Rəqəmsal İqtisadiyyatın Kiberdayanıqlığına Təsir Edən Təhdidlərin Analizi

Ələvsət Əliyev[1], Xəyalə Əbdülhüseynova[2]
[1,2] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*alovsat_qaraca@mail.ru* , [2]*abdulxayala@gmail.com*

***Xülasə*— Məqalədə rəqəmsal iqtisadiyyatda təhlükəsizlik trendləri, rəqəmsal iqtisadiyyatın informasiya təhlükəsizliyi və kiberdayanıqlığı məsələləri tədqiq edilmişdir. Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin funksional təyinatına görə təsnifatı verilmiş və konseptual struktur modeli işlənilmişdir. Rəqəmsal iqtisadiyyatın kiberdayanıqlığının təmin olunmasının təkmilləşdirilməsi aspektləri müəyyən olunmuşdur. Tədqiqat işində iqtisadi infrastrukturun və iqtisadi informasiya sistemlərinin kiberdayanıqlığı, qlobal təhlükəsizlik səviyyəsinin gücləndirilməsi üçün kompleks strateji yanaşmalar təklif olunmuş, rəqəmsal ekosistemin dayanıqlı inkişafı üçün təhlükəsizlik üzrə müdafiə mexanizmlərinin tətbiqinin zəruriliyi əsaslandırılmış və müvafiq tövsiyələr verilmişdir.**

Açar sözlər*— *rəqəmsal iqtisadiyyat; informasiya təhlükəsizliyi; iqtisadi təhlükəsizlik; kiberdayanıqlıq; süni intellekt texnologiyaları; kiber-təhdidlər.

I. GİRİŞ

Müasir dövrdə rəqəmsal transformasiya cəmiyyətin bütün sahələrini, o cümlədən iqtisadiyyatı əhatə edən və özünə böyük investisiyaları cəlb edən qlobal fenomenə çevrilmişdir. Rəqəmsal iqtisadiyyatın transformasiyası ənənəvi iqtisadiyyat yanaşmasından tam rəqəmsallaşdırılmış rəqəmsal biznes konsepsiyalarına keçid yoludur. İqtisadiyyatın rəqəmsal transformasiyasının sürətli inkişafında Süni İntellekt, Böyük Verilənlər (Big Data), Blokçeyn, Bulud Hesablamaları, Əşyaların İnterneti (IoT) kimi inkişaf etməkdə olan texnologiyaların rolu böyükdür. Bu texnologiyaların qarşılıqlı fəaliyyəti nəticəsində rəqəmsallaşma prosesinin yeni nəsli formalaşır və iqtisadiyyatda tətbiqlərinin miqyası genişlənir.

Artıq rəqəmsal iqtisadiyyat qlobal iqtisadi sistemin əsas komponentlərindən birinə çevrilmişdir. Rəqəmsal texnologiyaların sürətli inkişafı iqtisadi fəaliyyətin böyük hissəsinin müvafiq rəqəmsal platformalar üzərində həyata keçirilməsini vacib edir. Bu isə iqtisadi sistemlərin effektivliyini artırmaqla yanaşı, onların kiber məkanda müxtəlif təhlükələrə məruz qalma riskini yüksəldir və kibertəhlükələr qarşısında daha həssas edir.

Dünyada bir çox tədqiqatlar məhz iqtisadi sistemlərin kiberdayanıqlıq səviyyəsinin artmasına həsr olunmuşdur. Dünya İqtisadi Forumunun (2024) hesabatlarında qeyd edildiyi kimi, kiber-hücumların qaçınılmaz olduğu bir mühitdə əsas diqqət kiberdayanıqlıq (cyber resilience) konsepsiyasına yönəlməlidir. Bu yanaşma sistemin təkcə kiber-hücumdan qorunmasını deyil, həm də hücum zamanı əsas funksiyalarını davam etdirməsini və insidentdən sonra minimum itki ilə sürətlə bərpa olunmasını (proaktiv dayanıqlılıq) nəzərdə tutur.

Rəqəmsal iqtisadi sistemləri kiber-təhlükələrdən qorumaq, bu proseslərin dayanıqlılığını artırmaq üçün kiberdayanıqlığın səviyyəsinin yüksəlməsi müasir dövrdə aktual məsələdir. Tədqiqat işinin əsas obyekti də rəqəmsal transformasiya şəraitində formalaşan rəqəmsal iqtisadi ekosistem, habelə bu sistemin tərkib hissəsi olan mühüm informasiya infrastrukturları və iqtisadi subyektlərin qarşılıqlı fəaliyyət göstərdiyi kiber-fiziki mühitin təhlükəsizliyi və onun kiberdayanıqlığı təşkil edir. Bu işin predmeti isə rəqəmsal iqtisadi mühitdə yaranan kiber-təhlükələrin analizi, onların iqtisadi subyektlərə təsir mexanizmləri və sistemlərin kiberdayanıqlıq səviyyəsinin yüksəldilməsi üzrə yanaşmaların təhlilidir. Tədqiqatın aparılmasının əsas məqsədi aktual problem olan rəqəmsal iqtisadi sahələrdə kibertəhlükələri analiz etmək, bu təhlükələrin qarşısının alınması ilə yanaşı, sistemlərin kiber hücumlara qarşı dinamik müqavimət göstərə bilməsini, habelə neqativ təsirlərdən sonra funksional fəaliyyətini sürətlə bərpa etməsini təmin edən mövcud multidissiplinar yanaşmaların öyrənilməsi və onların tətbiqi üçün müvafiq tövsiyələrin hazırlanmasıdır.

II. RƏQƏMSAL İQTİSADİYYATIN İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ KİBERDAYANIQLIĞI

Müasir dövrdə biznesin sürətlə rəqəmsal mühitə keçməsi kibertəhlükəsizliyi rəqəmsal iqtisadiyyatın əsas hərəkətverici qüvvəsinə çevirib. Son illərin statistikası sübut edir ki, kibertəhlükəsizlik bazarındakı artım rəqəmsal iqtisadiyyatın ümumi həcminə birbaşa müsbət təsir göstərir [1].

Kibertəhlükəsizlik yalnız texniki sahə deyil, həm də iqtisadi və maliyyə sabitliyinin təməlini təşkil edir. Dünya İqtisadi Forumu (2024) kiber-riskləri ən böyük qlobal təhdidlərdən biri kimi tanıyır və qeyd edir ki, kibertəhlükəsizlik bazarı qlobal iqtisadiyyatın özündən daha sürətlə böyüməkdədir. Bu artım kiberhücumların həm sayının çoxalması, həm də onların daha mürəkkəb və təhlükəli xarakter alması ilə bağlıdır. Hazırda dünyadakı maliyyə əməliyyatlarının yarıdan çoxu rəqəmsal mühitdə baş tutur. Bu şəraitdə kiber-insidentlər sadəcə pul itkisinə deyil, həm də biznes fəaliyyətinin dayanmasına və maliyyə sistemlərinə olan inamın sarsılmasına, etimadın azalmasına yol açır [2].

Rəqəmsal iqtisadiyyatda kiberdayanıqlıq zərərli proqramların, fişinq fırıldaqlarının və haker hücumları kimi onlayn təhdidlərin qarşısının alınması üçün nəzərdə tutulur.

DOI: 10.25045/forensic.gov.2026.64

Tədqiqatlar göstərir ki, effektiv bir kibertəhlükəsizlik sistemi həm dövlət qurumları, həm də özəl müəssisələr üçün kiber təhdidlərin yarada biləcəyi iqtisadi itkiləri minimuma endirir.

Süni intellekt, bulud hesablamaları və blokçeyn texnologiyalarının geniş tətbiqi iqtisadi səmərəliliyi artırsa da, eyni zamanda yeni kiber-təhlükəsizlik halları da yaradır. İqtisadiyyatın rəqəmsallaşması virtual məkanda xidmətlərin sayını artırsa da, informasiya cəmiyyətinin İKT-dən asılılığını daha çox gücləndirir. Bu isə həm biznes, həm də fərdi həyatın mənfi xarici təsirlərə qarşı daha həssas olması ilə nəticələnir.

Müasir dövrün iqtisadi strukturları və prosesləri getdikcə daha mürəkkəb kibertəhlükələr ilə üzləşirlər və bu təhlükələrə qarşı ənənəvi təhlükəsizlik çərçivələri artıq kifayət qədər effektiv sayılmır. Mürəkkəbləşən kiber-təhdidlərin artması fonunda informasiya təhlükəsizliyinin əsas komponentləri olan konfidensiallıq, bütövlük və əlçatanlığın təmin edilməsi prosesləri effektivliyini itirməyə başlayır. İqtisadi proseslərdə kiber-təhlükələr zamanı kiber məkanda proseslərin fasiləsizliyini təmin etmək üçün kiberdayanıqlıq səviyyəsinin yüksəlməsinə ciddi diqqət yetirilməlidir. Bu sahədə ənənəvi modellər daha çox texniki mühafizəyə söykənsə də, müasir rəqəmsal ekosistem Kiberdayanıqlıq (cyber resilience) konsepsiyasına keçidin inkişafını sürətləndirmişdir. Bu yanaşma kiber-təhlükələr zamanı fasiləsizliyi təmin etmək üçün bir çox yeni mərhələləri 1) Qabaqlama - dəyişkən təhlükə mühitini öncədən hiss etmək; 2) Dözümlülük - təhlükələrə davam gətirmək üçün təşkilati güc və imkanların qurulması; 3) Bərpa - mərhələli düzəlişlər və bərpa müddətlərinə nəzarət olunması; 4) İnkişaf - baş verən təhlükələrdən, insidentlərdən və ətraf təsirlərdən sonra uyğunlaşma və dayanıqlıq gücünün artması [3] və s. özündə birləşdirir.

Bu aspektlər kiber-fiziki mühitdə yaranan təhlükələrə daha geniş - prosesin davamlılığı prizmasından yanaşır. Bu yanaşma yalnız texniki həllərlə məhdudlaşmır, həm də təşkilati strukturda və korporativ mühitdə köklü dəyişikliklərin edilməsini zəruri edir. Qeyd olunan bu mərhələlər (Qabaqlama, Dözümlülük, Bərpa və İnkişaf) kiberdayanıqlığın nəzəri çərçivəsini formalaşdırsa da, onların rəqəmsal iqtisadiyyatdakı effektivliyi konkret metodlar vasitəsilə qiymətləndirilir.

Nəticə etibarilə, informasiya təhlükəsizliyi və kiberdayanıqlığın bu metodoloji əsaslarla ölçülməsi, rəqəmsal iqtisadiyyat subyektləri üçün risklərin idarə edilməsində və investisiya qərarlarında mühüm rol oynayır. Rəqəmsal iqtisadiyyatın yeni sektorlarının formalaşması və rəqəmsal ekosistemin sürətli inkişafı, sosial-iqtisadi transformasiya nəticəsində toplanmış böyük həcmli rəqəmsal məlumatların itirilməsi, manipulyasiyası və ya sui-istifadəsi halları həndəsi silsilə üzrə artır. Müasir şəraitdə rəqəmsal iqtisadi sistemlərin təhlükəsiz fəaliyyətini təmin etmək yalnız mühafizə tədbiri deyil, həm də şirkətlərin strateji rəqabət üstünlüyü qazanması üçün fundamental şərtdir.

İqtisadiyyatın rəqəmsal transformasiyası şəraitində kibertəhlükəsizliyin əsas tendensiyaları və mövcud ekzogen-endogen problemlər kompleks şəkildə araşdırılmalıdır. Xüsusilə, insan və sosial amillərin həm təşkilati, həm də milli səviyyədə kiberdayanıqlığın (cyber resilience) formalaşmasına təsiri mexanizmləri analiz edilməlidir. İqtisadi sistemlərin kiberdayanıqlığı vahid mərkəzdən deyil, bir-birini tamamlayan üç ierarxik səviyyə üzərində qurulur (Cədvəl I.). Bu səviyyələrin hər biri fərqli iqtisadi risk qruplarını hədəfə alır:

- *Mikro səviyyə (Fərdi müəssisə müdafiəsi):* Fərdi müəssisə və təşkilatların daxili kiber-müdafiə sistemləri onların birbaşa qorunmasına yönəlir. EDR (Endpoint Detection and Response) sistemi hər bir kompüteri və cihazı real-vaxt rejimində monitorinq edərək, anomal davranışları saniyələr içində bloklayır. Bu zaman ZTA (Zero Trust) arxitekturası tətbiq edilir ki, bu da daxili şəbəkədə hər bir sorğunun təkrar yoxlanılmasını nəzərdə tutur. Məlumat sızmasının qarşısını alan DLP (Data Loss Prevention) sistemləri isə məxfi maliyyə sənədlərinin kənara icazəsiz çıxarılmasını qeyri-mümkün edir.
- *Mezo səviyyə (Sahəvi və regional şəbəkələr):* Sahəvi və regional rəqəmsal şəbəkələrin təhlükəsizliyi iqtisadi subyektlər arasındakı qarşılıqlı asılılığı nəzərə alır. Bu səviyyənin əsas funksiyası sistemdəki risklərin idarə olunmasıdır. Məlumat mübadiləsi və analiz mərkəzləri (ISACs) vasitəsilə banklar və digər strateji qurumlar baş vermiş kiberhücumlar barədə anonim məlumatları bölüşürlər; bu isə bir qurumda baş vermiş insidentin digərlərində təkrarlanmasının qarşısını almağa imkan verir. Müasir rəqəmsal texnologiyaları ilə regional rəqəmsal şəbəkələrdə tranzaksiyaların və log-faylların dəyişdirilməzliyi təmin oluna bilir. Bu daha çox iqtisadi şəbəkə daxilində şəffaflığı təmin edir.
- *Makro səviyyə (Milli və Beynəlxalq Strategiya):* Dövlətin ümumi rəqəmsal suverenliyini qoruyan bu səviyyə CERT/CSIRT (Kiber İnsidentlərə Qarşı Mübarizə Mərkəzləri) vasitəsilə milli kiber-ekosistemin fəaliyyətini tənzimləyir və hər bir sorğunun təkrar yoxlanılmasını nəzərdə tutur.

CƏDVƏL I. İQTİSADİ SİSTEMLƏRİN KİBERDAYANIQLIĞININ İERARXİK SƏVİYYƏLƏRİNƏ UYĞUN MÜDAFİƏ MEXANİZMLƏRİ

Səviyyə	**Təsir dairəsi**	**Tətbiq olunan texnoloji alətlər**	**İqtisadi hədəf**
Mikro (fərdi təşkilatlar)	Müəssisədaxili rəqəmsal resurslar, fərdi sənədlər və əməliyyat məlumatları	EDR, Zero Trust (ZTA), DLP	Birbaşa maliyyə itkilərinin qarşısının alınması və daxili dayanıqlıq.
Mezo (regional)	Sahəvi tranzaksiyalar, ortaq verilənlər bazaları və korporativ əlaqələr.	SOC, Blockchain, ISACs	Sistemli risklərin ("domino effekti") qarşısının alınması və dayanıqlıq.
Makro	Milli kritik infrastruktur, dövlət reyestrləri və iqtisadi suverenlik.	CERT/CSIRT,	Milli iqtisadiyyatın fasiləsizliyinin təmin edilməsi, qlobal rəqabət üstünlüyünün və dayanıqlığın qorunması..

Qeyd olunan mürəkkəb texnoloji sistemlərin (EDR, ZTA, SOC) mövcudluğu hələ tam kiberdayanıqlıq demək deyil. Rəqəmsal iqtisadiyyatda subyektlər şəbəkə daxilində bir-birinə

zəncirvari şəkildə bağlıdır. Bu inkişaf ilə fərdi təhlükəsizlik anlayışı arxa plana keçərək, yerini "sistemli kiber risk" reallığına verir. Bu o deməkdir ki, şəbəkənin hər hansı bir nöqtəsində baş verən kiçik sızma, bütün maliyyə sistemini iflic edə biləcək "domino effekti"nin yaranmasına səbəb olur [4]. Təcrübə göstərir ki, ən müasir texniki müdafiə sistemləri belə, istifadəçinin qeyri-düzgün qərarı nəticəsində səmərəsiz ola bilər. Buna görə də, kiberdayanıqlıq arxitekturasında texnoloji komponentlərdən sosial-təşkilati komponentlərə keçid zəruridir.

Kibertəhlükəsizlik sahəsindəki maneələrin analizi göstərir ki, kadr hazırlığının keyfiyyəti kiber-risklərin yaranma ehtimalı ilə tərs mütənasibdir. Bu, təkcə İT mütəxəssislərinə deyil, müəssisənin bütün əməkdaşlarına şamil olunur. Həmçinin işçilərin rəqəmsal savadlılıq səviyyəsi və onların düzgün idarə olunması kibertəhdidlərin baş vermə ehtimalına, eləcə də yayılma sürətinə birbaşa təsir göstərir.

Rəqəmsal təhdidlərin preventiv idarə olunması və onların neqativ iqtisadi təsirlərinin azaldılması məqsədilə təşkilati səviyyədə insan kapitalının aktivləşdirilməsi və kiber mədəniyyətinin yüksəldilməsi istiqamətində spesifik mexanizmlərin təhlili və tətbiqi [5] kibertəhlükələrin yayılma sürətini azaldır və iqtisadi subyektlərin rəqabət qabiliyyətini artırır.

III. RƏQƏMSAL İQTİSADİYYATIN KİBERDAYANIQLIĞINA TƏSİR EDƏN TƏHDİDLƏRİN TƏSNİFATI VƏ ANALİZİ

Rəqəmsal iqtisadiyyat İKT-nin geniş tətbiqi ilə xarakterizə olunur və bu proses yeni risklərin yaranmasına gətirib çıxarır. Aparılan tədqiqatlar göstərir ki, rəqəmsallaşma iqtisadi səmərəliliyi artırmaqla yanaşı, kibertəhlükələrin yaratdığı risklərin intensivliyini də yüksəldir [6]. Rəqəmsal ekosistemdə təhdidlərin artan çoxşaxəliliyi onların strukturlaşdırılmış şəkildə təhlilini və elmi əsaslandırılmış təsnifatını zəruri edir. Belə ki, kiberdayanıqlığa təsir edən təhdidlər texnoloji, insan amili, institusional və sistem xarakterli riskləri əhatə etməklə yanaşı, həm də daxili və xarici mənbələrdən qaynaqlana bilər. Bu təhdidlərin sistemli təsnifatı onların yaranma mexanizmlərinin, təsir sahələrinin və potensial nəticələrinin daha dərindən anlaşılmasına imkan yaradır.

Rəqəmsal iqtisadiyyatın kiberdayanıqlığı iqtisadi struktur və prosesləri əhatə edən rəqəmsal sistemlərin daxili və xarici hücumlara qarşı davamlılığı və bərpa olunma qabiliyyəti kimi müəyyən edilir [7]. Ona görə də kiber təhdidlərin təsnifatı çoxölçülü yanaşma tələb edir. Bu istiqamətdə rəqəmsal iqtisadiyyatın dayanıqlığı kompleks sistem kimi qiymətləndirilməlidir. Gələcək tədqiqatlar da maşın təlimi və süni intellekt əsaslı modellərə yönəlməlidir. Müasir təhdidlər daha çox adaptiv və çoxvektorlu xarakter daşıyır [8]. Aparılan təhlillər göstərir ki, kiber təhdidlər çoxparametrli və sistemlidir. Bunlar iqtisadi və texnoloji faktorların qarşılıqlı təsiri ilə formalaşır. Onlar dinamik və adaptiv xüsusiyyətlərə malikdirlər [7, 8]. Bu isə kiberdayanıqlığın təmin olunması üçün inteqrasiya olunmuş yanaşmaların vacibliyini göstərir.

Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin funksional təyinatına görə təsnifatını 1-ci şəkildəki kimi ifadə etmək olar.

Şəkil 1. Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin funksional təyinatına görə təsnifatı

Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin təsnifat metodologiyası: 1) sistem nəzəriyyəsi, 2)risk nəzəriyyəsi, 3)kompleks adaptiv sistemlər yanaşması, 4)kiber təhlükəsizlik modelləri və s. kimi nəzəri yanaşmalara əsaslanır. Bu yanaşmalar kiber təhdidlərin çoxsəviyyəli və qarşılıqlı əlaqəli xarakterini izah etməyə imkan verir [9].

Kibertəhdidlərin təsnifatı risklərin idarə olunmasında mühüm rol oynayır və bu təhdidləri anlamaq, eləcə də onlara reaksiya vermək üçün effektiv bir yanaşma təmin edir. Təhdidlərin təsnifatı kiberhücumun potensial təsirini anlamağa, təşkilatların qarşılaşdıqları riskləri azaltmağa kömək edir.

Akademik nəşrlərdə kiber təhdid anlayışı rəqəmsal aktivlərin konfidensiallığına, bütövlüyünə və əlçatanlığına qarşı yönəlmiş hər hansı potensial zərərli hadisə kimi xarakterizə olunur [10]. Müasir rəqəmsal iqtisadiyyat şəraitində bu təhdidlər sadəcə texniki boşluqlar deyil, həm də makroiqtisadi sabitliyi təhdid edən ciddi maliyyə riskləri kimi qəbul edilməlidir.

Təsnifat hər bir təhdid növü üzrə riskləri azaltmaq üçün tələb olunan müvafiq əks-tədbirləri müəyyən etməyə imkan verir. Bundan əlavə, rəqəmsallaşmış təşkilatları kiber təhdidlərdən qorumaq üçün istifadə olunan texniki, qeyri-texniki, təşkilati tədbirlər, habelə hüquqi və tənzimləyici mexanizmlər də tələb olunur. Həmçinin təşkilatlarda kibertəhdidlərin ən böyük çətinlik yaratmasının səbəbi onların sürətlə dəyişən təbiətidir ki, bu da ən son trendlər və texnologiyalarla hesablaşmağı çətinləşdirir.

Kiber təhdidlər əsasən dörd qrupda təsnif edilir:

1. Texniki təhdidlər (Sistemə birbaşa müdaxilə)

Zərərli proqramlar (Malware): Bura viruslar, soxulcanlar və xüsusilə son illər iqtisadi zərərinə görə fərqlənən Ransomware proqramları daxildir. Ransomware proqramı maliyyə qurumlarının məlumatlarını şifrələyərək onların fəaliyyətini dayandırır.

- DoS/DDoS hücumları: Şəbəkəni saxta sorğularla yükləyərək xidmətin göstərilməsini qeyri-mümkün edir.

- SQL inyeksiyası: Verilənlər bazasına sızıb müştəri məlumatlarını və gizli iqtisadi göstəriciləri oğurlamaq üçün istifadə olunur.

2. İnsan amilinə əsaslanan təhdidlər (Sosial mühəndislik)

- Fişinq (Phishing): İstifadəçiləri aldadaraq onlardan bank kartı məlumatlarını və ya giriş şifrələrini alaraq, kartlarından rahatlıqla istifadə edirlər.
- Spufinq (Spoofing): Özünü etibarlı bir tərəfdaş və ya rəsmi qurum kimi təqdim edərək iqtisadi əməliyyatları manipulyasiya məqsədilə istifadə olunur.

3. Daxili təhdidlər (Insider Threats)

Təşkilatın öz işçiləri və ya tərəfdaşları tərəfindən yaradılan təhdidlərdir. Bu, həm qəsdən, həm də ehtiyatsızlıqdan baş verə bilər.

4. Strateji və yeni nəsil təhdidlər

- APT (Advanced Persistent Threats): Hədəfə yönəlmiş, uzunmüddətli və gizli kiber-casusluq əməliyyatları.
- Tədarük zənciri hücumları: Şirkətin istifadə etdiyi proqram təminatı vasitəsilə sızmaların edilməsi [11].

Ən yaxşı kibertəhlükəsizlik tədbirlərinə baxmayaraq heç bir sistemin tam mükəmməl olmadığı qəbul edilir və qeyri-müəyyən risklər yalnız qorunmaya deyil, həm də kibertəhlükələrin aşkar edilməsi, onlara cavab verilməsi və bərpa olunmasına yönəlir. Bu yanaşma təkcə təhdidlərin təsirini əvvəlcədən nəzərə almağı deyil, həm də bərpa üçün güclü tədbirlərin hazırlanmasını əhatə edir. Buna görə də insidentlərə cavabvermə, biznes davamlılığı və fəlakətdən bərpa üçün güclü proses və protokolların qurulması dayanıqlı kibertəhlükəsizlik mövqeyi üçün vacibdir. Bundan əlavə, sosial mühəndislik hücumlarına qarşı insan faktorunun həssaslığı və kibertəhlükəsizlik üzrə maarifləndirmə və təlimlərin vacibliyi də xüsusi əhəmiyyət daşıyır.

Kibertəhlükəsizlik həmçinin təhdid kəşfiyyatının paylaşılması, davamlı monitorinq və effektiv insident cavabvermə imkanlarını birləşdirən kompleks yanaşmanı əhatə etməlidir. Bu yanaşma təşkilatlara kibertəhlükələri əvvəlcədən proqnozlaşdırmağa və insidentlər baş verdikdə sistemlərini effektiv şəkildə idarə etməyə imkan verir. Beləliklə, həm hadisədən əvvəl, həm də sonra rəqəmsal aktivlərin daha yaxşı qorunması və risklərin azaldılmasını onun kiberdayanıqlığı təmin edir.

IV. RƏQƏMSAL İQTİSADİYYATIN KİBERDAYANIQLIĞINA TƏSİR EDƏN TƏHDİDLƏRİN KONSEPTUAL STRUKTUR MODELİ

Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlər müasir iqtisadi sistemlərin sabitliyi və davamlı inkişafı baxımından strateji əhəmiyyət kəsb edən kompleks risklər toplusundan ibarətdir.

Rəqəmsal texnologiyaların, məlumat axınlarının və süni intellekt əsaslı qərar qəbuletmə mexanizmlərinin geniş tətbiqi iqtisadi fəaliyyətin səmərəliliyini artırmaqla yeni tip texnoloji, institusional və geosiyasi təhdidlərin formalaşmasına gətirib çıxarır. Bu təhdidlər yalnız informasiya təhlükəsizliyi ilə məhdudlaşmır. Eləcə də kritik infrastrukturun dayanıqlığına, iqtisadi və maliyyə sabitliyinə, eləcə də rəqəmsal mühitdə etimad və reputasiya sistemlərinə birbaşa təsir göstərir. Rəqəmsal iqtisadiyyatın kiberdayanıqlığının təmin edilməsi üçün təhdidlərin kompleks şəkildə identifikasiyası, sistemləşdirilməsi və qiymətləndirilməsi risklərin proqnozlaşdırılması və effektiv idarə olunması üçün metodoloji baza yaradır.

Yuxarıda qeyd olunanlar əsasında rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin konseptual konseptual struktur modelini 2-ci şəkildəki kimi vermək olar. Təklif olunan struktur sxem risklərin identifikasiyası, qiymətləndirilməsi və modelləşdirilməsi üçün analitik baza rolunu oynayır.

V. RƏQƏMSAL İQTİSADİYYATIN KİBERDAYANIQLIĞININ TƏMİN EDİLMƏSİNİN TƏKMİLLƏŞDİRİLMƏSİ ASPEKTLƏRİ

Məlumdur ki, transformasiyanın sürətlənməsi və proseslərə süni intellekt (Sİ) alətlərinin cəlb edilməsi kibertəhlükəsizlik risklərini artırır. Qlobal İnformasiya Təhlükəsizliyi Sorğusu (GISS) və Dünya İqtisadi Forumu (WEF) kimi təşkilatların hesabatlarına əsasən, dövlət və özəl sektor təşkilatlarının rəhbərlərinin 56%-dən çoxu yeni haker hücumlarına qarşı müdafiə sistemlərinin adekvatlığını qiymətləndirməkdə çətinlik çəkir. Hər iki sektorda kiberdayanıqlığın təmin edilməsi üçün aşağıdakı struktur komponentlərin (şəkil 3) qurulması mütləqdir:

- *Dizayn üzrə təhlükəsizlik (Security by Design - SbD).* Hər hansı bir təşkilatda sistemin, proqram təminatının və ya infrastrukturun yenilənməsi başlayırsa, ona həmin andan etibarən təhlükəsizlik tədbirləri daxil edilməlidir [12].
- *Kiber idarəetmə, risk və uyğunluq (GRC) proqramı.* Bu təşkilatın məlumat təhlükəsizliyini və rəqəmsal fəaliyyətini qanunvericilik tələbləri ilə uyğunlaşdıran, riskləri idarə edən vahid idarəetmə sistemidir. Dövlət təşkilatları yeni rəqəmsal xidmət yaratdıqda, GRC proqramı vasitəsilə həmin xidmətin təhlükəsizliyini yoxlayır, ISO 27001 standartına uyğun sistem qurur və vətəndaşların məlumatlarının GDPR-a uyğun olaraq sızmasının qarşısını alır [13].
- *Sosial-təşkilati inteqrasiya.* Bu yanaşmanın məqsədi təşkilatda kibertəhlükəsizliyin təmin edilməsi yalnız texniki mütəxəssislərin deyil, həm də bütün işçilərin ortaq məsuliyyətinə çevrilməsidir [14]. Bu yanaşma çərçivəsində işçilərin rəqəmsal savadlılıq səviyyəsi artırılır və onlar kiberhücumlara qarşı hazır olurlar.

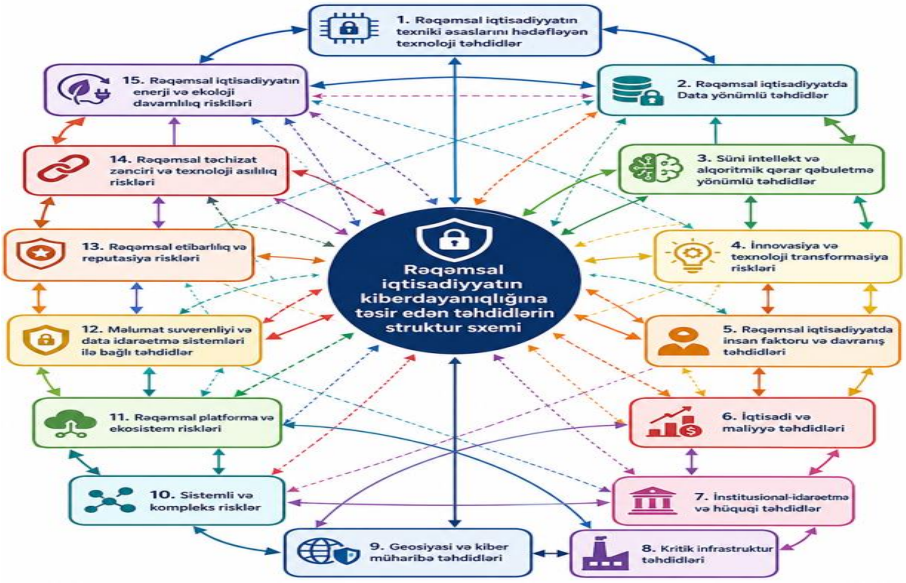
Məlumdur ki, informasiya texnologiyaları və sənaye idarəetmə sistemləri artıq bir çox sahələrdə əvəzolunmaz alətlərə çevrilmişdir. Hazırda dövlət üçün vacib olan infrastruktur sistemlərinin texnologiyalardan asılılığı artmaqdadır. Kiber məkanda müxtəlif zərərli qruplar dövlət təşkilatlarını daha çox kiber hücumlara məruz qoyur.

- *Dövlət sektorunda rəqəmsal risklər.* Təşkilatlarda işləri daha sürətlə rəqəmsallaşdırmaq istəyi bəzən təşkilatları təhlükəsizlik problemləri ilə üz-üzə qoyur. Bu boşluq məhz dövlət təşkilatlarında kiberhücumların artmasına səbəb olur. Dövlət təşkilatlarının əsas işi vətəndaşların

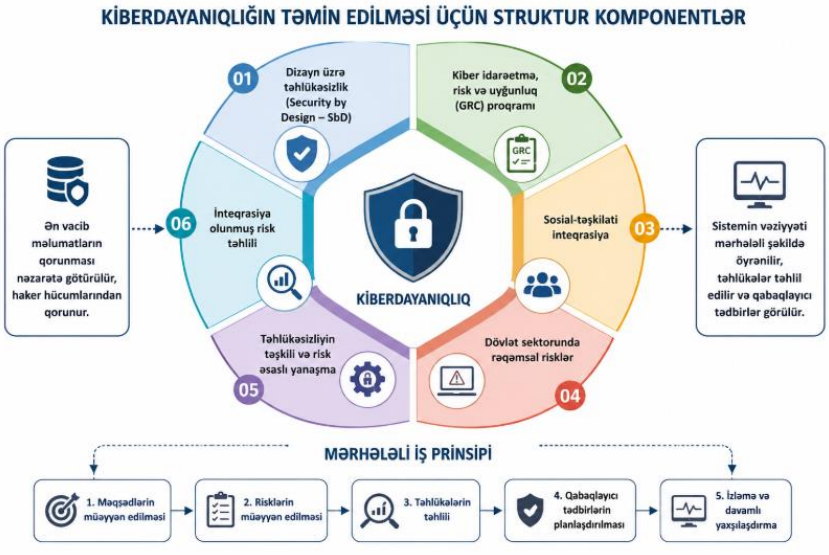
etimadını qazanmaq prinsipləri üzərində qurulur [13]. Bu etimadı qorumaq üçün məlumatların gizliliyi və sistemlərin fasiləsiz işləməsi təmin edilməlidir. Buna görə də kiberhücumlar dövlət sektoru üçün çox ciddi kibertəhdiddir.

- *Təhlükəsizliyin təşkili və risk əsaslı yanaşma.* Təşkilatlar kibertəhlükəsizliyi işin ilkin mərhələsində düşünməlidirlər. Bunun üçün bütün layihələrdə kibertəhlükəsizlik prinsipləri əsas götürülən idarəetmə proqramları tətbiq edilməlidir.
- *İnteqrasiya olunmuş risk təhlili.* Heç bir halda rəqəmsallaşmış təşkilatlar kiberhücumlardan tam sığortalana bilmir. Lakin güclü müdafiə sisteminə malik olan və riskləri düzgün qiymətləndirən qurumlar daha dözümlü və rəqabətqabiliyyətli olur. Təşkilatlar kiberhücumların qarşısını almaq üçün ən vacib məlumatların qorunmasını nəzarətə götürür, həmin məlumatları haker hücumlarından qoruyur [15]. Həmçinin mərhələli iş prinsipi ilə sistemin vəziyyətini öyrənir, təhlükələri təhlil edir və qabaqlayıcı tədbirlərin görülməsini vacib bilir.

Kibertəhlükəsizliyə risk əsaslı yanaşma təşkilatlara yüksək dəyərli informasiya aktivlərinin qorunmasına və ən çox təsir göstərən risklərin azaldılmasına diqqət yetirməyə, bununla da hücum səthini azaltmağa imkan verir. Dövlət təşkilatları kiberhücumların təsirini azaltmaq üçün xüsusi kibertəhlükəsizlik tədbirləri həyata keçirir. Bu məqsədlə sistemdəki boşluqlar yoxlanılır və sızma testlərinin həyata keçirilməsi kimi texniki addımlar atılır.



Şəkil 2. Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin konseptual struktur modeli



Şəkil 3. Rəqəmsal iqtisadiyyatın kiberdayanıqlığının təmininin struktur komponentləri

NƏTİCƏ

Müasir dövrdə rəqəmsal iqtisadiyyatın dayanıqlı inkişafı kiberdayanıqlığın təmin olunması ilə birbaşa bağlıdır. Rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən təhdidlərin analizi göstərir ki, kiber-mühafizə dövlətin strateji iqtisadi təhlükəsizliyinin əsas istiqamətlərindən biridir.

Aparılmış təhlillər göstərir ki, rəqəmsal iqtisadiyyatın formalaşdırdığı mürəkkəb mühit texnoloji, təşkilati, iqtisadi, hüquqi və sosial xarakterli çoxşaxəli təhdidlərin təsirinə məruz qalır. Kibertəhlükələr informasiya sistemlərinin texniki tamlığını pozmaqla yanaşı, eyni zamanda dövlət idarəçiliyinin, biznes proseslərinin, maliyyə institutlarının, kritik infrastrukturun və cəmiyyətin rəqəmsal etimad mühitinin sabitliyinə ciddi təsir göstərir.

Tədqiqatın nəticələri göstərir ki, rəqəmsal iqtisadiyyatın kiberdayanıqlığına təsir edən əsas risk faktorları sırasında kibercinayətkarlıq, məlumat sızmaları, kritik infrastruktur obyektlərinə yönəlmiş hücumlar, süni intellekt əsaslı manipulyasiya vasitələri, insan amili, proqram təminatındakı zəifliklər, geosiyasi kibermünaqişələr və normativ-hüquqi mexanizmlərin yetərsizliyi xüsusi yer tutur. Bu təhdidlərin dinamik və adaptiv xarakter daşıması ənənəvi təhlükəsizlik yanaşmalarının effektivliyini azaldır və qabaqlayıcı, çevik və inteqrasiya olunmuş təhlükəsizlik mexanizmlərinin tətbiqini zəruri edir.

Müəyyən edilmişdir ki, rəqəmsal iqtisadiyyatın kiberdayanıqlığının yüksəldilməsi yalnız texniki müdafiə vasitələrinin tətbiqi ilə məhdudlaşmamalı, eyni zamanda institusional idarəetmənin təkmilləşdirilməsi, beynəlxalq əməkdaşlığın genişləndirilməsi, rəqəmsal savadlılığın artırılması, risklərin proqnozlaşdırılması və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması ilə kompleks şəkildə həyata keçirilməlidir. Bununla yanaşı, süni intellekt, böyük verilənlər analitikası, blokçeyn və adaptiv təhlükəsizlik platformaları kimi innovativ texnologiyaların tətbiqi kiberdayanıqlığın gücləndirilməsində mühüm strateji alət kimi çıxış edir.

Rəqəmsal iqtisadiyyatın təhlükəsiz və davamlı inkişafının təmin olunması üçün kibertəhlükələrin sistemli şəkildə qiymətləndirilməsi, onların qarşılıqlı təsir mexanizmlərinin öyrənilməsi və çoxsəviyyəli müdafiə strategiyalarının formalaşdırılması prioritet istiqamətlərdən biri hesab edilməlidir. Bu yanaşma rəqəmsal transformasiya proseslərinin dayanıqlığını artırmaqla yanaşı, milli iqtisadi ekosistemin qlobal rəqabətədavamlılığını təmin edəcək, təhlükəsizliyin və rəqəmsal suverenliyin qorunmasına da mühüm töhfə verəcəkdir.

ƏDƏBİYYAT

[1] R. Alshahrani, M. Yenugula, H. Algethami, F. Alharbi, S. S. Goswami, Q. N. Naveed, and S. Zahmatkesh, "Establishing the fuzzy integrated hybrid MCDM framework to identify the key barriers to implementing artificial intelligence-enabled sustainable cloud system in an IT industry," Expert Systems with Applications, vol. 238, p. 121732, 2024.

[2] A. Valackienė and R. O. Odejayi, "The impact of cyber security management on the digital economy: multiple case study analysis," Intellectual Economics, vol. 18, no. 2, pp. 261–283, 2024.

[3] J. Zuo, Z. Guo, J. Gan, and Y. Lu, "Enhancing continuous service of information systems based on cyber resilience," in 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), IEEE, 2021, pp. 535–542.

[4] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," ACM Computing Surveys, vol. 55, no. 14s, pp. 1–40, 2023.

[5] H. Bei, "Problems of cybersecurity in the context of becoming and development of the new economy," Competitivitatea şi inovarea în economia cunoaşterii, pp. 438–448, 2019.

[6] D. Lesmana, M. Afifuddin, and A. Adriyanto, "Challenges and cybersecurity threats in digital economic transformation," International Journal of Humanities, Education and Social Sciences, vol. 2, 2023.

[7] Q. Zhu, "Foundations of cyber resilience: The confluence of game, control, and learning theories," in Cyber Resilience: Applied Perspectives, Springer Nature Switzerland, 2025, pp. 27–58.

[8] K. Singh, S. Chatterjee, M. Mariani, and S. F. Wamba, "Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment," Technovation, vol. 143, p. 103219, 2025.

[9] M. Segovia-Ferreira, J. Rubio-Hernan, A. Cavalli, and J. Garcia-Alfaro, "A survey on cyber-resilience approaches for cyber-physical systems," ACM Computing Surveys, vol. 56, no. 8, pp. 1–37, 2024.

[10] S. J. Shackelford, A. A. Proia, B. Martell, and A. N. Craig, "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices," Texas International Law Journal, vol. 50, p. 305, 2015.

[11] N. Mohamed, "State-of-the-art in Chinese APT attack and using threat intelligence for detection: A survey," Journal of Positive School Psychology, vol. 6, no. 5, 2022.

[12] S. Jain, "Integrating privacy by design: Enhancing cybersecurity practices in software development," Journal of Multidisciplinary, vol. 4, no. 11, pp. 1–11, 2024.

[13] E. A. Odedina, "Redefining governance, risk, and compliance (GRC) in the digital age: Integrating AI-driven risk management frameworks," World Journal of Advanced Engineering Technology and Sciences, vol. 10, no. 1, pp. 264–282, 2023.

[14] H. Taherdoost, "Towards an innovative model for cybersecurity awareness training," Information, vol. 15, no. 9, p. 512, 2024.

[15] S. Oparin, "Digital integration of the entity's risk management with strategy and business performance," in International Scientific Siberian Transport Forum, Springer International Publishing, 2021, pp. 221–229.

Analysis of Threats Affecting the Cyber Resilience of the Digital Economy

Alovsat Aliyev[1], Khayala Abdulhuseynova[2]

[1,2] Institute of Information Technology, Baku, Azerbaijan

[1]alovsat_qaraca@mail.ru, [2]abdulxayala@gmail.com

Abstract- The article studies security trends in the digital economy, information security, and cyber resilience issues of the digital economy. A classification of threats affecting the cyber resilience of the digital economy based on their functional purpose is provided, and a conceptual structural model has been developed. The aspects for improving the provision of cyber resilience in the digital economy are identified. The paper proposes comprehensive strategic approaches to strengthen the global security level of economic infrastructure, substantiates the necessity of implementing security defense mechanisms for the sustainable development of the digital ecosystem, and provides relevant recommendations.

Keywords- digital economy; information security; economic security; cyber resilience; Artificial Intelligence technologies; cyber threats.