QANUN № 06 (380), 2026, s. 30-42

Ağamalıyev Ümman İlqar oğlu,
hüquq üzrə fəlsəfə doktoru, Azərbaycan Respublikası Vəkillər Kollegiyasının üzvü,
Milli Aviasiya Akademiyasının Hüquq kafedrasının müəllimi,
Milli Aviasiya Akademiyasının doktorantı
Ünvan: Bakı ş., Cəfər Cabbarlı küç., 609, Globus Center, 5-ci mərtəbə
E-mail: umman.agamali@gmail.com

UOT 342
DOI: https://doi.org/10.30546/2218-9130.060.2026.0110

AZƏRBAYCAN RESPUBLİKASINDA RƏQƏMSAL DÖVLƏT TƏHLÜKƏSİZLİYİNİN HÜQUQİ ƏSASLARI VƏ KİBERSUVERENLİK PRİNSİPİ

Açar sözlər: *rəqəmsal dövlət təhlükəsizliyi, kibersuverenlik, dövlət informasiya ehtiyatları, dövlət informasiya sistemləri, kritik informasiya infrastrukturu, informasiya təhlükəsizliyi, kibertəhlükəsizlik, Hökumət buludu, EHİS, fərdi məlumatların mühafizəsi.*

Ключевые слова: *цифровая государственная безопасность, киберсуверенитет, государственные информационные ресурсы, государственные информационные системы, критическая информационная инфраструктура, информационная безопасность, кибербезопасность, Правительственное облако, защита персональных данных.*

Keywords: *digital state security, cyber sovereignty, state information resources, state information systems, critical information infrastructure, information security, cybersecurity, Government Cloud, e-government information system, personal data protection.*

Müasir dövlət idarəetməsində təhlükəsizlik anlayışı artıq yalnız sərhədlərin, hərbi infrastrukturun və ya klassik ictimai qaydanın qorunması ilə məhdudlaşmır. Dövlətin real idarəetmə qabiliyyəti getdikcə daha çox onun rəqəmsal infrastrukturlarının dayanıqlılığından, dövlət informasiya ehtiyatlarının bütövlüyündən, kritik informasiya infrastrukturu obyektlərinin fasiləsiz fəaliyyətindən və fərdi məlumatların qanuni mühafizəsindən asılı vəziyyətə düşür. Elektron xidmətlər, elektron sənəd dövriyyəsi, dövlət reyestrləri, dövlət informasiya sistemləri, Hökumət buludu, Elektron Hökumət İnformasiya Sistemi, rəqəmsal identifikasiya və qurumlararası məlumat mübadiləsi dövlət idarəetməsinin texniki yardımçı elementləri olmaqdan çıxaraq onun funksional nüvəsinə çevrilmişdir. Belə şəraitdə dövlətin rəqəmsal mühitdə təhlükəsizliyi təkcə texniki müdafiə tədbirləri deyil, həm də konstitusion hüquq, inzibati hüquq, informasiya hüququ və milli təhlükəsizlik hüququ ilə birbaşa bağlı kompleks hüquqi institut kimi nəzərdən keçirilməlidir.

Rəqəmsal dövlət təhlükəsizliyi anlayışının hüquqi məzmunu üç əsas istiqamətdə açılır. Birinci istiqamət dövlət informasiya ehtiyatlarının və sistemlərinin hüquqi rejimidir. Dövlət orqanlarının və publik hüquqi şəxslərin fəaliyyəti nəticəsində formalaşan məlumatlar sadəcə texniki verilənlər deyil, dövlət idarəetməsinin yaddaşı, qərar qəbul etmənin sübut bazası və ictimai xidmətlərin davamlılığının əsas şərtidir. İkinci istiqamət informasiya təhlükəsizliyi və kibertəhlükəsizlikdir. Burada məqsəd informasiyanın məxfiliyinin, bütövlüyünün, əlçatanlığının, autentikliyinin və inkarolunmazlığının təmin edilməsidir. Üçüncü istiqamət isə kibersuverenlik prinsipidir. Bu prinsip dövlətin rəqəmsal məkanında hüquqi yurisdiksiya, milli məlumat infrastrukturu, dövlət informasiya ehtiyatları üzərində nəzarət, kritik sistemlərin xarici asılılıqlardan qorunması və rəqəmsal xidmətlərin davamlılığı üzərində suveren səlahiyyətini ifadə edir.

Azərbaycan Respublikasında bu sahənin hüquqi bazası artıq çoxqatlı normativ arxitektura şəklində formalaşmışdır. Azərbaycan Respublikasının Konstitusiyası dövlətin suverenliyi, insan hüquqlarının təmin edilməsi, informasiya azadlığı, şəxsi toxunulmazlıq və məhkəmə müdafiəsi kimi ümumi hüquqi əsasları müəyyən edir [1]. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" qanun informasiya ehtiyatları, informasiya sistemləri, texnologiyalar və onların mühafizəsi ilə bağlı baza hüquqi çərçivə yaradır [2]. "Fərdi məlumatlar haqqında" qanun və fərdi məlumatların mühafizəsinə dair tələblər fərdi məlumatların toplanılması, işlənilməsi və qorunmasını dövlət informasiya sistemləri kontekstində xüsusi hüquqi rejimə tabe edir [3; 4]. "Dövlət sirri haqqında" qanun isə dövlət təhlükəsizliyi üçün xüsusi əhəmiyyət daşıyan məlumatların məxfilik rejimini müəyyən edir [5]. Bu normativ sənədlər rəqəmsal dövlət təhlükəsizliyinin klassik hüquqi əsaslarını təşkil edir.

Rəqəmsal təhlükəsizliyin xüsusi institusional mərhələsi kritik informasiya infrastrukturu ilə bağlı hüquqi rejimin formalaşdırılması ilə bağlıdır. Azərbaycan Respublikasında kritik informasiya infrastrukturu təhlükəsizliyi haqqında normativ aktlar dövlət, cəmiyyət və iqtisadiyyat üçün həyati əhəmiyyət daşıyan informasiya sistemlərinin müəyyənləşdirilməsini, onların təhlükəsizlik risklərinin idarə olunmasını, təhlükəsizlik tələblərinin tətbiqini, reyestr mexanizmlərini və nəzarət alətlərini nəzərdə tutur [8; 9]. Bu yanaşma onu göstərir ki, rəqəmsal dövlət təhlükəsizliyi yalnız məlumatların qorunması ilə məhdudlaşmır; burada dövlət xidmətlərinin fasiləsizliyi, kiberinsidentlərə reaksiya, infrastrukturun davamlılığı və milli idarəetmə qabiliyyətinin saxlanılması da eyni dərəcədə mühüm hüquqi məqsəd kimi çıxış edir.

Məqalənin məqsədi Azərbaycan Respublikasında rəqəmsal dövlət təhlükəsizliyinin hüquqi əsaslarını sistemli şəkildə təhlil etmək, dövlət informasiya ehtiyatlarının qorunması barədə normativ aktların bu sistemdə yerini müəyyənləşdirmək və kibersuverenlik prinsipinin konstitusion-hüquqi məzmununu araşdırmaqdan ibarətdir. Məqalədə dövlət informasiya ehtiyatları və sistemlərinin hüquqi rejimi, kritik informasiya infrastrukturu, Hökumət buludu, EHİS, fərdi məlumatların mühafizəsi, informasiya təhlükəsizliyi strategiyası və rəqəmsal inkişaf konsepsiyası vahid hüquqi ekosistem kimi nəzərdən keçirilir.

Rəqəmsal dövlət təhlükəsizliyinin konstitusion-hüquqi məzmunu

Rəqəmsal dövlət təhlükəsizliyi anlayışının konstitusion məzmunu dövlət suverenliyi ilə insan hüquqlarının qorunması arasında tarazlıq üzərində qurulur. Azərbaycan Respublikası Konstitusiyasının 7-ci maddəsində dövlət hakimiyyətinin təşkili, 12-ci maddəsində insan və vətəndaş hüquq və azadlıqlarının təmin edilməsi dövlətin ali məqsədi kimi müəyyən olunur.

Rəqəmsal idarəetmə mühitində bu müddəalar yeni məna qazanır. Çünki dövlət orqanlarının qərarları, elektron xidmətlər, informasiya sistemləri və reyestrlər vətəndaşın hüquqi vəziyyətinə birbaşa təsir göstərir. Məlumatın itirilməsi, təhrif olunması, qanunsuz əldə edilməsi və ya sistemlərin dayanması artıq texniki nasazlıq kimi deyil, vətəndaşın hüquqlarına, dövlət idarəçiliyinin qanuniliyinə və ictimai etimada zərbə kimi qiymətləndirilməlidir.

Konstitusiyanın 32-ci maddəsi şəxsi və ailə həyatının sirrini, şəxsi toxunulmazlığı və fərdi məlumatların qorunması ilə bağlı konstitusion təminatı müəyyən edir. Dövlət informasiya sistemlərində toplanan məlumatların böyük hissəsi fiziki şəxslərlə bağlı olduğundan rəqəmsal dövlət təhlükəsizliyi fərdi məlumatların hüquqi müdafiəsi olmadan təsəvvür edilə bilməz. Bu baxımdan "Fərdi məlumatlar haqqında" qanunun məqsədi yalnız məlumat sahibinin razılığı və ya məlumatların işlənilməsi qaydaları ilə bağlı deyil, həm də dövlətin rəqəmsal idarəetmə fəaliyyətində şəxsin ləyaqətinin və hüquqi muxtariyyətinin qorunması ilə bağlıdır [3]. Dövlət informasiya ehtiyatlarının qorunması təkcə dövlət marağının deyil, həm də vətəndaşın konstitusion hüquqlarının təminatıdır.

Konstitusiyanın 50-ci maddəsində təsbit olunan informasiya azadlığı da rəqəmsal dövlət təhlükəsizliyinin mühüm elementi kimi çıxış edir. İlk baxışdan informasiya təhlükəsizliyi ilə informasiya azadlığı arasında ziddiyyət görünə bilər. Lakin hüquqi dövlət modelində bu anlayışlar bir-birini inkar etmir. Əksinə, etibarlı, bütöv və təhlükəsiz dövlət informasiya ehtiyatları olmadan vətəndaşın doğru, aktual və qanuni informasiyaya çıxışı təmin edilə bilməz. Dövlət informasiya ehtiyatlarının mühafizəsi informasiya azadlığını məhdudlaşdıran deyil, onun keyfiyyətli həyata keçirilməsinə şərait yaradan hüquqi mexanizm kimi dəyərləndirilməlidir.

Konstitusiyanın 57-ci maddəsində müraciət etmək hüququ, 60-cı maddəsində isə hüquq və azadlıqların inzibati və məhkəmə qaydasında müdafiəsi təmin olunur. Elektron müraciətlər, elektron məhkəmə, elektron xidmətlər və inzibati reyestrlər bu hüquqların rəqəmsal formalarını yaradır. Əgər belə sistemlər kiberhücum, texniki nasazlıq, məlumat itkisi və ya qanunsuz müdaxilə nəticəsində işləmirsə, vətəndaşın müraciət etmək və müdafiə olunmaq hüququ faktiki olaraq məhdudlaşa bilər. Buna görə rəqəmsal dövlət təhlükəsizliyi hüquqi dövlət prinsipinin texniki-institusional təminatı kimi çıxış edir.

Kibersuverenlik prinsipi də məhz bu konstitusion müstəvidə formalaşır. Suverenlik yalnız fiziki ərazi üzərində ali hakimiyyət deyil, həm də dövlətin rəqəmsal məkanında hüquqi və texnoloji müstəqilliyin təminidir. Dövlət informasiya ehtiyatlarının harada saxlanılması, hansı platformalarda işlənilməsi, hansı standartlarla qorunması, hansı subyektlərin onlara çıxış əldə etməsi və hansı hallarda xarici texnoloji asılılıqların mümkün olması kibersuverenliyin əsas suallarıdır. Bu mənada kibersuverenlik dövlətin rəqəmsal resursları üzərində mütləq qapalı nəzarət ideyası deyil; o, milli təhlükəsizlik, insan hüquqları, beynəlxalq əməkdaşlıq və texnoloji inkişaf arasında hüquqi balans prinsipidir.

Dövlət informasiya ehtiyatlarının və sistemlərinin hüquqi rejimi

Azərbaycan hüququnda dövlət informasiya ehtiyatları və sistemləri rəqəmsal dövlət təhlükəsizliyinin əsas normativ obyektidir. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" qanun informasiya ehtiyatlarını münasibət obyekti kimi tanıyır və onların dövlət, hüquqi və fiziki şəxslər üçün hüquqi əhəmiyyətini müəyyənləşdirir [2]. Bu yanaşma dövlət informasiya ehtiyatlarını sadəcə texniki baza və ya proqram təminatı kimi deyil, hüquqi rejimi olan, mülkiyyət, idarəetmə, mühafizə, çıxış, inteqrasiya və məsuliyyət məsələləri ilə

bağlı xüsusi obyekt kimi qəbul etməyə imkan verir.

Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi qaydaları bu sahədə xüsusi əhəmiyyət daşıyır [10]. Həmin qaydalar dövlət informasiya sistemlərinin yaradılmasını və fəaliyyətini vahid idarəetmə məntiqinə tabe edir. Burada əsas məqsəd müxtəlif dövlət qurumlarının informasiya sistemlərinin paralel, təkrar və uyğunsuz şəkildə inkişaf etməsinin qarşısını almaq, məlumat mübadiləsini standartlaşdırmaq, dövlət reyestrlərinin hüquqi və texniki dayanıqlığını təmin etməkdir. Rəqəmsal dövlət təhlükəsizliyi baxımından bu qaydalar məlumatların itməsi, təkrar toplanması, qeyridəqiq inteqrasiya və hüquqi məsuliyyətin parçalanması risklərini azaltmağa xidmət edir.

"Dövlət informasiya ehtiyatlarının və sistemlərinin Nümunəvi Əsasnaməsi" dövlət informasiya ehtiyatlarının idarə olunmasında daha konkret institusional çərçivə yaradır [11]. Bu sənəd dövlət informasiya ehtiyatının məqsədini, strukturunu, istifadəçilərini, mühafizə tədbirlərini və sahiblik-idarəetmə mexanizmlərini müəyyən etmək üçün model rolunu oynayır. Nümunəvi Əsasnamənin əhəmiyyəti ondadır ki, hər bir dövlət informasiya sistemi ayrıca yaradılarkən onun hüquqi rejimi eyni məntiqə uyğun qurulmalıdır. Bu, rəqəmsal dövlət təhlükəsizliyində sistemlilik və hüquqi müəyyənlik yaradır.

Dövlət informasiya ehtiyatlarının vahid reyestrinin aparılması qaydaları da xüsusi əhəmiyyətə malikdir [12]. Dövlət hansı informasiya ehtiyatlarına və sistemlərinə malik olduğunu, onların harada yerləşdiyini, hansı məqsədlə işlədiyini, hansı qurum tərəfindən idarə olunduğunu və hansı texniki arxitekturaya malik olduğunu bilmədən real təhlükəsizlik siyasəti qura bilməz. Vahid reyestr yalnız inventarlaşdırma mexanizmi deyil, həm də kibersuverenliyin praktiki alətidir. Çünki suveren nəzarət ilk növbədə dövlətin öz rəqəmsal aktivlərini tanıması, onların hüquqi statusunu müəyyənləşdirməsi və risk səviyyəsini qiymətləndirməsi ilə başlayır.

Dövlət informasiya ehtiyatlarının və elektron xidmətlərin formalaşdırılması ilə bağlı yeni qaydalar dövlət informasiya sistemlərinin aktiv hissəsinin Hökumət buludu infrastrukturu ilə əlaqələndirilməsini də ön plana çıxarır [13]. Bu yanaşma dövlət məlumatlarının parçalanmış və nəzarətsiz texniki mühitlərdə deyil, daha standartlaşdırılmış, audit edilə bilən və təhlükəsizlik tələblərinə uyğun infrastrukturlarda saxlanılmasını hədəfləyir. Lakin bu model eyni zamanda daha yüksək məsuliyyət yaradır: mərkəzləşmə təhlükəsizliyi artıra bilər, amma böyük həcmli kiberhücumlar və sistemli nasazlıqlar zamanı riskin təsir dairəsini də genişləndirə bilər. Buna görə hüquqi tənzimləmə yalnız mərkəzləşdirmə deyil, ehtiyat nüsxələmə, dayanıqlılıq, insident planı, giriş səlahiyyətləri və müstəqil audit mexanizmləri ilə tamamlanmalıdır.

Elektron sənəd və elektron imza haqqında qanunvericilik dövlət informasiya ehtiyatlarında formalaşan sənədlərin hüquqi qüvvəsinin təminində mühüm rol oynayır [6]. Rəqəmsal dövlət təhlükəsizliyi yalnız məlumatın qorunmasını deyil, həm də elektron sənədin mənşəyinin, bütövlüyünün və hüquqi qüvvəsinin təsdiqini tələb edir. Elektron imza və elektron sənəd dövriyyəsi olmadan dövlət informasiya sistemlərində aparılan əməliyyatların sübutetmə dəyəri zəifləyər, hüquqi mübahisələrdə etimad problemi yaranar. Buna görə elektron imza institutu rəqəmsal dövlət təhlükəsizliyinin həm texniki, həm də prosessual təminatıdır.

Kritik informasiya infrastrukturu və kibertəhlükəsizlik rejimi

Kritik informasiya infrastrukturu rəqəmsal dövlət təhlükəsizliyinin ən həssas və strateji hissəsidir. Bu anlayış dövlət, cəmiyyət və iqtisadiyyat üçün həyati əhəmiyyət daşıyan informasiya sistemlərini, şəbəkələri və rəqəmsal

xidmətləri əhatə edir. Energetika, rabitə, nəqliyyat, bank-maliyyə sistemi, səhiyyə, dövlət idarəetməsi və müdafiə ilə bağlı informasiya infrastrukturları kiberhücum nəticəsində sıradan çıxarsa, zərər yalnız texniki və iqtisadi sahədə deyil, həm də milli təhlükəsizlik, ictimai sabitlik və insan hüquqları sahəsində özünü göstərə bilər. Bu səbəbdən kritik informasiya infrastrukturu adi informasiya sistemi kimi deyil, xüsusi təhlükəsizlik rejiminə malik dövlət əhəmiyyətli obyekt kimi tənzimlənməlidir.

Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları bu sahədə hüquqi mexanizmlərin əsasını təşkil edir [8]. Bu qaydalar ümumi idarəetmənin təşkili, təhlükəsizlik risklərinin idarə olunması, təhlükəsizlik siyasətinin formalaşdırılması, insidentlərin idarə edilməsi və təhlükəsizlik tələblərinə riayət olunması kimi məsələləri əhatə edir. Burada təhlükəsizlik statik vəziyyət kimi deyil, daimi idarəetmə prosesi kimi başa düşülür. Başqa sözlə, kritik informasiya infrastrukturu bir dəfə qorunub sonra nəzarətsiz buraxılan texniki sistem deyil; o, risklərin mütəmadi qiymətləndirilməsi, monitorinqi, audit və yenilənmə tələb edən canlı hüquqi-texniki sistemdir.

Kritik informasiya infrastrukturu obyektlərinin reyestri də mühüm hüquqi alətdir [9]. Reyestr mexanizmi olmadan hansı obyektlərin kritik hesab edildiyi, hansı subyektlərin daha yüksək təhlükəsizlik öhdəliyi daşıdığı və hansı sistemlərin xüsusi nəzarət rejiminə daxil olduğu aydın olmaz. Reyestr həm hüquqi müəyyənlik, həm də təhlükəsizlik idarəetməsi baxımından zəruridir. Lakin bu reyestrin özü də həssas məlumat mənbəyidir. Buna görə onun aparılması, çıxış səviyyələri, məlumatların açıqlanma dərəcəsi və istifadə qaydası ayrıca məxfilik və təhlükəsizlik standartları ilə qorunmalıdır.

"Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" bu sahədə normativ aktlar sistemini strateji səviyyədə tamamlayır [7]. Strategiya informasiya təhlükəsizliyi və kibertəhlükəsizliyi dövlətin dayanıqlı inkişafı, milli təhlükəsizliyi, rəqəmsal iqtisadiyyatın etibarlılığı və vətəndaşların hüquqlarının qorunması ilə əlaqələndirir. Onun əhəmiyyəti ondadır ki, kibertəhlükəsizliyi dar texniki mühafizə sahəsi kimi deyil, dövlət siyasətinin üfüqi istiqaməti kimi təqdim edir. Strategiyada risklərin idarə edilməsi, institusional koordinasiya, kadr potensialı, beynəlxalq əməkdaşlıq, kritik infrastrukturun qorunması və maarifləndirmə kimi elementlər bir-biri ilə əlaqəli şəkildə nəzərdə tutulur.

Kibertəhlükəsizlik rejiminin hüquqi mahiyyəti həm də məsuliyyət və nəzarət mexanizmlərinin mövcudluğundan asılıdır. İnformasiya təhlükəsizliyi tələbləri yalnız tövsiyə xarakterli olduqda onların icra gücü zəifləyir. Bu baxımdan kritik informasiya infrastrukturu subyektlərinin öhdəliklərinin, təhlükəsizlik risklərinin sənədləşdirilməsinin, insident barədə məlumatlandırmanın, müvafiq qurumların nəzarət səlahiyyətlərinin və pozuntu hallarında hüquqi nəticələrin aydın müəyyənləşdirilməsi zəruridir. Rəqəmsal dövlət təhlükəsizliyi sahəsində hüquqi boşluq texniki boşluğa çevrilir; texniki boşluq isə dövlət idarəçiliyinin zəif nöqtəsinə çevrilə bilər.

Kritik informasiya infrastrukturu ilə bağlı normativ rejim dövlət sirri və fərdi məlumatların qorunması rejimi ilə də uzlaşdırılmalıdır. Çünki bir sıra kritik sistemlər eyni zamanda dövlət sirri təşkil edən məlumatları, fərdi məlumatları və kommersiya əhəmiyyətli məlumatları emal edə bilər. "Dövlət sirri haqqında" qanun dövlət təhlükəsizliyi məqsədilə məlumatların dövlət sirrinə aid edilməsi, mühafizəsi və istifadəsi qaydalarını müəyyən edir [5]. Bu rejim rəqəmsal sistemlərdə tətbiq edilərkən məxfi məlumatların kriptoqrafik qorunması, giriş səlahiyyətlərinin

məhdudlaşdırılması, audit izləri, informasiya daşıyıcılarının idarə olunması və bulud infrastrukturunda yerləşdirmə kimi məsələlər ayrıca nəzərə alınmalıdır.

Hökumət buludu, EHİS və platforma əsaslı kibersuverenlik

Rəqəmsal dövlət təhlükəsizliyinin müasir mərhələsində dövlət informasiya sistemlərinin qorunması ayrı-ayrı serverlərin, lokal bazaların və qurumdaxili texniki tədbirlərin səviyyəsində həll edilə bilməz. Dövlət idarəetməsi platforma məntiqinə keçdikcə kibersuverenlik də platforma əsaslı xarakter alır. "Hökumət buludu"nun yaradılması və bulud xidmətlərinin göstərilməsi ilə bağlı tədbirlər dövlət informasiya sistemlərinin və ehtiyatlarının daha vahid, təhlükəsiz və idarə olunan infrastruktura keçirilməsini nəzərdə tutur [14]. Hökumət buludu modeli dövlət məlumatlarının saxlanılması, emalı və ehtiyat nüsxələrinin yaradılması sahəsində texniki mərkəzləşmə ilə hüquqi nəzarəti birləşdirir.

Hökumət buludu kibersuverenlik baxımından ikiqat əhəmiyyət daşıyır. Bir tərəfdən, o, dövlət qurumlarının müxtəlif xarici və ya zəif qorunan texniki mühitlərdən asılılığını azaldır, məlumatların milli yurisdiksiya daxilində və vahid təhlükəsizlik standartları əsasında saxlanılmasına imkan verir. Digər tərəfdən, Hökumət buludunda toplanan məlumat və xidmətlərin həcmi artdıqca bu infrastrukturun özü daha yüksək strateji risk obyektinə çevrilir. Buna görə Hökumət buludu yalnız texnoloji layihə deyil, xüsusi hüquqi rejimə, risk idarəetməsinə, fasiləsizlik planına, məlumatların bərpa mexanizminə və müstəqil təhlükəsizlik auditinə ehtiyacı olan milli rəqəmsal infrastruktur kimi qiymətləndirilməlidir.

Elektron Hökumət İnformasiya Sistemi haqqında Əsasnamə dövlət informasiya ehtiyatları arasında məlumat mübadiləsi və elektron xidmətlərin təşkili baxımından xüsusi yer tutur [15]. EHİS rəqəmsal dövlətin inteqrasiya qatıdır. Onun vasitəsilə dövlət qurumları arasında məlumatların sorğulanması, ötürülməsi və istifadə olunması daha sistemli formaya düşür. Bu sistem bir tərəfdən "once-only" prinsipinin, yəni vətəndaşdan eyni məlumatın təkrar tələb edilməməsi ideyasının həyata keçirilməsinə xidmət edir, digər tərəfdən isə dövlət informasiya ehtiyatları arasında hüquqi və texniki qarşılıqlı əlaqəni təmin edir.

EHİS-in təhlükəsizliyi rəqəmsal dövlət təhlükəsizliyinin mərkəzi məsələlərindən biridir. Çünki inteqrasiya qatında baş verən pozuntu təkcə bir dövlət sisteminə deyil, bir neçə informasiya ehtiyatına təsir göstərə bilər. Buna görə EHİS-də autentifikasiya, avtorizasiya, sorğu jurnalları, audit izləri, məlumatların məqsədəuyğun istifadəsi, çıxış səlahiyyətlərinin məhdudlaşdırılması və məlumatların emal məqsədi üzrə hüquqi nəzarət xüsusi əhəmiyyət daşıyır. EHİS vasitəsilə məlumat mübadiləsi hüquqi əsas, məqsəd və səlahiyyət olmadan aparılmamalıdır. Əks halda inteqrasiya səmərəliliyi fərdi məlumatların qanunsuz dövriyyəsi riskinə çevrilə bilər.

Platforma əsaslı kibersuverenlik anlayışı məhz Hökumət buludu, EHİS, vahid reyestrlər və dövlət informasiya ehtiyatlarının inteqrasiyası üzərində qurulur. Bu modeldə dövlət rəqəmsal məkanını qapalı və təcrid olunmuş sistem kimi deyil, standartlaşdırılmış, audit edilə bilən, hüquqi əsasla işləyən və təhlükəsizlik səviyyələri müəyyən edilmiş ekosistem kimi idarə edir. Kibersuverenlik burada yalnız "məlumat ölkə daxilində saxlanılmalıdır" tezisi ilə məhdudlaşmır. O, həm də məlumatın kim tərəfindən, hansı məqsədlə, hansı müddətdə, hansı hüquqi əsasla və hansı texniki təhlükəsizlik tələbləri daxilində emal olunmasını müəyyən edən normativ idarəetmə prinsipidir.

Azərbaycan Respublikasında Rəqəmsal İnkişaf Konsepsiyası bu baxımdan rəqəmsal dövlət təhlükəsizliyinin gələcək istiqamətlərini müəy-

yən edən mühüm strateji sənəddir [16]. Konsepsiya rəqəmsal transformasiyanı dövlət xidmətlərinin sadəcə elektronlaşdırılması kimi deyil, dövlət idarəetməsi, iqtisadiyyat və cəmiyyətin rəqəmsal mühitə uyğun yenilənməsi kimi təqdim edir. Bu yenilənmə kibertəhlükəsizlik tələbləri ilə müşayiət olunmadıqda rəqəmsal inkişaf özü yeni asılılıq və risk mənbəyinə çevrilə bilər. Buna görə Konsepsiyanın praktiki icrası dövlət informasiya ehtiyatlarının qorunması, Hökumət buludunun dayanıqlılığı, EHİS-in təhlükəsizliyi və kritik sistemlərin mühafizəsi ilə uzlaşdırılmalıdır.

Fərdi məlumatlar, dövlət sirri və informasiya azadlığı arasında balans

Rəqəmsal dövlət təhlükəsizliyinin ən çətin hüquqi məsələlərindən biri təhlükəsizlik, şəffaflıq və şəxsi həyatın qorunması arasında balansın təmin edilməsidir. Dövlət informasiya ehtiyatlarının qorunması adı altında bütün məlumatların qapalı rejimə keçirilməsi hüquqi dövlət prinsipi ilə uzlaşmaz. Eyni zamanda açıq məlumat siyasəti və elektron xidmətlərin genişləndirilməsi məxfi məlumatların, fərdi məlumatların və kritik infrastruktur məlumatlarının nəzarətsiz yayılmasına səbəb olmamalıdır. Buna görə hüquqi tənzimləmə "maksimum açıqlıq" və "maksimum məxfilik" arasında deyil, məlumatın hüquqi təbiətinə uyğun differensial rejim üzərində qurulmalıdır.

Fərdi məlumatların qorunması bu balansın birinci sütunudur. "Fərdi məlumatlar haqqında" Qanun fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi ilə bağlı münasibətləri tənzimləyir [3]. Dövlət informasiya sistemlərində fərdi məlumatların emalı qanuni məqsəd, zərurilik, proporsionallıq, təhlükəsizlik və məlumat subyektinin hüquqları prinsipləri ilə məhdudlaşdırılmalıdır. Dövlətin vətəndaş barədə məlumat toplamaq səlahiyyəti onun həmin məlumatdan istənilən məqsədlə istifadə etmək hüququ demək deyil. Məqsəd məhdudluğu, məlumatların minimumlaşdırılması və saxlanma müddətinin əsaslandırılması rəqəmsal dövlət təhlükəsizliyinin insan hüquqları ilə uzlaşması üçün vacibdir.

Fərdi məlumatların mühafizəsinə dair tələblər informasiya sistemləri qarşısında konkret təhlükəsizlik tələbləri müəyyən edir [4]. Bu tələblər göstərir ki, fərdi məlumatların qorunması yalnız hüquqi razılıq və ya prosedur məsələsi deyil, həm də texniki və təşkilati təhlükəsizlik məsələsidir. Dövlət informasiya sistemlərində istifadəçi identifikasiyası, giriş səlahiyyətlərinin bölüşdürülməsi, audit izlərinin aparılması, məlumatların icazəsiz dəyişdirilməsinin qarşısının alınması və təhlükəsizlik insidentlərinin idarə olunması fərdi məlumatların hüquqi müdafiəsinin real təminatıdır.

Dövlət sirri rejimi isə təhlükəsizlik balansının ikinci sütunudur. "Dövlət sirri haqqında" Qanun dövlət təhlükəsizliyinin təmin edilməsi məqsədilə məlumatların dövlət sirrinə aid edilməsi, mühafizəsi və istifadəsi qaydalarını müəyyən edir [5]. Rəqəmsal mühitdə dövlət sirrinin qorunması daha mürəkkəb xarakter alır. Əvvəllər məxfi sənəd əsasən fiziki daşıyıcıda qorunurdusa, indi məlumat elektron bazalarda, ehtiyat nüsxələrdə, şəbəkə trafikində, bulud mühitində və inteqrasiya kanallarında mövcud ola bilər. Buna görə məxfilik rejimi bütün məlumat həyat dövrünü əhatə etməlidir: yaradılma, saxlanma, ötürülmə, istifadə, arxivləşdirmə və məhv edilmə.

İnformasiya azadlığı balansın üçüncü sütunudur. Dövlət informasiya ehtiyatlarının qorunması və kibertəhlükəsizlik ictimai nəzarəti tam aradan qaldırmamalıdır. Açıq dövlət məlumatları, şəffaf elektron xidmətlər, dövlət qərarlarının əsaslandırılması və müraciətlərə cavab verilməsi rəqəmsal dövlətin legitimliyi üçün zəruridir. Lakin açıq məlumat siyasəti hazırlanarkən fərdi məlumatlar, dövlət sirri, kritik infrastruktur məlumatları və kommersiya sir-

ri ayrıca süzgəcdən keçirilməlidir. Hüquqi dövlət üçün əsas məsələ məlumatın gizlədilməsi deyil, onun hüquqi kateqoriyasının düzgün müəyyənləşdirilməsidir.

Bu balans kibersuverenlik prinsipinin də məzmununu müəyyən edir. Kibersuverenlik informasiya axınlarının tam qapadılması deyil. Əksinə, dövlətin informasiya axınlarını qanunilik, təhlükəsizlik və insan hüquqları əsasında idarə etmək qabiliyyətidir. Dövlət həm beynəlxalq məlumat mübadiləsində iştirak etməli, həm rəqəmsal iqtisadiyyatı inkişaf etdirməli, həm də kritik məlumatların xarici asılılıq, kiberhücum və hüquqsuz emal risklərindən qorunmasını təmin etməlidir. Beləliklə, kibersuverenlik rəqəmsal izolyasiya deyil, normativ nəzarət və hüquqi cavabdehlik prinsipidir.

Dövlət informasiya ehtiyatlarının qorunmasında institusional məsuliyyət və audit

Rəqəmsal dövlət təhlükəsizliyinin effektivliyi yalnız normativ aktların mövcudluğundan deyil, həmin aktların icrasını təmin edən institusional məsuliyyətdən asılıdır. Dövlət informasiya ehtiyatlarının sahibi, operatoru, istifadəçisi, texniki xidmət göstərən subyekti və nəzarət orqanı arasında səlahiyyət bölgüsü aydın olmadıqda təhlükəsizlik öhdəlikləri formal xarakter ala bilər. Bu səbəbdən hər bir dövlət informasiya sistemi üzrə hüquqi rejimdə məlumat sahibinin, sistem sahibinin, operatorun, administratorun, istifadəçinin və nəzarət subyektinin funksiyaları konkret göstərilməlidir.

Dövlət informasiya ehtiyatlarının və sistemlərinin texniki tələbləri bu sahədə mühüm rol oynayır [17]. Texniki tələblər hüquqi normanın tətbiq mexanizminə çevrilir. Qanun "mühafizə olunmalıdır" dedikdə, bu mühafizənin necə həyata keçiriləcəyi standartlar, arxitektura tələbləri, informasiya təhlükəsizliyi siyasəti, ehtiyat nüsxələmə, giriş səlahiyyətləri, protokollaşdırma və bərpa mexanizmləri vasitəsilə konkretləşdirilməlidir. Hüquqi tənzimləmə texniki standartlarla əlaqələndirilmədikdə norma ümumi bəyanat səviyyəsində qalır.

İnformasiya təhlükəsizliyi riskləri reyestrinin aparılması qaydası bu baxımdan mühüm yeni mərhələ kimi qiymətləndirilə bilər [18]. Risk reyestri təhlükəsizlik risklərinin təsadüfi və epizodik şəkildə deyil, sistemli və sənədləşdirilmiş qaydada idarə olunmasına imkan verir. Rəqəmsal dövlət təhlükəsizliyi risklərin tanınması, prioritetləşdirilməsi, məsul subyektin müəyyən edilməsi, riskin azaldılması tədbirlərinin izlənilməsi və nəticələrin qiymətləndirilməsi olmadan təmin edilə bilməz. Risk reyestri hüquqi məsuliyyət üçün də əhəmiyyətlidir: pozuntu baş verdikdə hansı riskin əvvəlcədən məlum olduğu, hansı tədbirin görülmədiyi və hansı subyektin öhdəliyini yerinə yetirmədiyi daha aydın müəyyən edilə bilər.

Audit rəqəmsal dövlət təhlükəsizliyinin ayrılmaz elementidir. Dövlət informasiya ehtiyatlarının qorunması yalnız daxili özünüyoxlama ilə məhdudlaşdırıldıqda obyektivlik zəifləyə bilər. Xüsusilə kritik informasiya infrastrukturu, Hökumət buludu, EHİS və böyük dövlət reyestrləri üzrə müntəzəm təhlükəsizlik auditi, uyğunluq yoxlaması və insident sonrası qiymətləndirmə mexanizmləri zəruridir. Audit təkcə texniki zəifliklərin aşkarlanması deyil, həm də hüquqi uyğunluğun, məlumat emalı məqsədlərinin və giriş səlahiyyətlərinin qanuniliyinin yoxlanılması deməkdir.

Dövlət orqanlarının internet informasiya ehtiyatlarının və elektron poçt ünvanlarının təhlükəsizliyi ilə bağlı tələblər rəqəmsal dövlətin "ön qapısı"nın qorunması baxımından vacibdir [19]. Vətəndaş dövlətlə çox vaxt rəsmi sayt, elektron xidmət və elektron poçt vasitəsilə təmas qurur. Bu resursların saxta versiyalarla əvəz edilməsi, ələ keçirilməsi, məlumat sızması və ya zərərli proqramlarla yoluxdurulması ictimai etimada ciddi zərbə vurur. Buna görə rəsmi domenlərin, elektron poçt sistemlərinin, SSL/TLS təhlükəsizliyinin,

identifikasiya mexanizmlərinin və məzmunun idarə olunmasının hüquqi-texniki qaydalarla qorunması rəqəmsal dövlət təhlükəsizliyinin ilkin səviyyəsidir.

Məsuliyyət mexanizmləri də ayrıca vurğulanmalıdır. Rəqəmsal dövlət təhlükəsizliyi pozulduqda zərər dövlətə, vətəndaşa, biznesə və ictimai marağa eyni anda toxuna bilər. Buna görə məsuliyyət yalnız intizam və ya inzibati xarakter daşımamalı, zərərin xarakterindən asılı olaraq mülki, inzibati, intizam və cinayət hüquqi nəticələrlə tamamlanmalıdır. Lakin məsuliyyətin effektivliyi üçün əvvəlcədən aydın öhdəliklər, sənədləşdirilmiş risklər, audit izləri və səlahiyyət bölgüsü olmalıdır. Əks halda kiberinsidentdən sonra "texniki nasazlıq" arqumenti hüquqi cavabdehliyi kölgədə qoya bilər.

Kibersuverenlik prinsipinin Azərbaycan modeli üçün perspektivləri

Azərbaycan Respublikasında kibersuverenlik prinsipinin inkişafı üçün mövcud normativ baza mühüm başlanğıc yaradır. Dövlət informasiya ehtiyatları və sistemləri haqqında qaydalar, Hökumət buludu, EHİS, kritik informasiya infrastrukturu rejimi, fərdi məlumatların qorunması və kibertəhlükəsizlik strategiyası vahid hüquqi ekosistemin ayrı-ayrı elementləri kimi çıxış edir. Lakin bu elementlərin gələcək mərhələdə daha aydın doktrinal çərçivəyə salınması vacibdir. Kibersuverenlik ayrıca hüquqi prinsip kimi ifadə olunmasa belə, onun məzmunu artıq normativ aktların müxtəlif hissələrində mövcuddur: dövlət məlumatlarının qorunması, milli infrastrukturda yerləşdirilməsi, kritik sistemlərin təhlükəsizliyi, informasiya resurslarının reyestrləşdirilməsi və dövlətin rəqəmsal riskləri idarə etmək səlahiyyəti.

Bu prinsipin inkişafı üçün birinci istiqamət məlumat suverenliyidir. Dövlət informasiya ehtiyatlarında formalaşan məlumatların hüquqi statusu, mülkiyyət rejimi, saxlanma yeri, xarici servis provayderləri ilə münasibəti və transsərhəd ötürülməsi məsələləri daha dəqiq tənzimlənməlidir. Xüsusilə bulud texnologiyalarının genişləndiyi şəraitdə dövlət məlumatlarının xarici yurisdiksiyalarda saxlanılması və ya xarici şirkətlərin texniki idarəetmə təsiri altında olması milli təhlükəsizlik və hüquqi yurisdiksiya baxımından risklər yarada bilər. Bu risklərin həlli qapalı rəqəmsal siyasət deyil, risk əsaslı yerləşdirmə və məlumat kateqoriyalaşdırılması ilə mümkündür.

İkinci istiqamət texnoloji suverenlikdir. Dövlət informasiya sistemləri yalnız proqram təminatı və avadanlıqdan ibarət deyil; onlar standartlar, API-lər, məlumat modelləri, identifikasiya mexanizmləri, şifrələmə vasitələri və audit protokolları üzərində qurulur. Xarici texnoloji asılılıq tam aradan qaldırıla bilməsə də, kritik sistemlər üzrə alternativlik, açıq standartlar, kod təhlükəsizliyi, yerli ekspertiza və təchizat zənciri risklərinin idarə olunması təmin edilməlidir. Texnoloji suverenlik bütün sistemlərin mütləq yerli istehsal olması deyil; kritik funksiyalar üzrə idarəetmə və nəzarət imkanının dövlətin əlində qalmasıdır.

Üçüncü istiqamət hüquqi suverenlikdir. Rəqəmsal dövlət mühitində məlumatların emalı, saxlanılması və ötürülməsi Azərbaycan Respublikasının qanunvericiliyinə, məhkəmə nəzarətinə və inzibati məsuliyyət mexanizmlərinə tabe olmalıdır. Xarici platformaların iştirakı hallarında müqavilə şərtləri, məlumatların yerləşdiyi yurisdiksiya, audit hüququ, insident barədə məlumatlandırma və dövlət məlumatlarının geri qaytarılması mexanizmləri əvvəlcədən müəyyən edilməlidir. Bu, kibersuverenliyin praktiki hüquqi təminatıdır.

Dördüncü istiqamət insan hüquqları yönümlü kibersuverenlikdir. Kibersuverenlik anlayışı bəzən təhlükəsizlik və nəzarət ritorikası ilə izah edilir. Lakin demokratik hüquqi dövlətdə bu prinsip vətəndaşın hüquqlarını məhdudlaşdırmaq üçün deyil, onun rəqəmsal mühitdə müdafiəsini

gücləndirmək üçün tətbiq olunmalıdır. Dövlət informasiya ehtiyatlarının qorunması fərdi məlumatların təhlükəsizliyini, elektron xidmətlərin etibarlılığını, hüquqi müdafiəyə çıxışı və məlumatların qanuni istifadəsini təmin etməlidir. Bu baxımdan kibersuverenlik hüquq və təhlükəsizlik arasında balanslaşdırıcı prinsip kimi başa düşülməlidir.

Beşinci istiqamət normativ inteqrasiyadır. Mövcud hüquqi bazanın ayrı-ayrı aktlar üzrə dağınıq olması praktikada tətbiq çətinlikləri yarada bilər. Gələcəkdə dövlət informasiya ehtiyatlarının qorunması, kritik informasiya infrastrukturu, Hökumət buludu, EHİS, fərdi məlumatlar, açıq məlumatlar və kiberinsidentlərin idarə olunması arasında əlaqəni daha aydın göstərən sistemləşdirilmiş hüquqi yanaşmaya ehtiyac vardır. Bu, ayrıca "rəqəmsal dövlət təhlükəsizliyi" konsepsiyası və ya mövcud normativ aktların əlaqələndirilmiş tətbiq mexanizmi formasında həyata keçirilə bilər.

Nəticə

Aparılmış təhlil göstərir ki, Azərbaycan Respublikasında rəqəmsal dövlət təhlükəsizliyinin hüquqi əsasları artıq çoxsəviyyəli normativ sistem şəklində formalaşmışdır. Bu sistemin konstitusion bazasını dövlət suverenliyi, insan hüquqlarının təmin edilməsi, şəxsi toxunulmazlıq, informasiya azadlığı, müraciət etmək və məhkəmə müdafiəsi hüquqları təşkil edir. Sahəvi normativ bazanı isə "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanun, "Fərdi məlumatlar haqqında" Qanun, "Dövlət sirri haqqında" Qanun, "Elektron imza və elektron sənəd haqqında" Qanun, kritik informasiya infrastrukturu təhlükəsizliyi qaydaları, dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması və aparılması qaydaları, Hökumət buludu, EHİS və kibertəhlükəsizlik strategiyası tamamlayır.

Dövlət informasiya ehtiyatlarının qorunması rəqəmsal dövlət təhlükəsizliyinin mərkəzi elementi kimi çıxış edir. Çünki dövlətin rəqəmsal idarəetmə qabiliyyəti məlumatların bütövlüyü, məxfiliyi, əlçatanlığı və hüquqi qüvvəsi üzərində qurulur. Dövlət reyestrləri, elektron xidmətlər, EHİS və Hökumət buludu yalnız texniki infrastruktur deyil, hüquqi dövlətin rəqəmsal fəaliyyət mühitidir. Bu sistemlərdə baş verən pozuntu vətəndaşın hüquqlarına, dövlət qərarlarının legitimliyinə və milli təhlükəsizliyə birbaşa təsir göstərir.

Kritik informasiya infrastrukturu ilə bağlı hüquqi rejim rəqəmsal təhlükəsizliyi daha yüksək strateji səviyyəyə qaldırır. Burada məqsəd yalnız ayrı-ayrı məlumatların qorunması deyil, dövlət və cəmiyyət üçün həyati əhəmiyyətli rəqəmsal xidmətlərin fasiləsizliyinin təmin edilməsidir. Bu səbəbdən risklərin idarə olunması, reyestrləşdirmə, audit, insidentlərə reaksiya, ehtiyat nüsxələmə və dayanıqlılıq planları hüquqi tənzimləmənin əsas komponentləri olmalıdır.

Kibersuverenlik prinsipi Azərbaycan hüquq sistemi üçün perspektivli nəzəri və praktik kateqoriyadır. Bu prinsip dövlətin rəqəmsal məkanında məlumat, infrastruktur, texnologiya və hüquqi yurisdiksiya üzərində effektiv və qanuni nəzarətini ifadə edir. Lakin kibersuverenlik rəqəmsal izolyasiya kimi deyil, milli təhlükəsizlik, insan hüquqları, açıq dövlət, beynəlxalq əməkdaşlıq və texnoloji inkişaf arasında balanslaşdırıcı prinsip kimi başa düşülməlidir. Azərbaycan üçün optimal model məlumatların kateqoriyalaşdırılması, kritik sistemlərin milli nəzarətdə saxlanılması, Hökumət buludunun təhlükəsiz inkişafı, EHİS-in audit edilə bilən inteqrasiyası və fərdi məlumatların konstitusion səviyyədə qorunması üzərində qurulmalıdır.

Gələcək mərhələdə dövlət informasiya ehtiyatlarının qorunması sahəsində normativ sistemin daha da təkmilləşdirilməsi üçün bir neçə istiqamət xüsusi əhəmiyyət daşıyır. Birincisi, dövlət informasiya sistemləri üzrə məsuliyyət bölgüsü daha dəqiq müəyyən edilməlidir. İkin-

cisi, kritik informasiya infrastrukturu üzrə risk əsaslı audit və insident hesabatlılığı gücləndirilməlidir. Üçüncüsü, Hökumət buludu və EHİS üzrə məlumatların yerləşdirilməsi, ehtiyat nüsxələnməsi, giriş səlahiyyətləri və audit izləri daha aydın hüquqi standartlara tabe edilməlidir. Dördüncüsü, fərdi məlumatların qorunması, dövlət sirri və informasiya azadlığı arasında balans praktik tətbiq mexanizmləri ilə təmin olunmalıdır. Beşincisi, kibersuverenlik prinsipi rəqəmsal inkişaf strategiyalarında və dövlət informasiya ehtiyatları haqqında normativ aktlarda daha açıq şəkildə ifadə edilməlidir.

Beləliklə, rəqəmsal dövlət təhlükəsizliyi Azərbaycan Respublikasında yeni hüquqi institut kimi formalaşmaqdadır. Bu institut klassik informasiya təhlükəsizliyi anlayışını aşaraq konstitusion hüquq, milli təhlükəsizlik, inzibati idarəetmə, fərdi məlumatların qorunması və platforma əsaslı dövlət idarəetməsini birləşdirir. Onun keyfiyyətli inkişafı rəqəmsal transformasiyanın hüquqi legitimliyini, elektron xidmətlərə ictimai etimadı və dövlətin kiberməkanda suveren idarəetmə qabiliyyətini təmin edən əsas şərtlərdən biridir.

İstifadə edilmiş ədəbiyyat siyahısı:

1. Azərbaycan Respublikasının Konstitusiyası // 12 noyabr 1995-ci ildə qəbul edilmişdir (26 sentyabr 2016-cı il tarixdə olan əlavə və dəyişikliklər). [Elektron resurs]/URL: http://www.e-qanun.az/framework/897

2. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu. [Elektron resurs]/URL: e-qanun.az/framework/3525.

3. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu. [Elektron resurs]/URL:e-qanun.az/framework/19675.

4. "Fərdi məlumatların mühafizəsinə dair Tələblər"in təsdiq edilməsi haqqında. [Elektron resurs]/URL: e-qanun.az-framework/20046.

5. "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu. [Elektron resurs]/URL: e-qanun.az, framework/5526.

6. "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu, e-qanun.az, framework/5916.

7. "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nın təsdiq edilməsi haqqında. [Elektron resurs]/URL: e-qanun.az/framework/55045.

8. "Azərbaycan Respublikasında kritik informasiya infrastrukturu təhlükəsizliyinin təmin edilməsi Qaydaları"nın təsdiq edilməsi haqqında. [Elektron resurs]/URL: e-qanun.az/framework/54651.

9. Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması Qaydası, [Elektron resurs]/URL: e-qanun.az/framework/54652.

10. Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları. [Elektron resurs]/URL: e-qanun.az/framework/40020.

11. Dövlət informasiya ehtiyatlarının və sistemlərinin Nümunəvi Əsasnaməsi. [Elektron resurs]/URL: e-qanun.az, framework/58058.

12. Dövlət informasiya ehtiyatlarının, sistemlərinin və elektron xidmətlərin vahid reyestrinin aparılması Qaydaları. [Elektron resurs]/URL: e-qanun.az, framework/60322.

13. Dövlət informasiya ehtiyatları və sistemləri, habelə elektron xidmətlərlə bağlı Qayda. [Elektron resurs]/URL: e-qanun.az/framework/59985.

14. "Hökumət buludu"nun (G-cloud) yaradılması və "bulud" xidmətlərinin göstərilməsi sahəsində tədbirlər haqqında. [Elektron resurs]/URL: e-qanun.az/framework/42560.

15. Elektron Hökumət İnformasiya Sistemi haqqında Əsasnamə. [Elektron resurs]/URL: e-qanun.az/framework/60355.

16. "Azərbaycan Respublikasında Rəqəmsal İnkişaf Konsepsiyası"nın təsdiq edilməsi haqqında. [Elektron resurs]/URL: e-qanun.az/framework/58765.

17. Dövlət informasiya ehtiyatlarının və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi ilə bağlı texniki tələblər. [Elektron resurs]/URL: e-qanun.az/framework/41290.

18. İnformasiya təhlükəsizliyi riskləri reyestrinin aparılma Qaydası. [Elektron resurs]/URL:e-qanun.az/framework/61107.

19. Azərbaycan Respublikası dövlət orqanlarının internet informasiya ehtiyatlarının və elektron poçt ünvanlarının təhlükəsizliyinin təmin edilməsi üzrə Tələblər. [Elektron resurs]/URL: e-qanun.az/framework/24256.

20. OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2015.

21. European Union Agency for Cybersecurity (ENISA), National Cybersecurity Strategies: Practical Guide on Development and Execution, 2016.

22. Council of Europe, Convention on Cybercrime, Budapest, 2001.

23. Kello, Lucas, The Virtual Weapon and International Order, Yale University Press, 2017.

24. Chander, Anupam; Le, Uyên P., "Data Nationalism", Emory Law Journal, Vol. 64, 2015.

25. Lessig, Lawrence, Code and Other Laws of Cyberspace, Basic Books, 1999.

Агамалиев Умман Ильгар оглу,
доктор философии по праву, член Коллегии адвокатов Азербайджанской Республики,
преподаватель юридического факультета Национальной авиационной академии,
докторант Национальной авиационной академии

ПРАВОВЫЕ ОСНОВЫ ЦИФРОВОЙ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ В АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКЕ И ПРИНЦИП КИБЕРСУВЕРЕНИТЕТА

РЕЗЮМЕ

В статье рассматриваются правовые основы цифровой государственной безопасности в Азербайджанской Республике и раскрывается содержание принципа киберсуверенитета. Обосновывается, что государственные информационные ресурсы, государственные информационные системы, критическая информационная инфраструктура, Правительственное облако и Электронная правительственная информационная система уже являются не вспомогательными техническими средствами, а ключевыми элементами функционирования современного государства.

Анализируются Конституция Азербайджанской Республики, законы об информации, информатизации и защите информации, о персональных данных, о государственной тайне, об электронной подписи и электронном документе, а также подзаконные акты, регулирующие формирование, ведение, интеграцию, регистрацию и защиту государственных информационных ресурсов. Особое внимание уделяется критической информационной инфраструктуре, управлению рисками, аудиту, реестровым механизмам и требованиям информационной безопасности.

В статье делается вывод, что киберсуверенитет не должен пониматься как цифровая изоляция. Он выражает способность государства законно и эффективно управлять данными, инфраструктурой, технологиями и юрисдикцией в цифровом пространстве, обеспечивая баланс между национальной безопасностью, правами человека, открытым государством и международным сотрудничеством.

Agamaliyev Umman Ilgar,
PhD in Law, member of the Bar Association of the Republic of Azerbaijan,
Lecturer, Law Department of the National Aviation Academy,
Doctoral Student, National Aviation Academy

LEGAL FOUNDATIONS OF DIGITAL STATE SECURITY IN THE REPUBLIC OF AZERBAIJAN AND THE PRINCIPLE OF CYBER SOVEREIGNTY

SUMMARY

The article examines the legal foundations of digital state security in the Republic of Azerbaijan and explains the legal meaning of the principle of cyber sovereignty. It argues that state information resources, state information systems, critical information infrastructure, the Government Cloud and the E-Government Information System are no longer merely technical tools; they have become core elements of modern public administration and state resilience.

The article analyzes the Constitution of the Republic of Azerbaijan, the legislation on information, informatization and information protection, personal data, state secrets, electronic signature and electronic documents, as well as subordinate normative acts governing the creation, operation, integration, registration and protection of state information resources. Special attention is paid to critical information infrastructure, risk management, audit, registry mechanisms and information security requirements.

The article concludes that cyber sovereignty should not be understood as digital isolation. Rather, it reflects the state's lawful and effective capacity to govern data, infrastructure, technologies and jurisdiction in cyberspace while balancing national security, human rights, open government and international cooperation.

Redaksiyaya daxilolma tarixi: 17.05.2026
Təkrar işlənməyə göndərilmə tarixi: göndərilməyib
Çapa qəbul olunma tarixi: 19.06.2026