QANUN № 01 (375), 2026, s. 63-67

**Hacıyev Həbib Bəhruz oğlu,**
hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universitetinin doktorantı
E-mail: h.hajiyev@hotmail.com

**UOT 34:004.8:341**
**DOI: https://doi.org/10.30546/2218-9130.041.2026.4015**

# KİBERTƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİNDƏ DÖVLƏT-ÖZƏL ƏMƏKDAŞLIĞININ BƏZİ XÜSUSİYYƏTLƏRİ

***Açar sözlər:*** *kibertəhlükəsizlik, informasiya təhlükəsizliyi, rəqəmsallaşma, onlayn xidmətlər, texnoloji həllər, dövlət-özəl əməkdaşlığı.*

***Ключевые слова****: кибербезопасность, информационная безопасность, цифровизация, онлайн-сервисы, технологические решения, государственно-частное сотрудничество.*

***Keywords:*** *cybersecurity, information security, digitalization, online services, technological solutions, public-private cooperation.*

Müasir dövrdə kibertəhlükəsizlik problemi nəinki ayrı-ayrı milli dövlətlərin, bütövlüklə beynəlxalq ictimaiyyətin diqqət mərkəzinə çevrilib. Təsadüfi deyildir ki, BMT Təhlükəsizlik Şurasının üzv dövlətlərin nümayəndələrinin iştirakı ilə 29 iyun 2021-ci il tarixdə şəffaf beynəlxalq informasiya təhlükəsizliyi sisteminin inkişafı və təhlükəsizliyə təhdid yaradan kiberinsidentlər məsələlərinin nəzərdən keçirilməsinə həsr olunmuş "Beynəlxalq sülhün və təhlükəsizliyin qorunması: Kibertəhlükəsizlik" mövzusunda iclası keçirilmişdir. Bununla belə, bəhs etdiyimiz sferada həm milli qanunvericilik, həm də beynəlxalq səviyyədə hələ də tam həcmdə adekvat tənzimləmə mexanizmlərinin yaradılmadığı etiraf edilməlidir.

Bu sahədə müəyyən ətalətli vəziyyətin mövcud olmasının səbəbləri sırasında kibertəhlükəsizliyin özünün xüsusiyyətləri, əhatə dairəsi və konseptual çərçivəsi üzrə bir-sıra qeyri-müəyyənliklərin olduğu da vurğulanmalıdır. Terminoloji qeyri-müəyyənliyin özü də müəyyən praktiki nəticələr doğurur. Nəzərdən keçirilən kontekstdə kibertəhlükəsizliyin tərifi nədən, kimdən və necə qorunmağa çalışıldığından, eləcə də imkanların atributunun mümkün olub-olmamasından bilavasitə asılıdır. Kibertəhlükəsizliyin anlayışı qeyri-müəyyən olduqda onun təmin edilməsi üçün məsuliyyətin kimin üzərinə qoyulmasının müəyyən edilməsi də çətin olur və praktiki baxımdan müəyyən çətinlikləri doğurur.

Ayrı-ayrı ölkələrdə istifadə olunan rəqəmsal alətlərin və texnoloji inkişaf tendensiyalarının müxtəlifliyinə baxmayaraq, onların ümumi palitrası demək olar ki, dünyanın hər yerində eynidir. Qlobal miqyasda ən mühüm rəqəmsal texnologiyalara süni intellekt, kiber-fiziki texnologiyalar, rəqəmsal infrastruktur, rəqəmsal maliyyə, 4-cü sənaye inqilabı, kibertəhlükəsizlik kimi texnoloji klasterlər aid edilir. Ağıllı saatlar, rəqəmsal eynəklər, bilərziklər, qulaqlıqlar və sensorlar

əməliyyatların müxtəlif aspektlərinə nəzarət etməyə kömək edir. Onlar həmçinin sağlamlıq və ətraf mühit haqqında məlumat ötürür və məlumatlara çıxışı təmin edir.

2028-ci ilə qədər həm şəxsi, həm də sənaye istifadəsi üzrə taxıla bilən cihazlar üçün qlobal bazarın üç dəfədən çox böyüyərək 380,5 milyard dollara çatacağı proqnozlaşdırılır. Texnologiyaları tətbiq edən şirkətlərin 76%-i (Amazon və Walmart da daxil olmaqla) bunun işçilərin məhsuldarlığını, istehsal təhlükəsizliyini artırdığını, səhvləri və xərcləri azaltdığını və bununla da səmərəliliyin artırılmasına kömək etdiyini qeyd edirlər. Rəqəmsal əkizlər sənayesinin[4] orta illik artım səviyyəsi 60%-ə çatmaqdadır. MarketsandMarkets-in məlumatına görə, istehsalçı şirkətlər bu texnologiyanın əsas müştərilərə çevrilirlər və 2027-ci ilə qədər bu texnologiyaya əsaslanan həllər üçün qlobal bazarın həcmi 73,5 milyard dollara çatacaqdır. Sistemlərin və proseslərin virtual nüsxələri fərziyyələri sınaqdan keçirməyə və səhvləri müəyyən etməyə kömək edir, nəticədə resurslara qənaət edilir və əməliyyatlar optimallaşdırılır. Məsələn, virtual əkizlərin sayəsində iri yük maşını istehsalçısı olan CNH Industrial texniki xidmət zamanı avadanlıqların dayanma müddətinin azaldılmasına nail olmuşdur, əks halda bu, hər bir dəqiqədə 160.000 dollar itkiyə gətirib çıxara bilir [3].

Bütün bu texnoloji inkişaf prosesləri paralel olaraq kibertəhlükəsizlik xərclərinin və bu sahəyə qoyulan qlobal investisiyaların həcminin artırılmasını da labüd edir. Belə ki, şirkətlərin rəqəmsal immuniteti avtomatlaşdırmadan tutmuş sınaqlara qədər müxtəlif kibertəhlükəsizlik texnologiyaları və təcrübələrindən istifadə edilməklə qurulmasına ehtiyac duyulur. Həmin texnologiyalar məcmu halında məhsulların, xidmətlərin və sistemlərin davamlılığını artırır. Bu baxımdan şirkətlərə onlayn rejimdə davamlı informasiya texnologiyalarının sistem sınaqlarından tutmuş texniki nasazlıqların qarşısını almağa və azaltmağa kömək edən xaos mühəndisliyinə qədər texnoloji həlləri nəzərdə tutan kibertəhlükəsizlik strategiyalarının işlənib hazırlanması tövsiyə edilir.

Geniş mənada kibertəhlükəsizlik kibermühiti, təşkilatın və istifadəçinin resurslarını qorumaq üçün istifadə edilə bilən alətlər, strategiyalar, təhlükəsizlik prinsipləri, təhlükəsizlik tədbirləri, təlimatlar, risklərin idarə edilməsi, praktik təcrübə, sığorta, texnologiyalar və s. toplusudur. Təşkilatın və istifadəçinin resurslarına qoşulmuş hesablama cihazları, personal, infrastruktur, müxtəlif tətbiqlər, xidmətlər, telekommunikasiya sistemləri və kibermühitdə ötürülən və ya saxlanılan bütün məlumatlar aid edilir. Kibertəhdidlər termini, əsasən, kompüterlər və ya kompüter şəbəkələri vasitəsilə həyata keçirilən qanunsuz fəaliyyəti əhatə edir. Kibertəhdidin bir növü kimi çıxış edən kibercinayətkarlığa nümunə olaraq bu vasitələrdən istifadə edilməklə törədilən oğurluq, şəxsi həyatın toxunulmazlığının pozulması, vacib infrastruktura edilən kiberhücumlar və s. neqativ əməllər aid edilir.

Məsələ burasındadır ki, bu günədək kibertəhlükəsizliyin anlayışı ilə bağlı universal yanaşma formalaşmamışdır və bu səbəbdən mütəxəssislər kontentdən asılı olaraq bu termini fərqli-fərqli mənada istifadə edirlər. 2010-cu ilin 4-22 oktyabr tarixlərində Meksikanın Qvadalaxara şəhərində Beynəlxalq Telekommunikasiya İttifaqının (BTİ) 18-ci Səlahiyyətli Konfransı (PP-10 kimi də tanınır) keçirilmişdir. Konfransda üzv dövlətlər BTİ-nin gələcəyini, onun İKT-nin inkişafındakı rolunu müəyyən etmiş və 2000-dən çox iştirakçını bir araya gətirərək qlobal rəqəmsallaşmaya

[4]Rəqəmsal əkizlər sənayesi - fiziki obyektlərin, sistemlərin və ya proseslərin virtual modelini yaradaraq, onları simulyasiya etməklə səmərəliliyi optimallaşdırmağa, nasazlıqları proqnozlaşdırmağa və daha yaxşı qərarlar qəbul etməyə imkan verən innovativ bir sahədir. Bu texnologiya istehsal, səhiyyə, tikinti, avtomobil və enerji kimi müxtəlif sektorlarda tətbiq olunaraq, dizayn, işləmə və texniki xidmətdə inqilabi dəyişikliklər yaradır, daha sürətli rəqəmsallaşmaya xidmət edir.

diqqət yetirərək idarəetmə orqanlarını seçmişlər. Birləşmiş Millətlər Təşkilatı (BMT) tərəfindən kibertəhlükəsizliyin istifadə edilən anlayışı məhz həmin Səlahiyyətli Konfransda qəbul edilmişdir: Kibertəhlükəsizlik dedikdə, aktivləri (kompüterlər, infrastruktur, tətbiqlər, xidmətlər, rabitə və informasiya sistemləri) və kiberməkanı hücumdan, zərərdən və icazəsiz girişdən qorumağa yönəlmiş texnologiyalar, konsepsiyalar, dövlət siyasətləri, prosedurlar və təcrübələr nəzərdə tutulur [2].

Regional səviyyədə, xüsusən, Avropa İttifaqı miqyaslı təhlükəsizlik standartları, tənzimləyici çərçivə daxilində xeyli sayda sektor və təşkilatı əhatə etmək üçün müvafiq standartların əhatə dairəsini genişləndirir. Bu genişlənmənin əsas məqsədi təchizat zəncirinin təhlükəsizliyini gücləndirmək, hesabat tələblərini sadələşdirmək və ittifaq daxilində daha sərt kibertəhlükəsizlik risklərinin idarə edilməsi tədbirlərini tətbiq etmək, kritik rəqəmsal infrastrukturun qorunmasını və təşkilatların kibertəhlükəsizlik dayanıqlığının yüksək standartlarını qorunmasını təmin etməkdir. Təşkilatların əhəmiyyətlilik parametrlərinə görə ayrı-ayrı kateqoriyalara bölünməsi nəzərdə tutulur. Bu təsnifat təşkilatın kritik sektorlarla əlaqəsi və onun ümumi həcmi kimi amillərə əsaslanır. Çoxsaylı kibertəhlükəsizlik təşəbbüsləri daha geniş hüquqi çərçivənin yalnız kiçik bir hissəsini əhatə edir. Ümumiyyətlə, kibertəhlükəsizliyin tərifi və ya konsepsiyası çox vaxt konkret hüquqi mühit tərəfindən müəyyən edilir.

Kibertəhlükəsizlik anlayışının informasiya təhlükəsizliyi kontekstində nəzərdən keçirilməsi məqsədəuyğun hesab olunur. Müasir dövrdə informasiya təhlükəsizliyi sahəsində başlıca istiqamətlərdən biri dövlət-hökumət-biznes əməkdaşlığının təmin edilməsidir. Bu istiqaməti müəyyən edə biləcək və müzakirəyə təkan verən başlıca amillərdən biri 2013-cü ildən bəri Avropa İttifaqının müxtəlif qurumlarında Şəbəkə və İnformasiya Təhlükəsizliyi üzrə Direktivinin layihəsi olmuşdur. Direktivin qəbul edilməsində əsas məqsəd Aİ üzv dövlətlərində informasiya təhlükəsizliyi ilə bağlı yanaşmaların uyğunlaşdırılması olmuşdur. Sənədin vacib yeniliklərdən və ətrafında qızğın müzakirələrin aparıldığı təkliflərdən biri Avropa Komissiyasının özəl şirkətlərin üzərinə informasiya təhlükəsizliyi ilə bağlı baş verən hadisələr barədə məlumat vermək öhdəliyinin qoyulması olmuşdur. Bu öhdəliklərin əhatə dairəsi kritik infrastruktur operatorları (enerji, nəqliyyat, maliyyə və səhiyyə sahəsində) və informasiya təhlükəsizliyinin təmin edilməsinə dair müxtəlif yanaşmalarla bağlı maneəyə çevrilmiş internet sənayesindəki müxtəlif şirkətlər daxil olmaqla geniş İT şirkətlərini əhatə etmişdir. Üzərində informasiya təhlükəsizliyi hadisələri barədə məlumat vermək öhdəliyi qoyulan qurumların sayı isə kifayət qədər çoxdur.

Direktiv internet xidmətləri sahəsində fəaliyyət göstərən şirkətləri, informasiya mübadiləsi öhdəlikləri və məsuliyyətlərinin əhatə dairəsi baxımından, kritik infrastruktur operatorları ilə bərabərləşdirmişdir. Bu baxımdan Avropa İttifaqının Şəbəkə və İnformasiya Təhlükəsizliyi Direktivi üzv dövlətlərin şəbəkə və informasiya sistemlərinin təhlükəsizliyinin gücləndirilməsini hədəfləmişdir. Direktiv həmçinin kritik infrastruktur və vacib xidmətlərin operatorlarını müvafiq təhlükəsizlik tədbirlərini həyata keçirməyə və hər hansı bir hadisə barədə dərhal müvafiq orqanlara və maraqlı tərəflərə məlumat verməyə məcbur edir [1].

Aİ-nin Şəbəkə və İnformasiya Təhlükəsizliyi Direktivi və onun ətrafında gedən müzakirələr əslində informasiya təhlükəsizliyi sahəsində bir sıra fundamental məsələləri özündə əks etdirir. Avropa İttifaqında informasiya təhlükəsizliyi sahəsində hökumət-biznes əməkdaşlığına yanaşmalar və bu yanaşmaların uyğunlaşdırılması imkanları ilə bağlı müzakirələrdə əsas suallardan

biri də informasiya təhlükəsizliyini təmin etmək üçün internet xidməti təminatçılarını tənzimləmək zərurətinə kompromis cavabın tapılmasıdır. Tənzimləmə ehtimalı ilə bağlı müzakirələrin aparılması zərurəti bir çox ölkələrdə, o cümlədən Aİ-nin üzv dövlətlərində son onilliklər ərzində informasiya təhlükəsizliyində iştiraka yanaşma kiberhücumlar barədə məlumat mübadiləsində könüllü əməkdaşlığın inkişaf etdirilməsi və təhdidlərin qarşısını almaq üçün birgə və hərtərəfli mexanizmlərin hazırlanması ideyasına əsaslanmışdır.

İnformasiya cəmiyyəti xidmətlərini göstərən operatorların informasiya və şəbəkə təhlükəsizliyi sahəsində tənzimlənən subyektlər sırasına daxil edilməsi, tənzimlənən subyektlərin əhatə dairəsinin qeyri-müəyyənliyi, şəbəkə təhlükəsizliyi insidentləri barədə məlumat vermək öhdəliyi ilə bağlı aydınlığın olmaması, hökumətin könüllü tənzimləmə konsepsiyasından əməkdaşlıq konsepsiyasına keçməsi müvafiq sahədə müzakirələrin daha da genişlənməsinə rəvac vermişdir. Müzakirələrdən sonra Avropa Parlamenti 2014-cü ilin martında direktiv layihəni qəbul edərək, informasiya cəmiyyəti xidmətlərini göstərən operatorları tənzimləmə çərçivəsindən çıxarmışdır. Avropa Komissiyasının nümayəndələri və ekspertləri bu qərardan sonra həmin müddəaların istisna edilməsi üzrə öz narazılıqlarını ifadə etmişdir.

Ümumiyyətlə, Aİ-yə üzv dövlətlərin hökumət və biznes arasında etimadın yaradılması ilə bağlı mövqeyi milli səviyyədə dövlət-özəl sektor əməkdaşlığının vəziyyətindən və təbii ki, mövcud mexanizmlərdə etimadın oynadığı roldan birbaşa asılıdır. Məsələn, Böyük Britaniyada hökumət informasiya təhlükəsizliyi sahəsində dövlət-özəl əməkdaşlığın ən qızğın tərəfdarlarından biri kimi çıxış edir. Almaniya da, həmçinin, Avropa İttifaqının biznes subyektlərindən informasiya təhlükəsizliyi insidentləri barədə məlumat verilməsini nəzərdə tutan qanunu qəbul edən ilk dövlətlərdən biri sayılır.

2014-cü ilin oktyabrında informasiya cəmiyyəti xidmətlərinin tənzimlənməsi məsələsi əvvəlkindən daha çox aktuallaşmış və aydın olmuşdur ki, Aİ-yə üzv dövlətlər nəinki informasiya təhlükəsizliyi insidentləri barədə hesabat öhdəliklərinin kimlərə verilməsi və bu cür öhdəliklərin ümumiyyətlə tətbiq edilib-edilməməsi ilə bağlı konsensusa gələ bilmirlər. Nəticədə, informasiya cəmiyyəti xidmətlərinin tənzimlənməsi ilə bağlı direktiv layihədə iki əsas dəyişiklik edilmişdir. Birincisi, Avropa Parlamenti tərəfindən nəinki bütün informasiya cəmiyyəti xidmətlərini göstərən operatorlar tənzimlənən qurumlar siyahısından çıxarılmış, həm də Avropa Şurası internet mübadilə məntəqələri, domen adlarının qeydiyyatçıları və veb hostinq şirkətlərinin daxil edilməsi üçün siyahının genişləndirilməsini təklif etmişdir. İkincisi, Aİ-nin Üzv Dövlətləri tənzimlənən qurumların əhatə dairəsi ilə bağlı konsensusa gələ bilmədiklərinə görə, hər hansı bir şirkətin tənzimlənən qurumlar siyahısına daxil edilməsini Aİ Üzv Dövlətlərinin ixtiyarına buraxılmışdır [4].

Qeyd edilənlərə yekun vuraraq göstəririk ki, informasiya təhlükəsizliyinin vacib həlqələrindən biri kimi çıxış edən kibertəhlükəsizliyin mexanizmlərinin yaradılması hökumətdən və biznes subyektlərindən xeyli vaxt və əmək tələb edir. Və burada əsas məqsəd məhz dövlət-özəl əməkdaşlığında informasiya təhlükəsizliyinin təmin edilməsinə dair yanaşmaların uyğunlaşdırılmasına nail olmaqdır.

**İstifadə edilmiş ədəbiyyat siyahısı:**

1. Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза (документ не действует) / https://base.garant.ru/71737658/
2. Заключительные акты полномочной конференции (Гвадалахара, 2010 г.) / https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2010-PDF-R.pdf
3. Топ-10трендовцифровизации / https://rostelecom.vedomosti.ru/top-trends.html
4. Тропина Т. Проект Директивы Европейского союза о сетевой и информационной безопасности: попытка гармонизации или путь к фрагментации? / https://pircenter.org/editions/proekt-direktivy-evropejskogo-sojuza-o-setevoj-i-informacionnoj-bezopasnosti-br-popytka-garmonizacii-ili-put-k-fragmentacii/

**Гаджиев Хабиб Бахруз оглу,**
доктор философии по праву,
докторант Бакинского государственного университета

## НЕКОТОРЫЕ ОСОБЕННОСТИ ГОСУДАРСТВЕННО-ЧАСТНОГО СОТРУДНИЧЕСТВА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

### РЕЗЮМЕ

В современном мире развитие процессов цифровизации продолжается беспрецедентными темпами. Деятельность всех сфер жизни — от умных домов и городов до четвёртой промышленной революции — сопровождается цифровыми устройствами. Это, несомненно, создаёт большие возможности для повышения эффективности использования потенциала, но одновременно порождает серьёзные проблемы, такие как кибербезопасность, обеспечение конфиденциальности данных, требующие применения глобального регулирования и этических стандартов. Киберреволюция развивается настолько стремительно и непредсказуемо, что законодательство порой не успевает за этими нововведениями. В статье представлены позиции международных организаций и экспертов по этим вопросам.

**Hajiyev Habib Bahruz,**
PhD in Law, Doctoral Student, Baku State University

## SOME FEATURES OF PUBLIC-PRIVATE COOPERATION IN ENSURING CYBERSECURITY

### SUMMARY

In the modern world, the development of digitalization processes continues at an unprecedented pace. The activities of all spheres of life - from smart homes and cities to the 4th Industrial Revolution - are accompanied by digital devices. This undoubtedly creates great opportunities for increasing the efficiency of potential, but at the same time it creates serious problems such as cybersecurity, ensuring data confidentiality, which require the application of global regulation and ethical standards. The cyber revolution is progressing so rapidly and unpredictably that legislation sometimes cannot keep up with these innovations. The article presents the positions of international organizations and experts on these issues.

**Redaksiyaya daxilolma tarixi: 05.01.2026**
**Təkrar işlənməyə göndərilmə tarixi: 17.01.2026**
**Çapa qəbul olunma tarixi: 20.01.2026**