Əhalinin Rəqəmsal Savadlılıq Səviyyəsinin Dövlətin Kibersuverenliyinə Təsirinin Araşdırılması və Təhlili

Rəsmiyyə Mahmudova
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rasmahmudova@gmail.com

***Xülasə*— Bu tədqiqat işində əhalinin rəqəmsal savadlılıq səviyyəsi ilə dövlətin kibersuverenliyi arasındakı qarşılıqlı əlaqə araşdırılır. Müasir dövrdə kibersuverenlik təkcə infrastrukturun qorunması deyil, həm də vətəndaşların kiber-məkandakı davranışlarından birbaşa asılıdır. Məqalədə rəqəmsal savadlılığın aşağı olmasının sosial mühəndislik hücumlarına, dezinformasiya kampaniyalarına və fərdi məlumatların sızmasına şərait yaradaraq dövlətin rəqəmsal sərhədlərini necə zəiflətdiyi analiz edilir. Tədqiqatın nəticələri göstərir ki, kiber-savadlı cəmiyyət dövlətin kiber-müdafiə sisteminin "insan layını" təşkil edərək milli təhlükəsizliyin ayrılmaz hissəsinə çevrilir. Sonda əhalinin rəqəmsal bacarıqlarının artırılması vasitəsilə milli kiberdayanıqlılığın gücləndirilməsi üçün strateji tövsiyələr verilir.**

Açar sözlər— rəqəmsal savadlılıq; kibersuverenlik; informasiya təhlükəsizliyi; rəqəmsal transformasiya; insan faktoru.

I. GİRİŞ

Müasir dövrdə rəqəmsal texnologiyaların sürətli inkişafı dövlətlərin idarəetmə mexanizmlərinə, iqtisadiyyatına və təhlükəsizlik sistemlərinə güclü təsir göstərir. İnformasiya-kommunikasiya texnologiyalarının geniş tətbiqi və rəqəmsal xidmətlərin artması cəmiyyətin bütün təbəqələrinin rəqəmsal mühitdə iştirakını zəruri edir. Bu prosesdə əhalinin rəqəmsal savadlılıq səviyyəsi yalnız fərdi istifadə imkanlarını deyil, həm də dövlətin rəqəmsal müstəqilliyini və kibersuverenliyini müəyyən edən əsas amillərdən birinə çevrilir.

Rəqəmsal savadlılıq insanların informasiya texnologiyalarından düzgün, təhlükəsiz və səmərəli istifadə bacarığını ifadə edir. Bu bacarıqların zəif olması kiberhücumlara qarşı həssaslığı artırır, dövlətin rəqəmsal infrastrukturlarının müdafiəsini çətinləşdirir və milli təhlükəsizlik üçün risklər yaradır. Digər tərəfdən, yüksək rəqəmsal savadlılıq səviyyəsi cəmiyyətin rəqəmsal transformasiyaya adaptasiyasını sürətləndirir, elektron hökumət xidmətlərinin effektivliyini artırır və dövlətin kibersuverenliyini möhkəmləndirir.

Kibersuverenlik anlayışı dövlətlərin öz rəqəmsal məkanını müstəqil şəkildə idarə etmək, milli maraqlarını qorumaq və xarici təsirlərə qarşı dayanıqlı olmaq qabiliyyətini əhatə edir. Bu baxımdan, əhalinin rəqəmsal savadlılıq səviyyəsi kibersuverenliyin təmin olunmasında strateji əhəmiyyət daşıyır. Rəqəmsal savadlılığın aşağı olması dövlətin informasiya mühitində asılılığını artırır, yüksək olması isə milli rəqəmsal müstəqilliyi gücləndirir.

Bu məqalədə əhalinin rəqəmsal savadlılıq səviyyəsinin dövlətin kibersuverenliyinə təsiri araşdırılır və təhlil olunur. Məqsəd rəqəmsal savadlılığın kibersuverenliyin formalaşmasında oynadığı rolu müəyyənləşdirmək, mövcud çağırışları və perspektivləri dəyərləndirməkdir. Tədqiqat nəticələri dövlət siyasətində rəqəmsal savadlılığın artırılmasının vacibliyini göstərməklə yanaşı, kibersuverenliyin möhkəmləndirilməsi üçün praktik tövsiyələr təqdim etməyi hədəfləyir.

II. ƏDƏBİYYAT İCMALI

Qeyd edilməlidir ki, müasir elmi ədəbiyyatda “kibersuverenlik” anlayışı çox vaxt “rəqəmsal suverenlik” (digital sovereignty) termini ilə paralel şəkildə işlədilir və hər iki anlayış dövlətin rəqəmsal mühitdəki müstəqil iradəsini ifadə edir. Bu baxımdan, rəqəmsal savadlılıq müasir dövrdə yalnız fərdi bacarıq deyil, həm də milli təhlükəsizlik və dövlət siyasətinin əsas komponentlərindən biri kimi qəbul olunur. Valalnd (2023) qeyd edir ki, rəqəmsal savadlılıq, kibertəhlükəsizlik və texnoloji suverenlik cəmiyyətin dayanıqlılığını və milli təhlükəsizliyi formalaşdıran üç sütundur [1] .

Digər tərəfdən, Floridi və həmkarlarının (2024) araşdırması göstərir ki, “rəqəmsal suverenlik” anlayışı hələ də formalaşma mərhələsindədir və müxtəlif dövlətlər bu konsepti fərqli şəkildə şərh edirlər. Müəlliflər milli rəqəmsal suverenliyin effektivliyini radikal dəyişikliklər fonunda qiymətləndirərək, rəqəmsal savadlılığın bu prosesdə strateji rol oynadığını vurğulayırlar [2].

Tədqiqat işində [3] rəqəmsal suverenlik modellərinin müxtəlifliyi və onların milli siyasətlərdə tətbiqi məsələləri araşdırılır. Bu işdə rəqəmsal savadlılığın dövlətlərin rəqəmsal müstəqilliyinə təsiri xüsusi olaraq qeyd olunur.

Digər tərəfdən, beynəlxalq hüquq və kibertəhlükəsizlik üzrə aparılan tədqiqatlar göstərir ki, rəqəmsal suverenlik yalnız texnoloji müstəqilliklə deyil, həm də qlobal idarəetmə mexanizmləri ilə sıx bağlıdır. Bu yanaşma dövlətlərin kiberməkanda öz suverenliyini qorumaq üçün rəqəmsal savadlılıq səviyyəsini artırmasının vacibliyini ön plana çıxarır [4].

OECD və Dünya Bankının hesabatları isə rəqəmsal bacarıqların iqtisadi inkişaf və sosial inteqrasiya üçün əsas şərtlərdən biri olduğunu göstərir. Bu hesabatlarda rəqəmsal savadlılıq səviyyəsinin yüksəldilməsinin dövlətlərin rəqəmsal

DOI: 10.25045/cyber.gov.2026.41

transformasiya və kibersuverenlik siyasətlərinə birbaşa təsir etdiyi vurğulanır [4,5].

Bu ədəbiyyat icmalı göstərir ki, rəqəmsal savadlılıq səviyyəsi yalnız fərdi istifadəçilərin təhlükəsizliyini deyil, həm də dövlətlərin rəqəmsal müstəqilliyini və kibersuverenliyini müəyyən edən əsas amildir. Mövcud ədəbiyyatda rəqəmsal suverenliyin nəzəri və texnoloji tərəfləri geniş işıqlandırılsa da, əhalinin fərdi təhlükəsizlik mədəniyyətinin dövlət suverenliyinin qorunmasındakı spesifik rolu hələ də sistemli təhlilə ehtiyac duyur.

III. METODOLOGIYA

Tədqiqat işində əhalinin rəqəmsal savadlılıq səviyyəsinin dövlətin kibersuverenliyinə təsirini qiymətləndirmək üçün kompleks sosial-texniki yanaşma tətbiq edilmişdir. Kibersuverenlik yalnız texnoloji infrastrukturun lokallaşdırılması deyil, həm də həmin mühitdə fəaliyyət göstərən fərdlərin davranış modelindən və kiber-gigiyena vərdişlərindən birbaşa asılıdır. Tədqiqat çərçivəsində kibersuverenlik; informasiya məkanına nəzarət, infrastrukturun qorunması, milli verilənlərin təhlükəsizliyi və müstəqil kibermüdafiə qabiliyyəti ilə yanaşı, sosial-intellektual kapital olan rəqəmsal savadlılıq komponenti üzrə sistemli şəkildə modelləşdirilir. Təhlillər göstərir ki, müasir kibertəhdidlər, xüsusilə sosial mühəndislik və hədəflənmiş phishing hücumları texniki zəifliklərdən daha çox "insan faktoru" üzərində qurulur. Bu müstəvidə rəqəmsal savadlılıq dövlətin kiber-müdafiə arxitekturasında həlledici element rolunu oynayır [6].

Metodologiyanın elmi bazasını Avropa Komissiyasının "Vətəndaşlar üçün rəqəmsal kompetensiyalar çərçivəsi" (DigComp) təşkil edir. Bu çərçivəyə əsasən, rəqəmsal savadlılıq; informasiya savadlılığı, kommunikasiya, təhlükəsizlik və problem həlli bacarıqlarını ehtiva edən strateji kompetensiyadır. Tədqiqat zamanı rəqəmsal savadlılığın aşağı olmasının doğurduğu risklər dörd əsas müstəvi üzrə təhlil edilmişdir:

1) Kibertəhlükəsizlik riskləri: Əhalinin kiber-gigiyena qaydalarına riayət etməməsi, fərdi məlumatların qorunması mexanizmlərini bilməməsi dövlətin ümumi təhlükəsizlik ekosistemini zəiflədir. Sosial mühəndislik metodları ilə həyata keçirilən hücumlar, identiklik oğurluğu və məlumat sızmaları məhz fərdin texnoloji biliklərinin zəif olmasından deyil, psixoloji və koqnitiv zəifliyindən (manipulyasiyaya meyllilik, diqqətsizlik və s.) istifadə edir. Floridi və həmkarları (2024) qeyd edir ki, rəqəmsal suverenlik vətəndaşın öz məlumatları üzərindəki nəzarəti ilə başlayır; bu nəzarətin itirilməsi milli data suverenliyinə birbaşa təhdiddir [7].

2) İqtisadi və əmək bazarı riskləri: Rəqəmsal bacarıqların çatışmazlığı innovativ texnologiyaların (süni intellekt, bulud texnologiyaları) iqtisadiyyata inteqrasiyasını ləngidir. Bu, təkcə fərdin gəlir səviyyəsinə deyil, həm də dövlətin rəqəmsal iqtisadi müstəqilliyinə təsir edir. OECD hesabatlarına görə, rəqəmsal savadlılığın aşağı olduğu cəmiyyətlərdə xarici texnoloji asılılıq artır və daxili innovasiya potensialı bloklanır [9]. Adaptasiya çətinliyi dövlətin qlobal rəqəmsal zəncirdəki mövqeyini zəiflədir.

3) İnformasiya təhlükəsizliyi riskləri: Kritik təfəkkürün və rəqəmsal məzmunu analiz etmək qabiliyyətinin zəifliyi fonunda dezinformasiya və manipulyativ kontent daha sürətlə yayılır. Bu, dövlətin daxili sabitliyinə qarşı yönəlmiş "hibrid müharibə" elementidir. Kibersuverenlik kontekstində informasiya mühitinin təmizliyi vətəndaşın informasiyanı süzgəcdən keçirmə bacarığından asılıdır. Valalnd (2023) vurğulayır ki, texnoloji suverenlik yalnız infrastrukturla deyil, həm də cəmiyyətin informasiya dayanıqlılığı ilə ölçülməlidir [1]. Sosial inklüzivlik riskləri: E-xidmət baryerləri nəticəsində yaranan rəqəmsal bərabərsizlik.

4) Sosial inklüzivlik və rəqəmsal bərabərsizlik riskləri: Əhalinin rəqəmsal savadlılıq səviyyəsinin aşağı olması cəmiyyətdə "rəqəmsal uçurum"u dərinləşdirir. E-dövlət xidmətlərindən istifadə edə bilməyən vətəndaş qruplarının yaranması sosial narazılığa və dövlət-vətəndaş kommunikasiyasının qırılmasına səbəb olur. Bu bərabərsizlik kənar qüvvələrin daxili sosial manipulyasiyalar aparması üçün münbit şərait yaradır ki, bu da dolayısı ilə dövlətin siyasi suverenliyinə təsir göstərir [5].

Rəqəmsal savadlılıq dövlətin kibersuverenlik arxitekturasında təkcə "bilik" deyil, həm də 'Kollektiv Kiber-İmmunitet' funksiyasını yerinə yetirir. DigComp 2.2 çərçivəsində təsnif edilən 'Təhlükəsizlik' üzrə kompetensiyalar - yəni cihazların qorunması, fərdi məlumatların və məxfiliyin mühafizəsi, sağlamlığın və rifahın qorunması - birbaşa olaraq milli data suverenliyinə xidmət edir [10]. Fərdin kibergigiyena vərdişləri (məsələn, çoxfaktorlu autentifikasiyadan istifadə, deepfake məzmunların tanınması) dövlətin kritik informasiya infrastrukturuna sızma ehtimalını azaldır. Bu yanaşma, kibertəhlükəsizliyi mərkəzləşdirilmiş texniki müdafiədən, mərkəzsizləşdirilmiş və hər bir vətəndaşın aktiv iştirakçı olduğu dayanıqlı ekosistemə çevirir [11]. Beləliklə, fərdi səviyyədə rəqəmsal bacarıqların inkişafı dövlətin hibrid təhdidlərə qarşı koqnitiv müdafiə qabiliyyətini formalaşdırır [12].

IV. AZƏRBAYCANIN RƏQƏMSAL EKOSİSTEMİ VƏ KİBER-TƏHDİDLƏRİN ANALİZİ

Azərbaycanın rəqəmsal mənzərəsinin təhlili göstərir ki, texnoloji infrastrukturun sürətli inkişafı və internetə əlçatanlığın yüksək səviyyədə olması eyni zamanda kiber-risk amillərini də mütənasib şəkildə artırır. Bu bölmədə ölkənin rəqəmsal ekosistemi və əhalinin davranış modelinin kibersuverenliyə təsiri üç əsas istiqamət üzrə analiz edilir:

1) Rəqəmsal nüfuz və istifadə trendləri: 2024-cü ilin statistik göstəricilərinə əsasən, Azərbaycanda internet istifadəçilərinin sayı 9,27 milyon nəfərə (əhalinin 89%-i)

çatmışdır. Sosial media istifadəçilərinin sayının 7,61 milyon təşkil etməsi [7] ölkə əhalisinin böyük hissəsinin qlobal informasiya platformalarında aktiv olduğunu göstərir. Bu geniş miqyaslı rəqəmsallaşma dövlətin rəqəmsal sərhədlərinin hər bir fərdin cihazına qədər genişlənməsi deməkdir. Lakin rəqəmsal savadlılıq bu kəmiyyət artımı ilə paralel inkişaf etmədikdə, hər bir cihaz milli kiberməkanda potensial "zəif nöqtə"yə çevrilir.

2) Kiber-cinayətlərin strukturu və "insan faktoru": Azərbaycanda qeydə alınan kibercinayətlərin keyfiyyət analizi göstərir ki, insidentlərin 60-70%-i birbaşa bank kartı məlumatlarının və fərdi identiklik informasiyasının oğurlanması ilə bağlıdır. Maraqlıdır ki, bu cinayətlərin böyük əksəriyyəti mürəkkəb proqram sındırma metodları ilə deyil, rəqəmsal savadlılığı və kritik təfəkkürü aşağı olan vətəndaşlara qarşı tətbiq edilən sosial mühəndislik (phishing, vishing) üsulları ilə həyata keçirilir. Bu, dövlətin kiber-müdafiə arxitekturasında ən zəif həlqənin texniki sistemlər deyil, məhz "insan layı" olduğunu təsdiqləyir.

3) Milli data suverenliyinə təhdidlər: Azərbaycanın rəqəmsal məkanında fərdi məlumatların qorunması məsələsi milli təhlükəsizliyin strateji elementinə çevrilmişdir. Elektron Təhlükəsizlik Xidmətinin (ETX) 2025-ci il üzrə hesabatlarına əsasən, həyata keçirilən qabaqlayıcı monitorinq tədbirləri nəticəsində 3 milyondan artıq vətəndaşa aid fərdi məlumatın mümkün sızma hallarının və "Dark Web" platformalarında qanunsuz dövriyyəsinin qarşısı alınmışdır [9]. Bu miqyasda bir sızma ehtimalı fərdi kiber-gigiyena mədəniyyətinin aşağı olmasının toplu şəkildə dövlətin data suverenliyinin aşınmasına necə zəmin yaratdığını nümayiş etdirir. Vətəndaşların fərdi məlumatlarının (identiklik məlumatları, biometrik data, maliyyə rekvizitləri) kütləvi şəkildə xarici platformaların və ya bədniyyətli aktorların əlinə keçməsi, dövlətin rəqəmsal resursları üzərindəki nəzarətini zəiflədir və milli kiber-məkanın xarici təsirlərə qarşı həssaslığını artırır. Beləliklə, fərdi səviyyədəki informasiya təhlükəsizliyi boşluqları milli rəqəmsal ekosistemin bütövlüyünü pozaraq xarici aktorlar üçün dövlətin strateji resurslarına sızma imkanı yaradan "zəif həlqə" rolunu oynayır.

V. ƏHALİNİN RƏQƏMSAL SAVADLILIĞININ KİBERSUVERENLİYƏ TƏSİR MEXANİZMLƏRİ

Müasir elmi yanaşmalara əsasən, kibersuverenlik yalnız dövlətin texnoloji imkanları ilə deyil, həm də cəmiyyətin rəqəmsal kompetensiyaları ilə formalaşır. Bu təsir mexanizmi iki əsas istiqamətdə təzahür edir:

1. Sosial-funksional təsir: İnformasiya suverenliyi və kognitiv müdafiə. Bu səviyyədə rəqəmsal savadlılıq milli kiberməkanda təhlükəsizlik mühiti və "kollektiv immunitet" yaradır. [12]-də qeyd olunduğu kimi, dezinformasiya və manipulyasiya tənqidi düşüncə çatışmazlığından qidalanır. Odur ki, vətəndaşların informasiyanın mənşəyini analiz edə bilməsi informasiya sabitliyini təmin edir və xarici informasiya təsirlərinə qarşı qeyri-institusional müdafiə mexanizmi formalaşdırır. Nəticədə, cəmiyyətin rəqəmsal dəyişikliklərə çevik adaptasiyası böhran vəziyyətlərində dövlətin strateji dayanıqlılığını möhkəmləndirir.

2. İnstitusional təsir: Elektron dövlət və kollektiv kibermüdafiə. Dövlətin rəqəmsal transformasiyası və e-hökumət platformalarının təhlükəsizliyi əhəmiyyətli dərəcədə istifadəçi davranışlarından asılıdır. Aparılan araşdırmalar sübut edir ki, kiber-insidentlərin əksəriyyəti məhz insan faktoru ilə bağlıdır [13]. Rəqəmsal savadlılıq dövlət sistemlərinin insan-təhlükəsizlik interfeysini gücləndirərək vətəndaşı passiv istifadəçidən aktiv kibertəhlükəsizlik subyektinə çevirir. Bu, [14]-də irəli sürülən "kollektiv kibermüdafiə" modelinin reallaşmasına imkan yaradır və dövlətin müdafiə resurslarının daha effektiv istifadəsini təmin edir.

NƏTİCƏ VƏ TƏKLİFLƏR

Aparılan tədqiqat göstərir ki, müasir şəraitdə kibersuverenlik yalnız texnoloji və hüquqi infrastrukturun qorunması deyil, həm də vətəndaşların kiber-məkanındakı davranışlarından birbaşa asılı olan dinamik bir prosesdir. Əhalinin rəqəmsal savadlılıq səviyyəsi dövlətin kiber-müdafiə sisteminin "insan layını" təşkil edərək milli təhlükəsizliyin ayrılmaz hissəsinə çevrilir. Tədqiqatın nəticələri və slaydlarda təqdim olunan prioritetlər əsasında aşağıdakı strateji tövsiyələr irəli sürülür:

Rəqəmsal savadlılığın milli strategiyalara inteqrasiyası. Rəqəmsal savadlılıq sadəcə fərdi bacarıq deyil, milli təhlükəsizlik resursu kimi qəbul edilməlidir. Bu istiqamət milli kibertəhlükəsizlik və informasiya təhlükəsizliyi strategiyalarına sistemli şəkildə inteqrasiya edilməli, insan faktoru ilə bağlı risklər (sosial mühəndislik, manipulyasiya) ayrıca prioritet kimi nəzərə alınmalıdır.

Təhsil kurikulumlarının müasirləşdirilməsi**.** Orta məktəb səviyyəsindən başlayaraq ali təhsilə qədər bütün mərhələlərdə rəqəmsal təhlükəsizlik, media savadlılığı və tənqidi təfəkkür bacarıqları icbari kompetensiya kimi tədris proqramlarına daxil edilməlidir. Bu, cəmiyyətdə "kollektiv immunitetin" bünövrəsini təşkil edir.

Dövlət-özəl-akademiya əməkdaşlığı. Kibertəhlükəsizlik sahəsində dövlət qurumları, özəl sektor və akademik institutlar arasında əməkdaşlıq genişləndirilməlidir. Bu üçtərəfli sinerji həm innovativ texnoloji həllərin tətbiqinə, həm də cəmiyyətin maarifləndirilməsi üçün effektiv platformaların yaradılmasına imkan verir.

Kiber-risk modellərinin təkmilləşdirilməsi. Milli səviyyədə tətbiq olunan kibertəhlükəsizlik risk modellərində yalnız texniki komponentlər (firewall, şifrələmə) deyil, həm də sosial davranış modelləri və əhalinin rəqəmsal savadlılıq indeksləri mütləq şəkildə nəzərə alınmalıdır.

Yekun olaraq onu qeyd etmək lazımdır ki, rəqəmsal

savadlılığın artırılması dövlətin rəqəmsal müstəqilliyini gücləndirir, e-hökumət xidmətlərinin effektivliyini artırır və daxili informasiya mühitini xarici müdaxilələrdən qoruyur. İnsan faktoruna yatırılan hər bir rəqəmsal investisiya dövlətin kibersuverenliyinin uzunmüddətli davamlılığının əsas zəmanətidir.

Xüsusilə, 27 fevral 2026-cı il tarixində qəbul olunmuş Azərbaycan Respublikası Prezidentinin müvafiq Sərəncamı [8] rəqəmsal mühitdə təhlükəsiz davranışın təşviqini prioritet istiqamət kimi müəyyən etməklə, bu təsir mexanizminin dövlət idarəçiliyindəki strateji yerini təsdiq etmişdir. Beləliklə, əhalinin fərdi informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi dövlətin rəqəmsal sərhədlərinin qorunmasında həm preventiv müdafiə mexanizmi, həm də kollektiv kibermüdafiənin əsas hərəkətverici qüvvəsi kimi çıxış edir. Bu yanaşma, milli kiber-məkanı xarici aktorlar üçün əlçatan olan "zəif həlqələrdən" təmizləyərək, rəqəmsal ekosistemin bütövlüyünü və dövlətin data suverenliyini təmin edir [9].

ƏDƏBİYYAT

[1] B. Valalnd, “Digital Literacy, Cybersecurity, and Technological Sovereignty: A Societal Perspective,” Int. J. Novel Research and Development, vol. 8, no. 2, pp. 145–162, 2023.

[2] S. Fratini, E. Hine, C. Novelli, H. Roberts, and L. Floridi, “Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models,” Digital Society, vol. 3, article 59, Springer Nature, 2024.

[3] “Digital sovereignty in an era of cyber threats and global connectivity,” Academic Literature Review on International Law and Cybersecurity, 2024.

[4] OECD, Skills for a Digital World, OECD Publishing, Paris, 2022.

[5] World Bank, Digital Skills for Development: Policy Report, Washington, DC, 2023.

[6] ENISA, “Cybersecurity Skills Development in the EU,” ENISA Reports, 2023.

[7] Datareportal, “Digital 2024: Azerbaijan,” Global Digital Insights, Feb. 2024.

[8] “Azərbaycan Respublikasında rəqəmsal inkişafın sürətləndirilməsinə dair 2026−2028-ci illər üçün Fəaliyyət Planı”, 27 fevral 2026-cı il

[9] Elektron Təhlükəsizlik Xidməti, “ETX: Ötən il ərzində 3 milyondan artıq vətəndaşa aid fərdi məlumatların mümkün sızma hallarının qarşısı alınıb,” cert.az, 28 Yanvar 2026. https://cert.az/news/2026/etx-ferdi-melumatlarin-muhafizesi-gunu

[10] R. Mahmudova, “Issues of development of digital competencies of specialists for Industry 4.0,” Information Society, vol. 15, no. 1, pp. 32-41, 2024.

[11] European Commission, DigComp 2.2: The Digital Competence Framework for Citizens, Publications Office of the European Union, Luxembourg, 2022.

[12] S. Wardle and H. Derakhshan, “Information Disorder: Toward an interdisciplinary framework for research and policymaking,” Council of Europe Report, 2017.

[13] L. Hadlington, "Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," Heliyon, vol. 3, no. 7, art. no. e00346, Jul. 2017, doi: 10.1016/j.heliyon.2017.e00346.

[14] R. von Solms and J. van Niekerk, "From information security to cyber security," Computers & Security, vol. 38, pp. 97–102, 2013, doi:10.1016/j.cose.2013.04.004.

Analysis and Assessment of the Impact of Population's Digital Literacy Level on State Cyber Sovereignty

Rasmiyya Mahmudova

Institute of Information Technology, Baku, Azerbaijan

Abstract– This study explores the critical correlation between the population's digital literacy level and the maintenance of state cyber sovereignty. In the contemporary digital era, cyber sovereignty is not merely a matter of infrastructure protection but is increasingly dependent on the digital behavior and cyber-hygiene of citizens. The article analyzes how deficiencies in digital literacy create vulnerabilities to social engineering attacks, disinformation campaigns, and data breaches, thereby undermining a nation’s digital borders. Utilizing a socio-technical approach, the research evaluates digital literacy as a strategic component of national security. The findings suggest that a digitally literate society acts as the "human layer" of a state's cyber defense, enhancing institutional resilience and collective security. The study concludes with strategic recommendations for integrating digital literacy into national security policies and educational frameworks to strengthen national cyber resilience.

Keywords– Digital literacy, cyber sovereignty, national security, human factor, cyber resilience, digital divide, Azerbaijan digital ecosystem.