Sosial Təyinatlı Kiberfiziki Sistemlərdə Fərdi Məlumatların Transsərhəd Ötürülməsi Risklərinin Çoxmeyarlı Qiymətləndirilməsi

Araz Mustafa
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
araz.mmustafa@gmail.com

***Xülasə*— Tədqiqat işində sosial təyinatlı kiberfiziki sistemlərdə toplanan fərdi məlumatların ötürülməsi zamanı yaranan risklərin qiymətləndirilməsi üçün çoxmeyarlı yanaşma təklif edilir. Baxılan yanaşmada texnoloji boşluqlarla yanaşı, sosial mühit, insan amili, hüquqi tənzimləmə səviyyəsi və milli rəqəmsal infrastrukturun dayanıqlılığı kimi prioritetləşdirilməsi faktorlar da məqsədilə nəzərə alınır. Risklərin müasir qərarqəbuletmə metodlarından istifadə edilərək zəifliklərin müəyyənləşdirilməsi və onların kibersuverenliyə potensial təsirinin qiymətləndirilməsi üçün yanaşma təklif olunur. Əldə olunan nəticələr sosial təyinatlı kiberfiziki sistemlərdə fərdi məlumatların konfidensiallığının qorunması ilə yanaşı, milli rəqəmsal mühitdə idarəetmə və nəzarət mexanizmlərinin gücləndirilməsinə, eləcə də kibersuverenliyin təmin edilməsinə xidmət edir.**

Açar sözlər*— *Sosial təyinatlı kiberfiziki sistemlər; kibersuverenlik; fərdi məlumatların təhlükəsizliyi; risklərin qiymətləndirilməsi; çoxmeyarlı qiymətləndirmə; məlumatların ötürülməsi.

I. GİRİŞ

Müasir informasiya cəmiyyəti şəraitində rəqəmsallaşma dövlətin bir sıra sahələrində səhiyyədə, təhsildə, şəhər infrastrukturunda və s. kiberfiziki sistemlərin geniş tətbiqinə gətirib çıxarmışdır [1]. Bildiyimiz kimi, kiberfiziki sistemlər fiziki (KFS) proseslərin hesablama və kommunikasiya mühitləri ilə inteqrasiyasına əsaslanır və real vaxt rejimində məlumat mübadiləsini təmin edir [2]. Sosial təyinatlı kiberfiziki sistemlər (STKFS) isə fərdlərin fiziki, rəqəmsal və sosial mühitləri ilə birgə qarşılıqlı əlaqəsinə əsaslanır. STKFS-lərdə insan fəaliyyətinin müxtəlif sahələrindən böyük həcmdə fərdi məlumatlar toplanır və emal edilir. Bu məlumatların əhəmiyyətli hissəsi qlobal şəbəkə infrastrukturları vasitəsilə ölkə sərhədlərindən kənara ötürülür ki, bu da informasiya təhlükəsizliyi və dövlətin kibersuverenliyi baxımından müxtəlif risklər yaradır [3]. Tədqiqat işində sosial təyinatlı kiberfiziki sistemlərdə fərdi məlumatların transsərhəd ötürülməsi zamanı yaranan risklər təhlil olunur və onların qiymətləndirilməsi üçün çoxmeyarlı qərarvermə metodlarından istifadə imkanları araşdırılır. Təklif edilən yanaşma nəticələr sosial təyinatlı kiberfiziki sistemlərdə fərdi məlumatların konfidensiallığının qorunması ilə yanaşı, milli rəqəmsal mühitdə idarəetmə və nəzarət mexanizmlərinin gücləndirilməsinə, eləcə də kibersuverenliyin təmin edilməsinə xidmət edir.

II. SOSİAL TƏYİNATI KİBERFİZİKİ SİSTEMLƏR VƏ ONLARDA TOPLANAN FƏRDİ MƏLUMATLAR

STKFS-lər vətəndaşların fərdi məlumatlarının emalı ilə xarakterizə olunur. Bu sistemlərdə sensor şəbəkələri, mobil tətbiqlər, identifikasiya mexanizmləri, bulud hesablama platformaları və s. sinxron şəkildə fəaliyyət göstərir, real vaxt rejimində böyük həcmli fərdi məlumatların toplanmasını və emalını təmin edir. Bulud platformalarının yayılması ilə məlumatların saxlanması və emalı çox zaman digər ölkələrin serverlərində həyata keçirilir [4].

STKFS-lərin əsas xüsusiyyəti ondan ibarətdir ki, burada informasiya axınları yalnız texnoloji infrastrukturla məhdudlaşmır, eyni zamanda hüquqi, sosial və institusional mühitlə sıx bağlı olur. Müxtəlif sistemlərdə vətəndaşın biometrik məlumatları, sosial status göstəriciləri müxtəlif dövlət qurumları və bəzən beynəlxalq xidmət provayderləri arasında paylaşılır. Eyni şəkildə, qlobal rəqəmsal platformalarda pasiyent məlumatları diaqnostik analiz, süni intellekt əsaslı tibbi modelləşdirmə və məqsədlərlə müxtəlif ölkələrdə yerləşən serverlərdə saxlanıla və emal oluna bilər [5]. Bu proseslərin böyük hissəsi bulud texnologiyalarına əsaslandığından məlumatların fiziki yerləşmə yeri ilə hüquqi tənzimləmə zonası arasında fərq yaranır və nəticədə transsərhəd məlumat ötürülməsi baş verir. Transsərhəd ötürülmə yalnız texniki məsələ deyil, eyni zamanda hüquqi suverenlik, məlumatların mülkiyyəti və insan hüquqları ilə bağlı mürəkkəb məsələlər ortaya qoyur. Məlumatların bir dövlətin hüdudlarından kənara ötürülməsi həmin məlumatların fərqli normativ çərçivələrə tabe olması deməkdir. Bu da öz növbəsində məxfilik səviyyəsinin, nəzarət mexanizmlərinin və məsuliyyət bölgüsünün dəyişməsi ilə nəticələnə bilər. Xüsusilə müxtəlif ölkələrdə fərdi məlumatların qorunması üzrə standartların qeyri-bərabər inkişaf səviyyəsi hüquqi risklərin artmasına səbəb olur [6].

Bu kontekstdə beynəlxalq standartlarda informasiya təhlükəsizliyi risklərinin sistemli şəkildə müəyyənləşdirilməsi və idarə olunması üçün metodoloji baza mövcuddur. Lakin bu standart əsasən texniki zəifliklərin, təhlükə mənbələrinin və hərəkətlərin təsnifatına yönəlmişdir.

STKFS-lərdə toplanan fərdi məlumatların spesifik

DOI: 10.25045/cyber.gov.2026.09

xüsusiyyəti isə ondan ibarətdir ki, burada risk yalnız texniki zəiflikdən qaynaqlanmır. Məsələn, məlumatların geopolitik baxımdan gərgin regionlarda yerləşən serverlərdə saxlanılması, sanksiya rejimlərinin tətbiqi, beynəlxalq hüquqi mübahisələr və ya dövlətlərarası məlumat mübadiləsinə dair məhdudiyyətlər sistemin dayanıqlılığına birbaşa təsir göstərə bilər.

Yuxarıda da qeyd olunduğu kimi, STKFS-lərdə müxtəlif növ fərdi məlumatlar toplanır ki, onları da aşağıdakı kateqoriyalara bölmək mümkündür [7]:

- şəxsi identifikasiya məlumatları
- geolokasiya məlumatları
- davranış və fəaliyyət məlumatları
- biometrik məlumatlar
- sosial xidmətlərdən istifadə göstəriciləri.

Bu məlumatlar əsasən sensor cihazları, mobil qurğular və müxtəlif informasiya sistemləri vasitəsilə əldə edilir.

III. FƏRDİ MƏLUMATLARIN TRANSSƏRHƏD ÖTÜRÜLMƏSİ RİSKLƏRİ

Müasir informasiya mühitində fərdi məlumatların beynəlxalq şəbəkələr vasitəsilə ötürülməsi, rəqəmsal transformasiyanın vacib tərkib hissəsidir. Lakin belə proseslər məlumat subyektlərinin məxfiliyinin qorunması, məlumatlara icazəsiz müdaxilənin qarşısının alınması və dövlətlərin milli informasiya təhlükəsizliyinin təmin edilməsi baxımından bir sıra ciddi çağırışlar yaradır. İnformasiya axınlarının sərhədləri aşaraq müxtəlif hüquqi rejimlərə malik ölkələr arasında dövriyyəyə daxil olması, məlumatların qorunması üzrə vahid mexanizmlərin formalaşdırılmasını daha da çətinləşdirir [8].

Fərdi məlumatların beynəlxalq şəbəkələr vasitəsilə ötürülməsi müxtəlif təhlükəsizlik riskləri yaradır. Bu risklər əsasən aşağıdakı istiqamətlərdə özünü göstərir:

- məlumatların icazəsiz əldə olunması
- məlumatların dəyişdirilməsi və ya saxtalaşdırılması
- məlumatların üçüncü tərəflərə ötürülməsi
- milli informasiya suverenliyinin zəifləməsi.

Məlumatların icazəsiz əldə olunması – belə ki, fərdi məlumatların ötürülməsi zamanı ötürülmə kanallarının və server mühitlərinin yetərincə qorunmaması nəticəsində kənar şəxslər tərəfindən məlumatların ələ keçirilməsi riski artır. Bu hal kibercinayətkarlıq, sosial mühəndislik və fişinq hücumları kimi təhdidlərlə sıx bağlıdır.

Məlumatların dəyişdirilməsi və ya saxtalaşdırılması – transsərhəd məlumat ötürülməsi prosesində məlumat paketlərinin manipulyasiyası, saxta identifikasiya vasitəsilə autentifikasiya sistemlərinin pozulması mümkündür. Bu, hüquqi nəticələrə və məlumatın etibarlılığının itirilməsinə səbəb ola bilər.

Məlumatların üçüncü tərəflərə ötürülməsi – xarici xidmət təminatçıları və ya vasitəçi platformalar tərəfindən məlumatların kommersiya və ya siyasi məqsədlərlə üçüncü tərəflərə verilməsi fərdi məlumatların məxfiliyini pozur.

Milli informasiya suverenliyinin zəifləməsi – məlumatların ölkə xaricində yerləşən serverlərdə emal edilməsi dövlətin öz vətəndaşlarına məxsus informasiyaya nəzarət imkanlarını azaldır və milli informasiya resursları üzərində xarici asılılıq yaradır.

Transsərhəd məlumat ötürülməsi zamanı təhlükəsizlik risklərinin səviyyəsi bir sıra texnoloji, hüquqi və təşkilati amillərdən asılı olur:

1) Server infrastrukturunun yerləşdiyi ölkə – Serverlərin fiziki yerləşmə yeri həmin ölkənin hüquqi rejimi, məlumatların qorunması standartları və dövlət nəzarəti mexanizmləri ilə birbaşa əlaqədardır. Məlumatlar serverlərin yerləşdiyi ölkənin yurisdiksiyasına tabe olur və bu da məxfilik səviyyəsini müəyyən edir.

2) İstifadə olunan kommunikasiya şəbəkələri – Məlumat ötürülməsi prosesində istifadə olunan internet backbone-lar, telekommunikasiya kanalları və məlumat ötürmə protokollarının təhlükəsizlik səviyyəsi mühüm rol oynayır.

3) Hüquqi və normativ tənzimləmə mexanizmləri – Müxtəlif ölkələrdə fərdi məlumatların qorunması ilə bağlı qəbul olunmuş qanunvericilik fərqli səviyyədədir.

4) Texnoloji asılılıq səviyyəsi – Milli informasiya sistemlərinin əsas texnoloji platformalarının və proqram təminatlarının xarici istehsalçılardan asılı olması, informasiya suverenliyinə təhdid yaradır. Bu, həm təhlükəsizlik zəifliklərinin idarə edilməsini çətinləşdirir, həm də kiberhücumlar zamanı cavab tədbirlərini məhdudlaşdırır.

Bu meyarların kompleks şəkildə qiymətləndirilməsi məlumat təhlükəsizliyinin təmin edilməsi üçün mühüm əhəmiyyət kəsb edir.

IV. MƏLUMATLARIN TRANSSƏRHƏD ÖTÜRÜLMƏSİ ZAMANI RİSK MEYARLARI

Transsərhəd məlumat ötürülməsi risklərinin qiymətləndirilməsi üçün çoxmeyarlı qərarvermə metodlarından istifadə edilə bilər. Bu metodlar eyni zamanda bir neçə meyarın nəzərə alınmasına imkan verir.

Fərdi məlumatların transsərhəd ötürülməsi zamanı risklərin qiymətləndirilməsi üçün aşağıdakı əsas 4 meyar (strateji status, hüquqi tənzimləmə, texnoloji suverenlik və tranzit marşrut) müəyyən edilmişdir (Cədvəl 1.):

Meyar 1. Strateji status - məlumatların ötürülməsi zamanı strateji statusun qiymətləndirilməsi ilk növbədə məlumatın göndərildiyi və ya keçdiyi ölkələrin geosiyasi mövqeyi və etibarlılıq dərəcəsi ilə müəyyən edilir. Bu prosesdə ölkələrin dost, müttəfiq, neytral və ya rəqib olması əsas faktor kimi çıxış edərək ötürülən informasiyanın təhlükəsizlik səviyyəsinə birbaşa təsir göstərir. Müttəfiq ölkələrlə aparılan məlumat mübadiləsi qarşılıqlı etimad və strateji qazanc üzərində qurulduğu üçün burada təhdid səviyyəsi minimum hesab olunur, lakin neytral və xüsusilə qeyri-dost ölkələr söz mövzusu olduqda vəziyyət tamamilə dəyişir. Rəqib və ya düşmən hesab olunan tərəflərin nəzarətindəki serverlər və ya kommunikasiya kanalları vasitəsilə ötürülən hər bir məlumat, hətta sadə fərdi data olsa belə, həmin ölkələr tərəfindən sosial mühəndislik, şantaj və ya kütləvi manipulyasiya alətinə çevrilə bilər. Bu səbəbdən strateji status meyarının

CƏDVƏL 1. TRANSSƏRHƏD MƏLUMATLARIN ÖTÜRÜLMƏSİNİN QİYMƏTLƏNDİRİLMƏSİ MEYARLARI VƏ SƏVİYYƏLƏRİ

Meyar	Risk Səviyyəsi: Aşağı (1)	Risk Səviyyəsi: Orta (2)	Risk Səviyyəsi: Yüksək (3)
Strateji Status	Strateji tərəfdaş	Neytral və ya ticarət tərəfdaşı	Qeyri-dost və ya sanksiya tətbiq edilən ölkə
Hüquqi Tənzimləmə	Tam adekvat qanunvericilik	Qismən tənzimləmə, qeyri-müəyyən öhdəliklər	Heç bir hüquqi müdafiə və ya zəif nəzarət
Texnoloji Suverenlik	Sertifikatlaşdırılmış yerli və ya etibarlı vendor avadanlığı	Üçüncü tərəf, yoxlanılmış infrastruktur	Qapalı kodlu, mənşəyi şübhəli avadanlıqlar
Tranzit Marşrut	Birbaşa və ya yüksək şifrələnmiş qapalı kanallar	Çoxsaylı tranzit düyünləri olan standart internet yolları	Kiber-aktivliyin yüksək olduğu zonalar

qiymətləndirilməsi zamanı həm də həmin ölkələrin siyasi sabitliyi və gələcəkdə baş verə biləcək rejim dəyişikliklərinin məlumatların taleyinə necə təsir edəcəyi ciddi şəkildə nəzərə alınmalıdır.

Meyar 2. Hüquqi tənzimləmə ilk növbədə, məlumatların hansı ölkənin qanunvericiliyinə tabe olması və həmin ölkədə dövlət orqanlarının məlumatlara çıxış imkanları ilə bağlıdır. Məsələn, müəyyən dövlətlərdə milli təhlükəsizlik qanunvericiliyi bulud provayderlərini istifadəçi məlumatlarını dövlət qurumlarına təqdim etməyə məcbur edə bilər. Bu isə digər ölkələrin məxfilik qanunvericiliyi ilə ziddiyyət yarada bilər.

Meyar 3. Texnoloji suverenlik fərdi məlumatların transsərhəd ötürülməsi zamanı ən kritik komponentlərdən biri məlumatın hansı texnoloji infrastruktur üzərindən idarə olunması və bu infrastruktur üzərində real nəzarətin kimə məxsus olmasıdır. Texnoloji suverenlik dedikdə, məlumatların saxlanıldığı serverlərin, istifadə olunan proqram təminatının, şifrələmə mexanizmlərinin və ümumilikdə rəqəmsal ekosistemin hansı ölkəyə və ya şirkətə aid olması nəzərdə tutulur.

Əgər məlumatlar xarici texnologiyalara və ya üçüncü tərəf platformalara güclü şəkildə bağlıdırsa, bu zaman həmin platformaların sahib olduğu dövlət və ya təşkilat dolayı şəkildə məlumatlara təsir və ya çıxış imkanına malik ola bilər. Xüsusilə, qapalı mənbə proqram təminatı istifadə edildikdə sistemin daxili işləmə prinsipləri tam şəffaf olmur və bu da gizli zəifliklərin və ya arxa qapıların (backdoor) mövcudluğu riskini artırır.

Bununla yanaşı, texnoloji suverenlik yalnız texniki mülkiyyətlə məhdudlaşmır. Buraya həm də ölkənin özünün müstəqil kiberinfrastruktur qurmaq, məlumatları yerli səviyyədə emal etmək və kritik sistemlərdə xarici asılılığı minimuma endirmək qabiliyyəti daxildir. Yüksək texnoloji suverenliyə malik ölkələr məlumatların təhlükəsizliyini daha effektiv şəkildə təmin edə bilir, çünki onlar həm hüquqi, həm də texniki nəzarəti öz əllərində saxlayırlar.

Meyar 4. Tranzit Marşrut - fərdi məlumatların transsərhəd ötürülməsi zamanı məlumatın yalnız göndərildiyi və qəbul edildiyi ölkə deyil, həm də ötürülmə prosesində keçdiyi bütün aralıq marşrutlar mühüm risk faktoru kimi çıxış edir. İnternet infrastrukturu qlobal və çoxsəviyyəli olduğu üçün məlumat paketləri çox vaxt birbaşa deyil, müxtəlif ölkələrdə yerləşən serverlər, data mərkəzləri və şəbəkə qovşaqları vasitəsilə ötürülür.

Bu isə o deməkdir ki, məlumat hətta etibarlı iki tərəf arasında mübadilə olunsa belə, ötürülmə zamanı üçüncü ölkələrin nəzarətində olan infrastrukturdan keçə bilər. Belə hallarda həmin tranzit ölkələr texniki və ya hüquqi imkanlardan istifadə edərək məlumatlara müdaxilə, monitorinq və ya ələ keçirmə potensialına malik ola bilərlər. Xüsusilə, zəif şifrələmə istifadə edildikdə və ya açıq şəbəkələrdən ötürmə baş verdikdə bu risk daha da artır.

Göründüyün kimi qeyd olunan 4 meyarın aşağıda qeyd olunan bəzi risk amillər vardır. Bunlara ölkələrarası siyasi gərginlik və ya münaqişə ehtimalı; məlumatın rəqib və ya qeyri-dost ölkələrin infrastrukturundan keçməsi; rejim dəyişiklikləri və siyasi qeyri-sabitlik; dövlət səviyyəsində kiberkəşfiyyat və nəzarət fəaliyyəti; sosial mühəndislik, dezinformasiya və şantaj məqsədli istifadə riski; xarici ölkə qanunvericiliyinin məlumatlara məcburi çıxış imkanı verməsi; məlumatların qorunması üzrə qanunların zəif və ya qeyri-müəyyən olması; müxtəlif ölkələrin hüquqi tələbləri arasında ziddiyyət (məsələn, məxfilik vs milli təhlükəsizlik); məhkəmə qərarı olmadan məlumatlara çıxış imkanları; məlumatların saxlanma müddəti və istifadəsi ilə bağlı qeyri-şəffaflıq; beynəlxalq məlumat ötürülməsi üzrə razılaşmaların olmaması; xarici texnologiyalardan və platformalardan yüksək asılılıq; qapalı mənbə proqram təminatında potensial "backdoor" riskləri; şifrələmə mexanizmlərinin zəifliyi və ya üçüncü tərəflərin nəzarəti; məlumatların fiziki olaraq xarici serverlərdə saxlanılması; məlumatın keçdiyi aralıq ölkələrin etibarsız olması; şəbəkə marşrutlaşdırmasının qeyri-şəffaflığı (routing riskləri); kiberhücumlarının mümkünlüyü; şifrələnməmiş və ya zəif şifrələnmiş ötürmə kanalları; itimai və açıq şəbəkələrdən istifadə və s. göstərilə bilər.

Bütün bunlar nəzərə alaraq, məlumatların transsərhəd ötürülməsi zamanı bu meyarların birlikdə nəzərə alınmasının mühüm əhəmiyyət kəsb etdiyini qeyd etmək mümkündür.

Qiymətləndirmə zamanı bu meyarlar aşağı (1), orta (2) və yüksək (3) risk olmaqla qiymətləndirilir.

Aşağı risk dedikdə kiçik boşluqlar var, amma idarəolunandır.

Orta risk dedikdə Bəzi təhlükələr var, diqqətli olmaq lazımdır.

Yüksək risk dedikdə isə ciddi təhlükə mənbəyidir və məlumatların bura göndərilməsi təhlükəlidir.

Beləliklə, hər hansı bir xarici ölkəyə məlumat ötürülərkən bu 4 meyar üzrə [1-3] aralığında ballar verilir və toplanmış balların ədədi ortası tapılaraq ümumi risk indeksi hesablanır. Alınmış nəticələrin müqayisəsi üçün çoxmeyarlı qiymətləndirmə metodlarından istifadə edilərək transsərhəd ötürülən məlumatların risklərini qiymətləndirmək mümkündür. Əgər alınan nəticələr [1.00 - 1.66] olarsa bu aşağı riskli hesab olunur və məlumatların ötürülməsinə icazə verilir. [1.67 - 2.33] olarsa orta riskli hesab olunur və əlavə şifrələmə, nəzarət tələb olunur. [2.34 - 3.00] olarsa yüksək riskli hesab olunur və məlumatların transsərhəd ötürülməsi məqsədəuyğun hesab edilmir. Başqa sözlə fərdi məlumatların transsərhəd ötürülməsi kritik təhlükədir.

NƏTİCƏ

Tədqiqat işində fərdi məlumatların müasir informasiya cəmiyyətində strateji resurs kimi çıxış etdiyi nəzərə alınaraq, onların digər ölkələrin nəzarətinə keçmə ehtimalının və bu prosesin milli maraqlara vura biləcəyi potensial ziyanın sistemli şəkildə qiymətləndirilməsi məqsədilə çoxmeyarlı yanaşma təklif edilmişdir. Qloballaşma və rəqəmsallaşmanın sürətlənməsi fonunda fərdi məlumatların transsərhəd dövriyyəsi genişlənməkdədir ki, bu da məlumat təhlükəsizliyi, suverenlik və hüquqi nəzarət baxımından yeni risklərin yaranmasına səbəb olur. Bu baxımdan, qeyd olunan risklərin kompleks və obyektiv şəkildə təhlili xüsusi aktuallıq kəsb edir.

Təklif edilən yanaşmada fərdi məlumatların transsərhəd ötürülməsi zamanı risklərin qiymətləndirilməsi üçün dörd əsas meyar müəyyən edilmişdir. Hər bir meyar risk səviyyəsinə uyğun olaraq aşağı, orta və yüksək səviyyələr üzrə qiymətləndirilir. Bununla belə, qeyd etmək vacibdir ki, yalnız bir meyar əsasında aparılan qiymətləndirmə yetərli hesab olunmur. Çünki fərdi məlumatların təhlükəsizliyi çoxşaxəli və kompleks xarakter daşıyır. Bu baxımdan, risklərin daha dəqiq və etibarlı qiymətləndirilməsi üçün bütün meyarların qarşılıqlı əlaqədə və inteqrativ şəkildə təhlil olunması zəruridir.

Nəticə etibarilə, təklif olunan çoxmeyarlı yanaşma fərdi məlumatların transsərhəd ötürülməsi zamanı yaranan risklərin sistemli şəkildə müəyyən edilməsinə, onların səviyyəsinin əsaslandırılmış formada qiymətləndirilməsinə və müvafiq idarəetmə qərarlarının qəbuluna metodoloji əsas yaradır. Bu yanaşma həm milli təhlükəsizlik maraqlarının qorunmasına, həm də beynəlxalq məlumat mübadiləsinin daha təhlükəsiz və şəffaf şəkildə həyata keçirilməsinə töhfə verə bilər.

ƏDƏBİYYAT

[1] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyberphysical systems and their security issues," Computers in Industry, vol. 100, pp. 212–223, 2018, doi: 10.1016/j.compind.2018.04.017.

[2] E. A. Lee and S. A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, 2nd ed. Cambridge, MA, USA: MIT Press, 2017.

[3] A. M. Mustafa, "Analysis of sources of personal data formation in cyber-physical social systems," in Proc. IEEE 17th Int. Conf. Application of Information and Communication Technologies (AICT), 2023, pp. 1–4, doi: 10.1109/AICT59525.2023.10313201.

[4] R. Baheti and H. Gill, "Cyber-physical systems," in The Impact of Control Technology, T. Samad and A. M. Annaswamy, Eds., 2011, pp. 161–166.

[5] A. Mustafa, "Cyber-physical social systems: application areas, existing problems and perspectives," Problems of Information Society, vol. 16, no. 2, pp. 86–97, 2025, doi: 10.25045/jpis.v16.i2.10.

[6] T. Sobb, B. Turnbull, and N. Moustafa, "A holistic review of cyber–physical–social systems: New directions and opportunities," Sensors, vol. 23, no. 17, 2023, doi: 10.3390/s23177391.

[7] A. M. Mustafa, "Protection issues of personal data in the cyber physical social system," in Proc. 2nd Int. Scientific and Technical Conf. Infocommunication Systems and Artificial Intelligence Technologies, Dec. 4–5, 2024.

[8] R. Baheti and H. Gill, "Cyber-Physical Systems," in The Impact of Control Technology, T. Samad and A. M. Annaswamy, Eds., 2011. [Online]. Available: http://www.ieeecss.org

Multi-criteria Assessment of Risks of Transborder Transfer of Personal Data in Social Cyberphysical Systems

Araz Mustafa

Institute of Information Technology, Baku, Azerbaijan

Abstract— The research work proposes a multi-criteria approach to assess the risks arising during the transfer of personal data collected in social cyberphysical systems. In addition to technological gaps, the approach under consideration also takes into account factors such as the social environment, human factor, level of legal regulation and the sustainability of the national digital infrastructure for the purpose of prioritization. An approach is proposed to identify vulnerabilities and assess their potential impact on cybersovereignty using modern decision-making methods of risks. The results obtained serve to protect the confidentiality of personal data in social cyberphysical systems, as well as to strengthen management and control mechanisms in the national digital environment, as well as to ensure cybersovereignty.

Keywords— Social cyberphysical systems; cyber sovereignty; personal data security; risk assessment; multi-criteria assessment; data transfer.