aşkarlama, ölçmə meyarları və indikatorlarının 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 | müntəzəm | Aşkar edilən insidentlə-rin kateqoriya-lar üzrə analiz edilməsi | Fəaliyyətin təşkili üzrə metodiki sənədlərə dair meyarların müəyyən-ləşdirilməsi | 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, bununla əlaqədar təhlükəsizlik üzrə əməliyyat mərkəzinin yaradılmasını təmin etmək | RİNN | XRİTDX, DTX, DİN, MN | 2023 – 2025 | Milli CERT-in fəaliyyət istiqamətlə-rinə uyğun təhlükəsiz-lik üzrə əməliyyat mərkəzi üçün texniki imkanların və tələblərin müəyyən-ləşdirilməsi | Təhlükəsiz-lik 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 | Qabaqcıl təcrübənin öyrənilməsi | Vahid məlumat-landırma mexaniz-minin müəyyən-ləşdirilməsi | Vahid məlumatlandırma mexanizminin tətbiqi |

| | | | | | | |
|---|---|---|---|---|---|---|
| **8.2.2. İnformasiya mühafizəsinin texniki, kriptoqrafik, proqram və digər vasitələri üzrə təminatının təkmilləşdirilməsi və bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi** | | | | | | |
| 8.2.2.1. İnformasiya 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 | mütəmadi | Ehtiyac meyarları-nın müəyyən-ləşdirilməsi | Prioritet sahələrin müəyyən-ləşdirilməsi | İnformasiya mühafizəsi təminatının təkmilləşdirilməsi və bu sahədə yerli istehsalçıların inkişafına dəstək verilməsi |
| 8.2.2.2. İnformasiya mühafizəsi vasitələrinin yerli istehsalçılarının stimullaşdırılması məqsədilə təkliflər hazırlamaq | NK | İN, XRİTDX, RİNN, DTX | mütəmadi | Ehtiyac sahələrinin müəyyən-ləşdirilməsi | Prioritet sahələrin seçilməsi | Seçilmiş prioritet sahələr üzrə layihələrin həyata keçirilməsi ilə bağlı təkliflər hazırlanması |
| 8.2.2.3. İnformasiya mühafizəsi vasitələri istehsalının, milli rəqəmsal iqtisadiyyatın, xüsusilə proqram mühəndisliyinin inkişafına təşkilati və elmi dəstək vermək | DTX | ETN, XRİTDX, RİNN, ASK | mütəmadi | Ehtiyac sahələrinin müəyyən-ləşdirilməsi | Prioritet sahələrin seçilməsi | Layihələrin həyata keçirilməsinə təşkilati və elmi dəstək verilməsi |
| 8.2.2.4. İnformasiya mühafizəsi sahəsində yerli istehsalın inkişafı məqsədilə kriptoqrafik mühafizə sahəsində milli resursların hazırlanması üçün tədbirlər görmək | DTX | XRİTDX, AMEA | 2023 – 2024 | Ehtiyac sahələrinin müəyyən-ləşdirilməsi | Sahə üzrə qabaqcıl təcrübələrin öyrənilməsi | Müvafiq sahədə milli resursların hazırlanması |
| **8.2.3. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində startapların fəaliyyətinin genişləndirilməsi** | | | | | | |
| 8.2.3.1. İnformasiya 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 | mütəmadi | Startapların fəaliyyətinin təşviqi üçün təkliflər hazırlan-ması, dəstək imkanları və | Akselarasi-ya proqramla-rının işlənilməsi, dəstək imkanları və | Təklif və proqramların həyata keçirilməsi, seçilmiş həll və startap fəaliyyətinin dəstəklənməsi |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | vasitələrinin müəyyən olunması | vasitələri-nin açıqlan-ması | |
| 8.2.3.2. İnformasiya 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 ödənişlərlə əlaqədar güzəştlərin müəyyən edilməsi ilə bağlı təkliflərin hazırlan-ması | Müvafiq fəaliyyət üzrə vergi və digər icbari ödənişlərlə əlaqədar güzəştlərin müəyyən edilməsi ilə bağlı təkliflərin təqdim olunması |
| **8.3. Prioritet 3. İnformasiya məkanının informasiya təhlükəsizliyinin təmin olunması səviyyəsinin yüksəldilməsi** | | | | | | |
| **8.3.1. İKT xidmət subyektlərində fəaliyyətin təkmilləşdirilməsi** | | | | | | |
| 8.3.1.1. İnformasiya xidməti, elektron xidmət və texniki xidmət subyektlərində və onların fəaliyyəti üzrə müvafiq obyektlərdə informasiya təhlükəsizliyinin təmin edilməsi fəaliyyətinin standartlara və qabaqcıl təcrübəyə uyğun formalaşdırılmasını təşviq etmək | RİNN | XRİTDX, İN, ASİ, VXSİDA | müntəzəm | Müvafiq sahə üzrə standartla-rın və qabaqcıl təcrübənin öyrənilməsi | Təşviqat material-larının hazırlan-ması və təşviqat işlərinin həyata keçirilməsi | Müvafiq təlimlər keçirilməsi |
| 8.3.1.2. İnformasiya məkanının və onun ayrı-ayrı seqmentlərinin, xüsusən də fərdi məlumatlar üzrə seqmentinin informasiya təhlükəsizliyinin təmin olunma səviyyəsinin ölçülməsinə, | RİNN | XRİTDX, VXSİDA, DTX | müntəzəm | Müvafiq sahədə informasiya | İnformasiya təhlükəsiz-liyinin ölçülmə- | Müvafiq qiymətləndirmələrin və təhlillərin səmərəli |

| | | | | | | |
|---|---|---|---|---|---|---|
| qiymətləndirilməsinə və təhlilinə aid mexanizmlər hazırlamaq və tətbiq etmək | | | | təhlükəsiz-liyinin təmin olunma səviyyəsi-nin mövcud vəziyyətinin öyrənilməsi | sinə, qiymətlən-dirilməsinə və təhlilinə aid mexanizm-lərin hazırlan-ması | mexanizmlər əsasında həyata keçirilməsi |
| **8.3.2. "Ağıllı" sistemlərin təhlükəsizliyinin təkmilləşdirilməsi** | | | | | | |
| 8.3.2.1. "Ağıllı" sistemlərin (dronlar, pilotsuz aparatlar, humanoidlər, robotlar və s.) yaradılmasına, tətbiqinə və utilizasiyasına aid təhlükəsizlik tələblərini müəyyən etmək | RİNN | XRİTDX, DTX, ETN | 2023 – 2025 | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Məsələ ilə əlaqədar təkliflərin hazırlan-ması | Təhlükəsizlik tələblərinin müəyyən edilməsi |
| 8.3.2.2. "Ağıllı" sistemlərin yaradılmasına, tətbiqinə və utilizasiyasına aid elmi, texnoloji, hüquqi və s. məsələlərin kompleks həlli üçün təkliflər vermək | RİNN | XRİTDX, DTX, ETN | 2024 – 2027 | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Müxtəlif həllərin tətbiqi imkanları-nın tədqiqi | "Ağıllı" sistemlərin yaradılması, tətbiqi və utilizasiyası üzrə fəaliyyətin səmərəli təşkilinin təmin edilməsi |
| **8.3.3. Mediada, o cümlədən milli rəqəmsal efir məkanında informasiya təhlükəsizliyi və kibertəhlükəsizliyin davamlı təkmilləşdirilməsi** | | | | | | |
| 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 | mütəmadi | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Rəqəmsal efir məkanına təhdidlərin qiymətlən-dirilməsi | 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 | mütəmadi | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Təhdidlərin qiymətlən-dirilməsi | 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 | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Tələblərin müəyyən-ləşdirilməsi | Tələblərin icrasına nəzarət mexanizminin yaradılması |
| **8.4. Prioritet 4. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi** | | | | | | |
| 8.4.1. Fövqəladə hallarda, müharibə şəraitində kritik informasiya infrastrukturlarının təhlükəsizliyini, kritik informasiya infrastrukturlarının idarə olunmasını təmin etmək üçün təşkilati əsasların yaradılması**,** risklərin qiymətləndirilməsi və idarə olunması planının hazırlanması | DTX | XRİTDX | 2024 – 2025 | Risklərin reyestrdə toplanma-sının təmin edilməsi | Qiymətlən-dirmənin aparılması | Risklərin idarə olunması üzrə planın hazırlanması |
| 8.4.2. Kritik informasiya infrastrukturlarının insidentlər zamanı bərpa planlarının hazırlanması | DTX | XRİTDX, İnfrastruk-tur subyekt-ləri | mütəmadi | Təhdidlər və risklərin qiymətlən-dirilməsi | Müvafiq bərpa planlarının hazırlan-masının təşkil olunması | Bərpa planlarının hazırlanması və təsdiq edilməsi |
| **8.5. Prioritet 5. Kibercinayətkarlığa qarşı mübarizə, o cümlədən kiberkriminalistika sahəsində fəaliyyətin gücləndirilməsi** | | | | | | |
| 8.5.1. “Kibercinayətlər” elektron informasiya sistemini formalaşdırmaq və bu sistemə səlahiyyətli qurumların çıxışının təmin edilməsi ilə bağlı təkliflər hazırlamaq | NK | DİN, DTX, BP (tövsiyə olunur), XRİTDX, RİNN, VXSİDA | 2023 – 2024 | İnformasiya sisteminin operatoru-nun müəyyən olunması, texniki şərtin hazırlanma-sı | İnformasiya sisteminin texniki şərti və səlahiyyət-lərin müvafiq qurumlarla razılaşdı-rılması | Sistemin operatoru tərəfindən sistemin yaradılması və fəaliyyətinin təşkili |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.5.2. Kibercinayətkarlıq və ona qarşı mübarizə sahəsində müvafiq ölçmə mexanizmlərini formalaşdırmaq və bu sahədə mütəmadi qiymətləndirməni həyata keçirmək | DTX | DİN, XRİTDX, BP (tövsiyə olunur), ƏN | mütəmadi | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Ölçmə mexanizm-lərinin formalaş-dırılması | Qiymətləndirmənin aparılması |
| 8.5.3. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində cinayətlərin aşkarlanması, sübutların toplanılması, cinayət işlərinin istintaqının aparılması üçün texniki imkanların genişləndirilməsini təşkil etmək | DTX | DİN, XRİTDX, BP (tövsiyə olunur), ƏN | mütəmadi | Sahə üzrə qabaqcıl təcrübənin öyrənilməsi | Texniki imkanların tədqiqi və araşdırıl-ması | 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 | mütəmadi | Sahə üzrə qabaqcıl 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 | mütəmadi | Hüquq mühafizə orqanları ilə əməkdaşlı-ğa ehtiyacı olan informasiya sistemləri operator-larının, telekom-munikasiya operator-larının və provayder-lərin müəyyən-ləşdirilməsi | Sahə üzrə əlaqədar cavabdeh şəxslərin müəyyən-ləşdirilməsi | Əməkdaşlıq və koordinasiyanın təmin edilməsi |

| | | | | | | |
|---|---|---|---|---|---|---|
| **8.6. Prioritet 6. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialın gücləndirilməsi, institusional bazanın inkişaf etdirilməsi** | | | | | | |
| **8.6.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işlərinin aparılmasına təşkilati dəstək verilməsi** | | | | | | |
| 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 laboratori-yaların yaradıl-ması, mövcud olanların təkmilləşdi-rilməsi üzrə ehtiyacların qiymətlən-dirilməsi | Yeni laboratoriyaların yaradılması və mövcud olanların təkmilləşdirilməsi |
| 8.6.1.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində elmi tədqiqat və layihə-təcrübə işləri sırasından prioritet mövzuların tətbiqi üçün seçilməsini təşkil etmək | ETN | RİNN, XRİTDX, DTX | mütəmadi | Prioritet mövzuların müəyyən-ləşdirilməsi | Həmin mövzular üzrə elmi tədqiqat və layihə-təcrübə işlərinin keyfiyyəti-nin 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 | ETN | DTX, XİN, XRİTDX, | mütəmadi | İnformasiya təhlükəsiz-liyi və | Birgə elmi tədqiqat layihələrinə | Müvafiq sahədə xarici ölkələrin elmi mərkəzləri |

| | | | | | | |
|---|---|---|---|---|---|---|
| layihələrinin həyata keçirilməsinə, beynəlxalq seminar və konfranslarda iştirakın təmin edilməsinə təşkilati dəstək vermək | | RİNN | | kibertəhlü-kəsizlik sahəsində xarici ölkələrin qabaqcıl elmi mərkəzləri-nin müəyyən-ləşdirilməsi | başlanılma-sı | ilə əməkdaşlığın genişləndirilməsi |
| 8.6.1.4. Kriptoqrafiyanın əsaslarının dərindən öyrənilməsini, bu sahədə elmi tədqiqatların aparılmasını, milli kriptoqrafik alqoritmin tətbiq olunduğu informasiyanın kriptoqrafik mühafizə vasitələrinin layihələndirilməsini və təkmilləşdirilməsini təmin edəcək yüksəkixtisaslı kadrların və səriştəli mütəxəssislərin hazırlanmasını təşkil etmək | DTX | XRİTDX, ETN | 2023 – 2024 | Sahə üzrə siyasət və prioritetlərin müəyyən-ləşdirilməsi | Fəaliyyət planının hazırlan-ması | Yüksəkixtisaslı və səriştəli mütəxəssislərin hazırlanması |
| **8.6.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət üçün kompetensiya (bilik, bacarıq və səriştə) tələbatları, tədris və təlim proqramları, maarifləndirmə materialları bazasının formalaşdırılması və aktuallığının davamlı təmin olunması** | | | | | | |
| 8.6.2.1. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə fəaliyyət üçün zəruri olan kompetensiyalara (bilik, bacarıq və səriştə) aid tələbatların mütəmadi öyrənilməsini, adekvat perspektivli ixtisasların müəyyən olunmasını təşkil etmək | ETN | RİNN, XRİTDX, DTX, ƏƏSMN | mütəmadi | Sahə üzrə daim artan tələbatların müəyyən-ləşdirilməsi | Yeni kompeten-siyaların (bilik, bacarıq və səriştə) siyahısının və mövcud çatışmaz-lıqlar üzrə | Yeni kompetensiyalara (bilik, bacarıq və səriştə) uyğun ixtisasların müəyyən edilməsi və təkliflər verilməsi |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | priortitet-lərin müəyyən-ləşdirilməsi | |
| 8.6.2.2. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə kompetensiyalar (bilik, bacarıq və səriştə)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 səmərəsinin davamlı yüksəldilməsi üçün tövsiyə, təklif və təşkilati dəstək vermək | NK | ETN, RİNN, XRİTDX, DTX, ƏƏSMN | mütəmadi | Sahə üzrə tədrisin texnoloji yeniliklərə və tələblərə uyğunluğu-nun ölçülməsi | Ölçü nəticəsində müəyyən edilən çatışmaz-lıqlar üzrə prioritet-lərin müəyyən-ləşdirilməsi | Tədrisin texnoloji yeniliklərə və tələblərə uyğunluğunun davamlı təmin edilməsi üçün təkmilləşdirmə işlərinin həyata keçirilməsi |
| **8.6.3. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə kadr hazırlığının və ixtisaslaşmış struktur bölmələrin müvafiq kadrlarla təminatının gücləndirilməsi** | | | | | | |
| 8.6.3.1. Dövlət orqanlarında (qurumlarında) informasiya təhlükəsizliyi üzrə ixtisaslaşmış struktur bölmələrin yaradılması və onların müvafiq kadrlarla təminatının planlaşdırılması ilə bağlı təkliflər hazırlamaq | DTX | XRİTDX, ƏƏSMN, DİM, RİNN, ETN, MN | 2024 | Qurumlar-dan sahə üzrə kadr ehtiyacları haqqında məlumat-ların toplanması | Kadr təminatı üçün planlı yanaşma-nın tətbiqinin araşdırıl-ması | 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 qiymətlən-dirilməsinin özəl və dövlət qurumla-rında müqayisəli | Qurumlar-da sahə üzrə əməyin stimullaş-dırılması üçün müvafiq mexanizm- | İxtisaslı kadrların əməyinin stimullaşdırılması |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | təhlilinin aparılması | lərin hazırlan-ması | |
| **8.6.4. İnformasiya təhlükəsizliyi üzrə kadr hazırlığında təhsil müəssisələri ilə dövlət və özəl sektor arasında əməkdaşlığın genişləndirilməsi** | | | | | | |
| 8.6.4.1. İnformasiya təhlükəsizliyi üzrə mütəxəssislərin tədris prosesinə cəlb olunması və tələbələrin təcrübə keçmələrinə şərait yaradılmasını təmin etmək | ETN | RİNN, DTX, XRİTDX, MN | mütəmadi | Sahə üzrə təcrübə imkanları-nın araşdırıl-ması | Təcrübə proqramları üçün əməkdaş-lığın qurulması | Mütəxəssislərin tədris prosesinə cəlbi 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 təhsilin müvafiq sahələrinin araşdırıl-ması | Mütəxəssis hazırlığı ilə bağlı müvafiq proqram-ların 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 alınmaqla təkliflər hazırlan-ması | Beynəlxalq və yerli şirkətlərin təkliflərə uyğun laborato-riyaların formalaş-dırılmasına 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 biliklər bazasının toplanması | Prioritet-lərin seçilməsi | Müvafiq onlayn maarifləndirmə, məsləhət xidmətlərinin formalaş-dırılması, dəstək verilməsi işlərinin həyata keçirilməsi |
| **8.7. Prioritet 7. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində normativ bazanın təkmilləşdirilməsi** | | | | | | |
| 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 alətləri, praktiki tövsiyələri təşviq etmək, milli standartların davamlı təkmilləşdirilməsinə dəstək vermək | RİNN | DTX, XRİTDX, ETN İN | mütəmadi | Ölkədə beynəlxalq standart-ların tətbiq olunması, milli standart-ların aktuallıq vəziyyət-lərinin, problem-lərin və tələbatların mütəmadi araşdırıl-ması | Ölkədə beynəlxalq standart-ların tətbiqinə, milli standartlar bazasının genişlən-məsinə aid təkliflər verilməsi | Təşkilati və metodiki tövsiyələrin verilməsi, icmalın dərc olunması |
| **8.8. Prioritet 8. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin yüksəldilməsi** | | | | | | |
| **8.8.1. Cəmiyyətdə informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyəti üzrə zəruri biliklərin, bacarıqların artırılmasına və təbliğinə dəstək verilməsi** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 kibercinayətkarlığa qarşı ictimai mübarizə üsulları və bu üsullardan 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), özəl təşkilatlarda informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətini formalaşdırmaq – kibergigiyenanı təmin etmək məqsədilə tədbirlər görmək | XRİTDX | RINN, DİM, VXSİDA | 2023 – 2027 | Nümunəvi kibergigiyena pilot layihəsinin həyata keçirilməsi | Kibergigiyenanın əməkdaşlar üçün əhəmiyyətinin təşviq olunması | Dövlət orqanlarında (qurumlarında), özəl sektorda informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması və kibergigiyenanın təmin edilməsi |
| **8.8.2. Uşaqların internetdən təhlükəsiz istifadə imkanlarının möhkəmləndirilməsinə təşkilati dəstək verilməsi** | | | | | | |
| 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 yaradılmasını, həmin mərkəzin beynəlxalq şəbəkələrə inteqrasiyasını təmin etmək | AQUPDK | RİNN, ETN | mütəmadi | Milli onlayn məlumatlandırma mərkəzinin yaradılması | Milli onlayn məlumatlandırma mərkəzinin fəaliyyətinin təşviq olunması, beynəlxalq şəbəkələrə inteqrasi- | Uşaqların zərərli informasiyadan qorunmasının təmin edilməsi |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | yasının təmin edilməsi | |
| 8.8.2.3. Təhsilin bütün səviyyələrində kibertəhlükəsizlik üzrə təhsil modulları hazırlamaq, eləcə də internetdə təhlükələr barədə materialları tədris resurslarına daxil etmək | ETN | RİNN, DTX | mütəmadi | Təhsilin bütün səviyyələrinə uyğun sahə üzrə materialların yaradılması | Yaradılmış materialların tədris resurslarına daxil edilməsi | Bu materialların mütəmadi yenilənməsinin həyata keçirilməsi |
| **8.9. Prioritet 9. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə ölkədaxili və beynəlxalq əməkdaşlığın inkişaf etdirilməsi** | | | | | | |
| **8.9.1. Dövlət orqanları (qurumları), özəl sektor və vətəndaş cəmiyyəti institutları arasında əməkdaşlığın inkişaf etdirilməsi** | | | | | | |
| 8.9.1.1. İnformasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması, o cümlədən insidentlərə qarşı tədbirlər görülməsi üçün dövlət orqanları (qurumları), özəl sektor və vətəndaş cəmiyyəti institutları arasında əməkdaşlıq formalarını müəyyən etmək və onların hüquqi əsasını yaratmaq | XRİTDX | RİNN, DTX, DİN | 2023 – 2024 | Əməkdaşlığın müxtəlif formalarının effektivliyinin araşdırılması | Uyğun əməkdaşlıq formalarının seçilməsi | Əməkdaşlığın hüquqi əsasının yaradılması |
| 8.9.1.2. Təhdidləri qiymətləndirmə və həlli yollarını müəyyənetmə sahəsində dövlət–özəl 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) | RİNN | DTX, DİN, | müntəzəm | Təhdidlər, boşluqlar, | Əldə edilən məlumat- | Mexanizmlərin avtomatlaşdırılması |

| | | | | | | |
|---|---|---|---|---|---|---|
| informasiya mübadiləsi və qarşılıqlı əməkdaşlıq sahəsində əlaqələndirməni həyata keçirmək, təhdidlərə və hücumlara qarşı erkən xəbərdarlıq, cavabvermə imkanlarını formalaşdırmaq | | XRİTDX | | risklər və s. məlumatların əldə edilməsi və toplanmasının təşkili | ların bölüşdürülməsi və erkən xəbərvermə mexanizmlərinin yaradılması | 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 | Əməkdaşlığın müxtəlif formalarının effektivliyinin araşdırılması | Pilot layihələrin həyata keçirilməsi | Uğurlu layihələr üzrə əməkdaşlığın davam etdirilməsi |
| **8.9.2. İnformasiya təhlükəsizliyini idarəetmə sahəsində beynəlxalq təşkilatlarla əməkdaşlığın inkişaf etdirilməsi** | | | | | | |
| 8.9.2.1. Kibercinayətkarlığa qarşı mübarizə üzrə beynəlxalq əməkdaşlığı genişləndirmək, qabaqcıl təcrübənin mənimsənilməsini və bölüşdürülməsini 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, XKX | mütəmadi | İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə mütəxəs- | Qabaqcıl təcrübəyə əsaslanan təlimlərin və görüşlərin kataloqu- | Sahə üzrə mütəxəssislərin iştirakına təşkilati dəstək verilməsi |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | sislərlə davamlı əlaqə yaradılması | nun yaradılması | |
| 8.9.2.3. İnformasiya təhlükəsizliyi subyektləri, o cümlədən Milli CERT və digər CERT-lər səviyyəsində beynəlxalq əməkdaşlığın inkişaf etdirilməsini, kibertəhlükəsizlik sahəsində beynəlxalq təcrübənin öyrənilməsini təşkil etmək | RİNN | XRİTDX, ETN, DTX, MB | mütəmadi | Beynəlxalq CERT mərkəzləri ilə əməkdaş-lığın inkişaf etdirilməsi | Beynəlxalq CERT mərkəzlə-rinə üzvlüyün təmin edilməsi | Beynəlxalq fəaliyyətdə qarşılıqlı fəaliyyət və təcrübə mübadiləsinin gücləndirilməsi |

**Akronimlər**

AQUPDK – Azərbaycan Respublikasının Ailə, 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 (İşəgötürənlər) Təşkilatları Milli Konfederasiyası
BP – Azərbaycan Respublikasının Baş Prokurorluğu
DİM – 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 Əhalinin Sosial Müdafiəsi Nazirliyi
ƏN – Azərbaycan Respublikasının Ədliyyə Nazirliyi
XRİTDX – Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti
XİN – Azərbaycan Respublikasının Xarici İşlər Nazirliyi
XKX – Azərbaycan Respublikasının Xarici Kəşfiyyat Xidməti
İN – Azərbaycan Respublikasının İqtisadiyyat Nazirliyi
MB – Azərbaycan Respublikasının Mərkəzi Bankı
MN – Azərbaycan Respublikasının Müdafiə Nazirliyi
MdN – Azərbaycan Respublikasının Mədəniyyət Nazirliyi
NK – Azərbaycan Respublikasının Nazirlər Kabineti
RİNN – Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi
ETN – Azərbaycan Respublikasının Elm və Təhsil Nazirliyi
VXSİDA – Azərbaycan Respublikasının Prezidenti yanında Vətəndaşlara Xidmət və Sosial İnnovasiyalar üzrə Dövlət Agentliyi