Rəqəmsal Transformasiya Şəraitində İqtisadi İnformasiya Sistemlərinin Kibertəhlükəsizlik Problemləri

Roza Şahverdiyeva
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shahverdiyevar@gmail.com

***Xülasə*— Məqalədə iqtisadi xarakterli kibertəhdidlər və təhlükələr təsnif edilmiş, həmin təhdidlərin növləri araşdırılmış və müvafiq kibertəhlükəsizlik problemləri analiz olunmuşdur. İqtisadi informasiya sistemlərinin kibertəhlükəsizliyində tətbiq olunan əsas süni intellekt texnologiyaları izah olunmuşdur. Rəqəmsal transformasiya şəraitində iqtisadi informasiya sistemlərinin kibertəhlükəsizliyinin qorunması və dayanıqlığının yüksəldilməsi üzrə konseptual struktur model işlənilmişdir. İqtisadi informasiya sistemlərinin kibertəhlükəsizlik problemlərinin təhlili və onların həllinin perspektiv inkişaf istiqamətləri üzrə bəzi tövsiyələr verilmişdir.**

Açar sözlər— iqtisadiyyatın rəqəmsal transformasiyası; süni intellekt texnologiyaları; sənaye 4.0 platforması; kibertəhdidlər; iqtisadi informasiya sistemləri; kibertəhlükəsizlik.

I. GİRİŞ

Qlobal rəqəmsal transformasiya müasir iqtisadi sistemlərin, proseslərin və strukturların inkişaf dinamikasını fundamental şəkildə yenidən formalaşdıraraq rəqəmsal texnologiyaların iqtisadiyyata tətbiqini əhəmiyyətli dərəcədə sürətləndirmişdir. Bu kontekstdə iqtisadi informasiya sistemləri həm müəssisələrdə, həm də dövlət idarəetmə strukturlarında əsas qərar qəbuletmə prosesinə dəstək mexanizmi kimi çıxış edir. Bunlar böyük həcmli verilənlərin toplanmasını, emalını, saxlanılmasını və analitik təhlilini təmin edir. Rəqəmsal texnologiyalar iqtisadi prosesləri optimallaşdırmaqla, idarəetmə qərarlarının effektivliyini artırmaqla iqtisadiyyatın sahələrini tədricən transformasiya edir [1, 2].

Rəqəmsallaşmanın intensivləşməsi kibermühitdə risklərin də paralel şəkildə artmasına səbəb olmuşdur. Müasir şəraitdə kibertəhlükəsizlik artıq yalnız texniki məsələ kimi deyil, həm də makroiqtisadi sabitliyin və milli təhlükəsizliyin ayrılmaz elementi kimi qiymətləndirilir. İqtisadi informasiya sistemlərinə yönəlmiş kiberhücumlar məlumatların məxfiliyinin pozulması, bütövlüyünün deqradasiyası və əlçatanlığın məhdudlaşdırılması ilə nəticələnərək maliyyə itkiləri, institusional reputasiya zədələri və idarəetmə proseslərində disfunksiyalara səbəb olur.

Xüsusilə bulud hesablama infrastrukturları, böyük verilənlər ekosistemləri, süni intellekt əsaslı alqoritmlər və IoT platformalarının geniş tətbiqi funksional imkanları genişləndirməklə yanaşı, eyni zamanda hücum spektrini də artırır və yeni təhlükə vektorlarının formalaşmasına şərait yaradır. Bu baxımdan iqtisadi informasiya sistemlərinin kibertəhlükəsizlik problemlərinin təhlili kompleks, çoxsəviyyəli və sistem yanaşması tələb edən elmi-praktik istiqamət kimi çıxış edir. Bu kimi problemlər isə baxılan məsələnin aktuallığını şərtləndirir [3]. Böyük həcmli və yüksək sürətli məlumat axınlarının mövcudluğu şəraitində kibertəhdidlərin erkən aşkarlanması və qabaqlayıcı proqnozlaşdırılması üçün klassik metodların məhdudluğu aydın şəkildə müşahidə olunur. Bu isə maşın təlimi və dərin təlim alqoritmləri, eləcə də süni intellekt əsaslı adaptiv modellərin tətbiqini zəruri edir.

Burada rəqəmsal transformasiya şəraitində iqtisadi informasiya sistemlərinin kibertəhlükəsizlik səviyyəsinin artırılması üçün mövcud problemlərin sistemli şəkildə təhlili, risklərin qiymətləndirilməsi, müasir texnoloji yanaşmalar və rəqəmsal texnologiyaların tətbiqi ilə adaptiv, intellektual və kompleks təhlükəsizlik mexanizmlərinin işlənilməsi həlli tələb olunan əsas elmi problemlərdən birini təşkil edir.

Rəqəmsal transformasiya şəraitində iqtisadi informasiya sistemlərinin kibertəhlükəsizlik problemlərinin təhlili məsələləri ilə bağlı bir çox alim və tədqiqatçıların müəyyən elmi tədqiqatlar aparmalarına baxmayaraq oxşar sahədə həllini gözləyən bir çox problemlər hələ də mövcuddur [2, 4-10].

II. RƏQƏMSAL TRANSFORMASİYA ŞƏRAİTİNDƏ İQTİSADİ İNFORMASİYA SİSTEMLƏRİ VƏ KİBERTƏHLÜKƏSİZLİK TƏLƏBLƏRİ

Rəqəmsal transformasiya proseslərinin sürətlənməsi iqtisadi sistemlərin strukturunu köklü şəkildə dəyişdirərək informasiya axınlarının həcmini, mürəkkəbliyini və strateji əhəmiyyətini əhəmiyyətli dərəcədə artırmışdır. Müasir mərhələdə iqtisadi informasiya sistemləri yalnız məlumatların toplanması və emalı funksiyasını yerinə yetirmir, eyni zamanda qərar qəbuletmə, proqnozlaşdırma və resursların optimallaşdırılması kimi idarəetmə proseslərinin əsas infrastruktur komponentinə çevrilmişdir çevrilmişdir. Bu transformasiya isə paralel olaraq kibertəhlükəsizlik risklərinin intensivləşməsinə və yeni təhdidlərin formalaşmasına səbəb olur [9].

Rəqəmsal iqtisadiyyat ekosistemində fəaliyyət göstərən təşkilatlar üçün informasiya sistemlərinin təhlükəsizliyi artıq texniki məsələ olmaqdan çıxaraq strateji idarəetmə prioritetinə çevrilmişdir. Xüsusilə böyük verilənlər (Big Data), bulud texnologiyaları və süni intellekt əsaslı həllərin geniş tətbiqi informasiya aktivlərinin qorunması, məxfilik, bütövlük və

DOI: 10.25045/forensic.gov.2026.67

əlçatanlıq prinsiplərinin təmin edilməsini daha da aktuallaşdırır. Bu baxımdan, iqtisadi informasiya sistemlərinin kibertəhlükəsizlik tələbləri yalnız mövcud təhlükələrin qarşısının alınmasına deyil, həm də adaptiv, proaktiv və davamlı müdafiə mexanizmlərinin formalaşdırılmasına yönəldilməlidir.

Davamlı texnoloji irəliləyişlər və rəqəmsal transformasiyanın sürətlənməsi fonunda iqtisadi informasiya sistemlərinin aktual məsələlərindən biri kimi kibertəhlükəsizliyin əsas məqsədi həssas məlumatları icazəsiz girişdən və potensial kibertəhdidlərdən qorumaq üçün müdafiə mexanizmi kimi fəaliyyət göstərməkdir. Effektiv kibertəhlükəsizliyin təmin edilməsi, təhdidlərin qarşısının alınması, real-vaxt rejimində monitorinq və təhdidlərə operativ cavab mexanizmlərini əhatə edən hərtərəfli, çoxqatlı strategiyaların qəbul edilməsini zəruri edir. Bunlara şifrələmə və proqram təminatına əsaslanan müdafiə sistemləri kimi qabaqcıl texnologiyaların tətbiqi, eləcə də istifadəçi təhsili və ən yaxşı təcrübələr üzrə təlim vasitəsilə rəqəmsal təhlükəsizlik məlumatlılığının artırılması daxildir. Bu sahədəki əsas çətinlik kibertəhdidlərin daim inkişaf edən təbiətindədir. Zərərli aktorlar rəqəmsal infrastrukturları pozmaq üçün davamlı olaraq innovativ üsullar axtarırlar. Nəticədə, kibertəhlükəsizlik mütəxəssisləri bu risklərə effektiv şəkildə qarşı çıxmaq üçün ən son inkişaf və təhdidlər haqqında məlumatlı olmalıdırlar [11]. Bu çətinliklərin mürəkkəbliyinə baxmayaraq, güclü kibertəhlükəsizliyə strateji investisiyalar qoyulması, rəqəmsal təhlükəsizlik üzrə məlumatlılığın artırılması və geniş yayılmasına müvafiq dövlət orqanları arasında gücləndirilmiş əməkdaşlıq yolu ilə nail olmaq olar. Beləliklə, kibertəhlükəsizlik fərdləri, təşkilatları və dövlət qurumlarını əhatə edən ortaq məsuliyyət təşkil edir. Yüksək məlumatlılıq və əməkdaşlıq fəaliyyəti rəqəmsal ekosistemlərin qorunması və təhlükəsizliyinin təmin edilməsi üçün vacib təməl təşkil edir.

III. İQTİSADİ İNFORMASİYA SİSTEMLƏRİNƏ YÖNƏLMİŞ KİBERTƏHLÜKƏSİZLİK TƏHDİDLƏRİNİN TƏSNİFATI

İqtisadi informasiya sistemləri müasir rəqəmsal iqtisadiyyatın əsas dayaqlarından biri kimi çıxış etsə də, onların geniş inteqrasiyası və şəbəkələşməsi kibertəhlükəsizlik baxımından çoxşaxəli risk mühitinin formalaşmasına səbəb olmuşdur [9]. Bu sistemlərdə yaranan təhdidlər həm texnoloji arxitektura, həm də təşkilati faktorlarla sıx bağlıdır və nəticə etibarilə iqtisadi proseslərin davamlılığına birbaşa təsir göstərir.

İqtisadi informasiya sistemləri getdikcə daha çox müxtəlif kiberhücumlar, o cümlədən mürəkkəb süni intellektlə işləyən texnikalar və ransomware və fişinq kimi ənənəvi hücum vektorları tərəfindən təhdid altındadır. Bu təhdidlər həm köhnə, həm də müasir sistemlərdə mövcud olan zəifliklərdən istifadə edir və kritik infrastrukturların qarşılıqlı əlaqəsi ilə daha da çətinləşir. Müvafiq strategiyalar hazırda daha yaxşı aşkarlama, dayanıqlıq və tənzimləyici uyğunluq üçün süni intellekt və blokçeyn inteqrasiyası kimi qabaqcıl texnologiyaları əhatə edir [12].

İqtisadi informasiya sistemlərində ən geniş yayılmış təhdid növlərindən biri zərərli proqram təminatıdır (malware). Bu kateqoriyaya viruslar, troyanlar, şantaj proqramları (ransomware) və casus proqramları (spyware) kimi hücum vasitələri daxildir. Xüsusilə ransomware hücumları iqtisadi informasiya sistemlərində məlumatların şifrələnməsi və onların bərpası üçün vəsaitlər tələb edilməsi ilə xarakterizə olunur ki, bu da maliyyə itkiləri və əməliyyat dayanıqlığının pozulması ilə nəticələnir.

Digər mühüm təhdid kateqoriyası şəbəkə əsaslı hücumlardır. Buraya "man-in-the-middle", "denial-of-service (DoS/DDoS)" və paketlərin dinlənilməsi hücumları daxildir. Bu tip hücumlar sistemlərarası məlumat mübadiləsinin bütövlüyünü və əlçatanlığını pozaraq iqtisadi informasiya axınında ciddi gecikmələr və ya tam dayanmalar yarada bilər.

İnsan faktoru ilə bağlı təhdidlər də iqtisadi informasiya sistemlərinin zəif cəhətlərindən biri hesab olunur. Bu cür hücumlar texniki müdafiə sistemlərindən yan keçərək birbaşa insan davranışını hədəf alır [13].

Bundan əlavə, daxili təhdidlər (insider threats) təşkilat daxilində çalışan şəxslərin icazəli və ya icazəsiz şəkildə sistem resurslarına zərər verməsi ilə xarakterizə olunur. Bu təhdidlər çox vaxt aşkarlanması çətin olan və uzunmüddətli təsir yaradan risk kateqoriyasına daxildir.

Son illərdə bulud əsaslı iqtisadi informasiya sistemlərinin genişlənməsi ilə birlikdə virtual infrastruktur zəifliklərı də ön plana çıxmışdır. Konfiqurasiya səhvləri, zəif tətbiqi proqramlaşdırma interfeysi (API) təhlükəsizliyi və paylaşılan resurs modelləri məlumat sızması riskini artırır.

İqtisadi informasiya sistemlərində kibertəhlükəsizlik təhdidləri çoxsəviyyəli xarakter daşıyır və onların effektiv idarə olunması yalnız texniki müdafiə mexanizmləri ilə deyil, həm də risk əsaslı idarəetmə yanaşmaları və davamlı monitorinq sistemləri ilə təmin edilməlidir [9].

İqtisadi xarakterli kibertəhdidlər. İqtisadi xarakterli kibertəhdidlərdəki müasir tendensiyaları daim təhlil etmək lazımdır. Makro səviyyədə ən təhlükəli tendensiya ölkələr arasındakı münaqişələrdə kibertəhdidlərin istifadəsidir ki, bu da yeni formalar alır.

İqtisadi xarakterli mikrosəviyyəli kibertəhdidləri və təhlükələri aşağıdakı kimi təsnif etmək olar:

1)Fişinq kibercinayətkarlığın ən geniş yayılmış növlərindən biri hesab olunur və hər il çoxsaylı maliyyə itkilərinə səbəb olur.

2)Zərərli proqram təminatı kibercinayətkarlar tərəfindən şirkət cihazlarına davamlı və gizli giriş imkanı yaradan "backdoor" mexanizmlərinin formalaşdırılması məqsədilə hazırlanır.

3)Şantaj proqramı- zərərli proqram təminatının elə bir növüdür ki, müəssisələr üçün ciddi və bəzən dağıdıcı nəticələrə səbəb ola bilər. Bu tip hücumlar informasiya sistemlərinə çıxışı məhdudlaşdıraraq və ya tam bloklayaraq təşkilatları kritik məlumatlara əlçatanlıqdan məhrum edir.

4)Korporativ e-poçtun ələ keçirilməsi- ən yüksək maliyyə zərərləri ilə nəticələnən kibercinayət növlərindən biri hesab olunur.

5)Daxili təhdidlər müəssisə daxilində məxfi məlumatlara çıxış imkanı olan şəxslərlə bağlı riskləri ifadə edir.

6)Qeyri-ixtiyari məlumat sızması əməkdaşların ehtiyatsızlığı və ya diqqətsizliyi nəticəsində məxfi informasiyanın təsadüfən açıqlanması ilə xarakterizə olunur.

7) Bulud əsaslı məlumatların saxlanılması.. Kibercinayətkarlar xüsusilə zəif qorunan və ya düzgün

konfiqurasiya olunmamış bulud yaddaş resurslarını hədəf alaraq məlumatlara çıxış əldə etməyə və onlardan sui-istifadə etməyə çalışırlar.

8)Sosial mühəndislik kibercinayətkarların sosial şəbəkələr [14] və digər kommunikasiya platformaları üzərindən saxta şəxsiyyətlər və profillər yaradaraq potensial qurbanların etimadını qazanmasına əsaslanan hücum üsuludur.

IV. RƏQƏMSAL TRANSFORMASİYA ŞƏRAİTİNDƏ İQTİSADİ İNFORMASİYA SİSTEMLƏRİNİN KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİ

İqtisadi informasiya sistemlərində kibertəhlükəsizlik problemləri çoxaspektlidir. Süni intellektlə işləyən hücumlar və IoT zəifliklərı kimi inkişaf etmiş və inkişaf edən təhdidləri də əhatə edir. İşçilərin təlimi və çoxfaktorlu identifikasiya kimi mövcud kibertəhlükəsizlik tədbirləri effektiv olsa da, onların təsiri müxtəlif kontekstlərdə dəyişir. Süni intellekt, blokçeyn və s. kimi inkişaf etməkdə olan texnologiyalar təhdidlərin aşkarlanmasını və məlumatların bütövlüyünü artırmaq üçün inteqrasiya olunur [2, 15-17]. Bununla belə, əsas çətinliklər istifadə rahatlığının təhlükəsizliklə balanslaşdırılması, tətbiqlərin standartlaşdırılması və iqtisadi siyasətlərin texniki təhlükəsizlik tədbirləri ilə inteqrasiyasında qalmaqdadır. Bu sistemlərin dinamik və qarşılıqlı əlaqəli təbiəti iqtisadi sabitliyi qorumaq üçün çoxsahəli tədqiqatlar və davamlı innovasiyalar tələb edir.

İqtisadi informasiya sistemləri rəqəmsal innovasiya və sistem risklərinin mərkəzindədir. Onlar süni intellekt, IoT və artan qarşılıqlı əlaqənin yaratdığı sürətlə inkişaf edən təhlükələr ilə üzləşir. Süni intellekt, blokçeyn və s. kimi texnologiyalar məlumatların bütövlüyünü dəyişdirərək yeni mürəkkəbliklər yaradır. Bu çətinliklərin həlli davamlı innovasiya, investisiya və ən əsası, texniki, iqtisadi və siyasət sahələrini birləşdirən çoxsahəli əməkdaşlıq tələb edir. Yalnız inteqrasiya olunmuş yanaşmalar vasitəsilə rəqəmsal dövrdə iqtisadi informasiya sistemlərinin təhlükəsizliyi və dayanıqlığı təmin edilə bilər.

Rəqəmsal transformasiya iqtisadi informasiya sistemlərini müəssisə və dövlət idarəçiliyinin mərkəzi informasiya infrastrukturuna çevirir. Bununla yanaşı, məlumat axınlarının, inteqrasiyaların, uzaqdan çıxışların və platformalararası asılılıqların artması hücum səthini də genişləndirir. Təhlillər göstərir ki, rəqəmsallaşma biznes proseslərinə daha dərin nüfuz etdikcə informasiya strateji aktivə çevrildiyindən təhlükəsizlik də təşkilati davamlılıq şərti kimi çıxış edir. Bu kontekstdə rəqəmsal transformasiyanın verdiyi səmərəlilik üstünlükləri daha mürəkkəb kiberrisklər yaradır [18].

Rəqəmsal transformasiya şəraitində iqtisadi informasiya sistemlərinin kibertəhlükəsizlik problemlərini belə sistemləşdirmək olar:

Hücum istiqamətlərinin genişlənməsi və sistem mürəkkəbliyi. Rəqəmsal transformasiya nəticəsində bulud texnologiyaları, IoT, tətbiqi proqramlaşdırma interfeysi inteqrasiyaları və platformalararası əlaqələr sürətlə artır. Bu isə potensial zəif nöqtələrin sayını genişləndirərək hücumları çoxsəviyyəli edir. Belə mühitdə sistemlərin tam nəzarətdə saxlanılması çətinləşir və təhlükəsizlik arxitekturası mürəkkəbləşir [18].

Məlumat sızıntıları və məxfilik riskləri. İqtisadi informasiya sistemləri böyük həcmdə həssas məlumatları (maliyyə göstəriciləri, müştəri məlumatları, strateji planlar) emal edir. Bu sistemlərdə məlumatın paylanması artdıqca icazəsiz çıxış, daxili sızmalar və məlumatın qeyri-qanuni istifadəsi riskləri də yüksəlir [9].

İnsan faktoru və kadr çatışmazlığı. Kibertəhlükəsizlik insidentlərinin əhəmiyyətli hissəsi insan səhvləri ilə bağlıdır: zəif parollar, fişinq hücumlarına məruz qalma, təhlükəsizlik prosedurlarına əməl olunmaması və s. Eyni zamanda yüksək ixtisaslı kibertəhlükəsizlik mütəxəssislərinin çatışmazlığı həmin problemləri daha da dərinləşdirir [10].

Risklərin adekvat qiymətləndirilməməsi. Bir çox təşkilatlar kiberriskləri texniki məsələ kimi qəbul edir və onları ümumi biznes risk idarəetmə sisteminə inteqrasiya etmir. Nəticədə risklərin prioritetləşdirilməsi və resursların optimal bölüşdürülməsi zəifləyir

Bulud və paylanmış infrastrukturlarda təhlükəsizlik boşluqları təhlükəsizlik boşluqları. Bulud texnologiyalarının geniş istifadəsi məlumatların fiziki nəzarətdən çıxmasına səbəb olur. Ona görə də multi-cloud və hibrid arxitekturalarda təhlükəsizlik siyasətlərinin standartlaşdırılması və monitorinqi də çətinləşir

Kibertəhlükəsizliyin iqtisadi səmərəliliyinin qeyri-müəyyənliyi. Kibertəhlükəsizlik investisiyalarının iqtisadi səmərəliliyi çox vaxt birbaşa ölçülə bilmir. Bu səbəbdən təşkilatlar optimal investisiya səviyyəsini müəyyən etməkdə çətinlik çəkir və ya təhlükəsizliyə zəruri resurs ayırmır.

Təchizat zənciri (supply chain) riskləri. Rəqəmsal ekosistemlərdə xidmət təminatçıları, proqram komponentləri və platformalar da geniş istifadə olunur. Bunlar isə "zəif halqa" effekti yaradaraq təhlükəsizlik zəifliyi kimi tərəfdaşlardan biri vasitəsilə bütün sistemə təsir edə bilər [19].

Real-vaxt rejimində monitorinq və insidentlərin idarə olunması çətinliyi. Rəqəmsal iqtisadi sistemlərdə məlumat axınlarının sürəti və həcmi ənənəvi monitorinq metodlarını qeyri-effektiv edir. Bu səbəbdən anomaliyaların aşkarlanması və insidentə operativ reaksiya mexanizmləri yetərli səviyyədə olmur [9].

Normativ-hüquqi və standartlaşdırma problemləri. Kibertəhlükəsizlik sahəsində beynəlxalq və milli standartların müxtəlifliyi, uyğunluq tələblərinin mürəkkəbliyi təşkilatların vahid təhlükəsizlik strategiyası qurmasını çətinləşdirir (OECD, 2022. https://www.oecd.org/en/publications/oecd-policy-framework-on-digital-security_a69df866-en.html).

Rəqəmsal transformasiya və təhlükəsizlik arasında balansın qorunması. İnnovasiya sürəti ilə təhlükəsizlik tələbləri arasında ziddiyyət yaranır. Sürətli rəqəmsallaşma çox vaxt təhlükəsizlik testlərinin və auditlərin səthi aparılmasına səbəb olur. Bu isə uzunmüddətli riskləri artırır [10].

Süni intellekt əsaslı hücumların artması. Süni intellekt və maşın təlimi yalnız müdafiə üçün deyil, hücum məqsədləri üçün də istifadə olunur (məsələn, avtomatlaşdırılmış fişinq, deepfake

hücumları). Bu hal ənənəvi təhlükəsizlik yanaşmalarını qeyri-kafi edir [19].

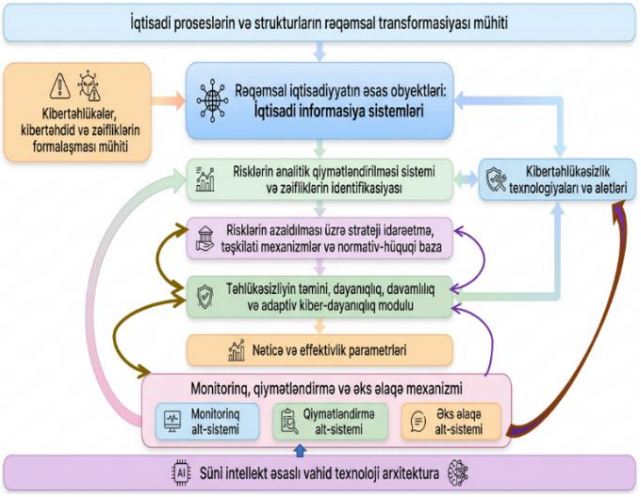
Sistem davamlılığı və bərpaolunma problemləri. Kibercinayətkarlığın artması fonunda yalnız hücumların qarşısını almaq deyil, həm də sistemlərin tez bərpası (cyber resilience) əsas problemə çevrilir. Bir çox iqtisadi informasiya sistemləri bu baxımdan yetərli hazırlığa malik deyil.

Aparılan tədqiqatlar göstərir ki, rəqəmsal transformasiya şəraitində kibertəhlükəsizlik problemi çoxölçülü və dinamik xarakter daşıyır. İqtisadi informasiya sistemlərinin effektiv qorunması üçün texnoloji həllərlə yanaşı, risk yönümlü idarəetmə, insan kapitalının inkişafı və institusional uyğunlaşma zəruridir [20, 21]. Müasir yanaşma kibertəhlükəsizliyi xərclər kateqoriyası kimi deyil, rəqəmsal iqtisadiyyatın dayanıqlığını təmin edən strateji faktor kimi qiymətləndirməyi tələb edir. Təhlillər göstərir ki, qeyd olunan problemlərin həll istiqamətlərində əksər modellər dinamik, inkişaf edən təhdid mühitlərini və cavabların fasiləsiz təbiətini əks etdirə bilmir. Tənzimləyici təsirləri, xarici təsirləri və təşviq uyğunluğunu özündə birləşdirən modellərə ehtiyac vardır. Bu aspektdə iqtisadiyyat, siyasət və texniki tədqiqatların daha geniş inteqrasiyasına ehtiyac vardır [22-24].

V. İQTİSADİ İNFORMASİYA SİSTEMLƏRİNİN KİBERTƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ VƏ DAYANIQLIĞININ ARTIRILMASI ÜZRƏ KONSEPTUAL MODELİ

Rəqəmsal transformasiyanın sürətlənməsi iqtisadi informasiya sistemlərinin funksional imkanlarını genişləndirməklə yanaşı, onların kibertəhlükəsizlik baxımından yeni risk və təhdidlərə məruz qalma ehtimalını da əhəmiyyətli dərəcədə artırmışdır. Müasir iqtisadi mühitdə məlumatların həcmi, müxtəlifliyi və emal sürəti artdıqca, informasiya sistemlərinin etibarlılığı və dayanıqlığı strateji prioritetə çevrilir. Xüsusilə, paylanmış arxitekturalar, bulud texnologiyaları və süni intellekt əsaslı qərarları dəstəkləyən sistemlərin geniş tətbiqi kibermühitin mürəkkəbliyini daha da artırır və ənənəvi təhlükəsizlik yanaşmalarının effektivliyini azaldır. Bu kontekstdə iqtisadi informasiya sistemlərinin kibertəhlükəsizliyinin təmin olunması yalnız texniki müdafiə tədbirləri ilə kifayətlənməyərək, risklərin proaktiv idarə olunmasına, adaptiv təhlükəsizlik mexanizmlərinə və sistemin ümumi dayanıqlığının yüksəldilməsinə yönəlmiş kompleks yanaşma tələb edir. Belə bir yanaşma, monitorinq, qiymətləndirmə və əks əlaqə mexanizmlərinin inteqrasiyası əsasında formalaşan və real-vaxt rejimində qərar qəbuletməni dəstəkləyən konseptual modelin işlənilməsini zəruri edir.

Bu baxımdan, rəqəmsal transformasiya şəraitində iqtisadi informasiya sistemlərinin kibertəhlükəsizliyinin təmini və onların funksional dayanıqlığının artırılması üçün inteqrasiya olunmuş, süni intellekt əsaslı konseptual modelin işlənilməsinə tələbat böyükdür. Rəqəmsal transformasiya mühitində bu modeli Şəkil 1-də göstərildiyi kimi konseptual sxem şəklində təklif etmək olar. Bu sxem ardıcıl məntiqi komponentlərdən – Sistemli yanaşma, Təhdid, Risk, Müdafiə, İdarəetmə, Dayanıqlıq, Monitorinq və Nəticə – ibarətdir. Bundan əlavə, sadalanan komponentlərin hər birinin özünə aid alt komponentləri də mövcuddur.



Şəkil 1. İqtisadi informasiya sistemlərinin kibertəhlükəsizliyinin təmin edilməsi və dayanıqlığının artırılması üzrə konseptual model

NƏTİCƏ

Rəqəmsal transformasiya iqtisadi informasiya sistemlərinin funksionallığını, çevikliyini və qərarvermə imkanlarını əhəmiyyətli dərəcədə genişləndirsə də, onların kibertəhlükəsizlik baxımından həssaslığını da artırır. Bulud texnologiyaları, böyük verilənlər, süni intellekt və inteqrasiya olunmuş platformalar məlumat axınını sürətləndirməklə yanaşı, məlumatların məxfiliyi, bütövlüyü və əlçatanlığı üçün yeni risklər yaradır. Bu baxımdan, iqtisadi informasiya sistemlərinin təhlükəsizliyi strateji idarəetmə, institusional davamlılıq və iqtisadi sabitlik məsələsinə çevrilmişdir.

Kibertəhlükəsizlik problemləri ilə bağlı risklər iqtisadi subyektlərin əməliyyat səmərəliliyini azaldır, maliyyə itkiləri yaradır, idarəetmə qərarlarının etibarlılığını zəiflədir və rəqəmsal iqtisadiyyatın inkişaf tempinə mənfi təsir göstərir. Buna görə də effektiv müdafiə modeli çoxsəviyyəli yanaşma tələb edir. Belə ki, iqtisadi informasiya sistemlərinin dayanıqlığının təmin edilməsi üçün proaktiv təhlükəsizlik siyasətinin formalaşdırılması, təhlükəsizlik mədəniyyətinin gücləndirilməsi və qabaqlayıcı nəzarət mexanizmlərinin tətbiqi vacibdir. Yalnız bu halda iqtisadi informasiya sistemləri rəqəmsal mühitdə səmərəli, təhlükəsiz fəaliyyət göstərə bilər və rəqəmsal iqtisadiyyatın davamlı inkişafına töhfə verə bilər.

İqtisadiyyatda kibertəhlükəsizlik problemləri mürəkkəb şəraitdə inkişaf edir və rəqəmsal transformasiya və iqtisadi qarşılıqlı asılılıq prosesləri ilə dərinləşir. Təhdidlərin müxtəlifliyi, sektora xas zəifliklər və əhəmiyyətli iqtisadi nəticələr həm birbaşa, həm də birbaşa və dolayı təsirləri nəzərə alan adaptiv, çoxsəviyyəli müdafiə strategiyalarına ehtiyac olduğunu göstərir. Süni intellekt kimi qabaqcıl texnologiyalar da yeni risklər və etik çətinliklər yaradır. Bu prosesdə dövlət-özəl tərəfdaşlığı və beynəlxalq əməkdaşlıq sistemli dayanıqlıq üçün vacibdir.

ƏDƏBİYYAT

[1] T.Shestakovska et al., "The role of business process ınnovation in sustainable economic growth: Integrating technology, efficiency, and

resilience", European Journal of Sustainable Development, 2025, 14(2), pp.823-840. DOİ: 10.14207/ejsd.2025.v14n2p823.

[2] A.Mahmoudi, "Cybersecurity challenges in Smart economies: Managing risks in a digital-first world", Dynamic and Safe Economy in the Age of Smart Technologies, 2025, 16 p. DOI: 10.4018/979-8-3693-4369-2.ch009

[3] Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası. Bakı, 28 avqust 2023. https://president.az/az/articles/view/60949

[4] S.Adam et al., "Cybersecurity and sustainable development – bibliometric study", Procedia Computer Science, 2025 (270), pp.5625–5633. DOİ:10.1016/j.procs.2025.10.031

[5] Z.Mamadiyarov, S.J.Khamdamov et al., "Cybersecurity challenges in the expanding digital economy", ACM International Conference Proceeding Series, 2025. DOI:10.1145/3726122.3726144

[6] V.Aggarwal, H.Gupta, "A comprehensive analysis of emerging threats in the digital era", 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO 2024), India 14-15 March 2024, pp.1613-1616.

[7] O.Astanakulov, M.E.Balbaa et al., "Exploring financial cybersecurity as the foundation of the digital economy: Challenges and prospects", Lecture Notes in Computer Science, 2025, vol.15554, pp.243–257.

[8] Global Cybersecurity Outlook 2026. 64 p. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.

[9] S.Saeed et al., "Digital transformation and cybersecurity challenges for businesses resilience: Issues and Recommendations", Sensors, 2023, 23, 6666. https://doi.org/10.3390/s23156666.

[10] H.Stewart, "Digital transformation security challenges", Journal of Computer Information Systems, 2023, 63(4), pp.919–936.

[11] H.Bouhafs, "Cybersecurity in the Digital era: Between digital transformation and protection challenges", Internatıonal Journal of Law: Law and World, 2025, №35, volume 11, Issue 3, pp.117-131. doi.https://doi.org/10.36475/11.3.8

[12] F.Fotis, "Economic ımpact of cyber attacks and effective cyber rısk management strategies: A light literature review and case study analysis", Procedia Computer Science, 2024. https://easychair.org/publications/preprint/vfks/open

[13] C.Hadnagy, "Social engineering: The science of human hacking", 2nd Edition, Wiley. 2018. https://doi.org/10.1002/9781119433729

[14] V.Krasnobayev et al., "Economic and cyber security: Collective monograph", PC Technology Center, Kharkiv. 2023. https://doi.org/10.15587/978-617-7319-98-5.

[15] A.M.Stanciu, "Emerging technologies in cybersecurity: Key concepts and future impact", 29th IEEE International Conference on Intelligent Engineering Systems, 2025. DOI:10.1109/INES67149.2025.11078213.

[16] V.Krasnobayev, A.Yanko, "Information security of the National economy is based on an effective data control method", Journal of International Commerce, Economics and Policy, 2023, vol.14(03), pp.1-25.

[17] A.G.Aliyev, R.O. Shahverdiyeva, "Some problems of the formation of the new generation digital economy based on artificial intelligence technologies", Informatica Economica journal, 2024, vol. 28, no. 3, pp.49-64.

[18] B.K.Gebremeskel, G.M.Jonathan et al., "Information security challenges during digital transformation", Procedia Computer Science, 2023, volume 219, pp.44–51. https://doi.org/10.1016/j.procs.2023.01.262

[19] N.Kasianova et al., "Cybersecurity as a catalyst for digital transformation and economic development: A fuzzy system dynamics approach, CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine. https://ceur-ws.org/Vol-4024/paper26.pdf

[20] A.G.Aliyev, R.O.Shahverdiyeva, "Scientific and methodological bases of complex assessment of threats and damage to information systems of the digital economy", International Journal Information Engineering and Electronic Business, 2022, №2, pp.23-38.

[21] Aliyev A.G., Shahverdiyeva R.O., "Management problems of information support of technical and economic systems based on artificial intelligence technologies", Advances in Transdisciplinary Engineering, 2024, volume 48, pp.193–204.

[22] M.Kianpour et al., "Systematically understanding cybersecurity economics: A survey", Sustainability, 2021, 13, 13677. https://doi.org/10.3390/su132413677.

[23] L.Abrardi, S.Comino et al., "The economics of cyber risk: A survey of the literature", Journal of Industrial and Business Economics, 2025. https://doi.org/10.1007/s40812-025-00370-3

[24] A.G.Aliyev, R.O.Shahverdiyeva, "Research and perspectives of new generation technological economic development problems on the Industry 4.0 platform", Informatica Economica, 2025, vol.29, no. 2, pp.32-44.

Cybersecurity Problems of Economic Information Systems in the Context of Digital Transformation

Roza Shahverdiyeva
Institute of Information Technology, Baku, Azerbaijan
shahverdiyevar@gmail.com

Abstract- The article classifies cyber threats and dangers of an economic nature, examines these threat types, and analyzes the relevant cybersecurity problems. The main artificial intelligence technologies applied in the cybersecurity of economic information systems are explained. A conceptual model for protecting and enhancing the resilience of economic information systems in the context of digital transformation is developed. Some recommendations are given on the analysis of cybersecurity problems of economic information systems and the prospective development directions of their solution.

Keywords- digital transformation of the economy; artificial intelligence technologies; Industry 4.0 platform; cyberthreats; economic information systems; cybersecurity.