[3] Garcia, Maria. "Understanding the Concept of Capitulation Theory in Information Security." International Conference on Cybersecurity, 2021.
[4] Wang, Li. "User Compliance with Information Security Policies: A Review." Journal of Computer Security, vol. 25, no. 4, 2024, pp. 78-94.
[5] Brown, David. "Human Factor in Information Security: Challenges and Solutions." Annual Conference on Cybersecurity, 2023

KİBERFİZİKİ SİSTEMLƏR ÜÇÜN SÜNİ İNTELLEKTƏ ƏSASLANAN KİBERTƏHLÜKƏSİZLİK

Abdullayeva Ölkə
Rəhimova Nazilə
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə
Bu məqalədə kiber – fiziki sistemlər, bu sistemlərdə baş verə biləcək kibertəhlükələr və bu təhlükələrin aradan qaldırılması haqqında danışılmışdır. Eyni zamanda kiber – fiziki sistemlərdə kibertəhlükəsizliyin təmin olunması üçün süni intellektdən istifadə qaydalarından da bəhs olunub.
Açar sözlər: kiber – fiziki sistemlər, kibertəhlükəsizlik, süni intellekt.

Məqsəd
Məqalədə əsas məqsəd kiberfiziki sistemlərdə yarana biləcək kibertəhlükələri aradan qaldırmaq üçün süni intellekt sistemlərindən istifadənin rolu və əhəmiyyətini aşkara çıxarmaqdır. Süni intellekt texnologiyalarından istifadə etməklə istənilən sahədə yarana biləcək kibertəhlükələri aradan qaldıra bilərik.

Giriş.
Kiber-Fiziki Sistemlər (CPS) fiziki sistemlərdən (hardware), proqram sistemlərindən və potensial olaraq digər sistem növlərindən (məsələn, insan sistemləri) ibarət sistemlərdir. Bunlar bəzi qlobal davranışları təmin etmək üçün yaxından inteqrasiya olunur və şəbəkələşir. Buna görə də, bu sistemlər çox vaxt real dünya ilə, eləcə də mürəkkəb proqram elementləri ilə qarşılıqlı əlaqədə olan sensorlar, aktuatorlar və oxşar quraşdırılmış sistemlər kimi avadanlıqları əhatə edir. Kiber – fiziki sistemlərə kənd təsərrüfatı, nəqliyyat, ev avtomatlaşdırılması, səhiyyə, enerji və bir çox digər sosial əhəmiyyətli sahələrdə rast gələ bilərik. [2]
Kiber – fiziki sistemlər əhəmiyyətli sosial faydalar əldə etmək potensialına malikdir və buna görə də ardıcıl və etibarlı fövqəladə davranışları təmin edən təhlükəsiz sistemləri layihələndirmək və qura bilmək vacibdir. Robotlar, ağıllı binalar, implantasiya edilə bilən tibbi cihazlar, özlərini idarə edən avtomobillər və ya idarə olunan hava məkanında avtomatik uçan təyyarələr - bütün bunlar CPS-in nümunələridir. [5,7]
Kiber – fiziki sistemlər istehsal sənayesində bütün istehsal prosesini avtomatlaşdırmaqla, bütün fabriklər üçün vahid mərkəzləşdirilməmiş platforma yaratmaqla prosesləri optimallaşdırmaq üçün istifadə oluna bilər. İstehsalda avtomatlaşdırma əmək və material xərclərinə qənaət edir və istehsal vaxtını azaldır.
Kiberfiziki sistemlər geniş çeşiddə müxtəliflik nümayiş etdirir. Variasiyaların geniş diapazonuna görə, modeli öyrətmək üçün xüsusi məlumat dəstlərindən istifadə etmək lazımdır. Funksional kiberfiziki sistemə hücumlar vasitəsilə verilənlər bazası yaratmaq mümkün deyil. [6]
Son günlərdə kiber-fiziki sistemlər (CPS) çox mürəkkəb, daha mürəkkəb, ağıllı və avtonom hala gəlib. CPS nümunələrinə enerji sektorunda ağıllı şəbəkə, ağıllı fabrik və sənaye 4.0, intellektual nəqliyyat sistemləri, səhiyyə və tibb sistemləri və robot sistemləri daxildir. CPS-lər heterojen kiber və fiziki komponentlər arasında çox mürəkkəb qarşılıqlı əlaqə təklif edir; bu mürəkkəbliyə əlavə olaraq, davranışlarının proqnozlaşdırılmasını aid etmək olar. Bu arada, CPS üçün kibertəhlükəsizlik həm

sənayedə, həm də akademik sahədə tədqiqatçı alimlərin diqqətini cəlb edir, çünki kiberhücumların sayı durmadan artmaqdadır və onların davranışları daha mürəkkəbləşib. Bu mürəkkəblik isə adətən "sıfır gün (zero-day)" təhdidləri kimi tanınır.[5]

Müdaxilənin aşkarlanması və qarşısının alınması sistemləri (IDS/IPS) və girişə nəzarət kimi adi kibertəhlükəsizlik mexanizmləri bu kateqoriya kiberhücumları aşkar etmək, qarşısını almaq və bloklamaq qabiliyyətinə malik deyil, çünki sıfır gün təhlükələri naməlum səhv davranış nümayiş etdirir. Son zamanlarda CPS-ləri sıfır gün hücumlarından qorumaq üçün süni intellektə (AI) əsaslanan kibertəhlükəsizlik mexanizmlərinin yeni dövrü inkişaf mərhələsindədir. Kibertəhlükəsizlik kontekstində maşın öyrənmə texnologiyaları avtomatik olaraq müxtəlif hücum patentləri yaratmaq və beləliklə də gələcək təcavüzkarların yanlış davranışlarını dəqiq proqnozlaşdırmaq məqsədi ilə müxtəlif məlumat mənbələrindən gələn çoxlu sayda heterojen məlumatları idarə etmək üçün istifadə olunur. Oyun-nəzəri yanaşmalar kibermüdafiə kontekstində qərar qəbul etmə (yəni, şübhəli cihazın hücumçu olub-olmaması) və hücumun proqnozlaşdırılması məsələlərini həll etmək üçün istifadə edilmişdir. [7]

Sıfır gün hücumlarının qarşısının alınması müxtəlif süni intellekt sistemləri, o cümlədən maşın öyrənməsi və oyun nəzəriyyəsi, eləcə də təhlükəsizlik üzrə ekspert müdaxiləsi arasında əməkdaşlıq tələb edir. Əslində, qərar qəbul etmə prosesinə insanın müdaxiləsi hücumun aşkarlanmasının yaxşılaşmasına səbəb olur, çünki insan-maşın qarşılıqlı əlaqəsinin məqsədi yanlış pozitivlərin sayını azaltmaqdır.

Kibertəhlükəsizlik kompüterlərin, serverlərin, mobil cihazların, elektron sistemlərin, şəbəkələrin və məlumatların zərərli hücumlardan müdafiə təcrübəsidir. O, həmçinin informasiya texnologiyaları təhlükəsizliyi və ya elektron informasiya təhlükəsizliyi kimi də tanınır. [1,3]

"Kibertəhlükəsizlik" termini biznesdən tutmuş mobil hesablamaya qədər müxtəlif kontekstlərdə tətbiq edilir və bir neçə ümumi kateqoriyaya bölünə bilər. [1]

- Şəbəkə təhlükəsizliyi – kompüter şəbəkəsini təcavüzkarlardan və ya fürsətçi zərərli proqramlardan qorumaq təcrübəsidir.
- Tətbiq təhlükəsizliyi – proqram təminatının və cihazların təhlükələrdən azad olmasına diqqət yetirir.
- İnformasiya təhlükəsizliyi – həm saxlama, həm də tranzit zamanı məlumatların bütövlüyünü və məxfiliyini qoruyur.
- Əməliyyat təhlükəsizliyi – məlumat aktivlərinin idarə edilməsi və qorunması üçün prosesləri və qərarları əhatə edir.

Kibertəhlükəsizliyin əhəmiyyəti hər gün artmağa davam edir. Son illərdə baş verən kiberhücumlardan sonra hökumətlər bir sıra qaydalar tətbiq ediblər. Texnologiyanın və rəqəmsallaşmanın inkişafı kiber hücumçuların istifadə edə biləcəyi yeni boşluqların yaranmasına səbəb olub. Enerji paylayıcı şəbəkələr və su infrastrukturu kimi obyektlərin rəqəmsallaşdırılması onların səmərəliliyini artırıb və bununla da dövlətlərə və cəmiyyətə fayda verib.

Kiberhücumların bütün formaları zərərli olsa da, kritik kiberfiziki sistemləri hədəfə almaq yüksək səviyyəli təhlükə yaradır. Bu hücumlar ictimai quruluşu pozmaq və insan həyatı üçün təhlükə yaratmaq potensialına malikdir. Bu obyektlərin təhlükəsizliyini təmin etmək üçün müxtəlif texnikalardan istifadə edilir ki, bu da son dərəcə vacibdir. [3]

Kibertəhlükəsizlikdə süni intellektdən istifadə

Süni intellekt (AI) artıq iqtisadiyyatımızı və cəmiyyətimizi dəyişdirir və artan süni intellekt qərar qəbulu potensial zərərlər və süni intellekt qərarlarının daha şəffaf verilməsi zərurəti ilə bağlı müzakirələrə səbəb olub . Süni intellekt vasitəsilə motivasiya, emosiya, şəxsiyyət və digər müvafiq aspektləri özündə birləşdirən, həqiqətən də ağıllı insana bənzər performansı təmsil edən koqnitiv arxitekturalar yaratmaq mümkündür . [5,6]

Süni intellekt üsulları və onların yerləşdirildiyi vasitələr virtual istehsalçının fəaliyyət göstərdiyi cihazın əsasını təşkil edir, İstehsalı təşkil edən aspektlər (texnoloji resurslar, təşkilat və s.) ümumi arxitekturada birləşərək kiberfiziki sistemdə sənayeləşmiş elementin əsasını təşkil edir.

CPS şəbəkələrinin təhlükəsizliyini təmin etmək bu şəbəkə sistemlərinin unikal mürəkkəbliyi və çətinlikləri daha mürəkkəb anlayışdır. CPS cihazlarının məhdud hesablama gücü bunun bir nümunəsidir. Təhlükəsizlik sistemləri bütün mövcud resursları tükətmədən ciddi məhdudiyyətlər daxilində səmərəli və effektiv işləməlidir. Bu səbəbdən, fərdiləşdirilmiş təhlükəsizlik həllərinin inkişafı ilə bağlı CPS dizaynını, xüsusi tətbiqləri və təhlükəsizlik problemlərini düzgün araşdırmaq vacibdir. [10]
Kibertəhlükəsizliyi təmin etmək üçün süni intellekt ilk növbədə davranış nümunələrini izləyir və təhlil edir. Baza yaratmaq üçün bu nümunələrdən istifadə edərək, AI qeyri-adi davranışları aşkarlaya və sistemlərə icazəsiz girişi məhdudlaşdıra bilər. Süni intellekt həmçinin riski prioritetləşdirməyə, zərərli proqram və müdaxilə imkanlarını başlamazdan əvvəl dərhal aşkar etməyə kömək edə bilər.

Süni intellektin kibertəhlükəsizliyə tətbiqi

Süni intellekt real vaxt rejimində kibertəhlükələri izləyə, təhlil edə və onlara cavab verə bilər. Süni intellekt alqoritmləri kiber təhlükənin göstəricisi olan nümunələri aşkar etmək üçün böyük həcmdə məlumatı təhlil etdikcə, o, həmçinin ümumi kiberhücum növlərinin qarşısını almaq üçün bütün şəbəkəni zəifliklər üçün skan edə bilər.
Düzgün tətbiq edildikdə, AI təkrarlanan tapşırıqları avtomatlaşdıraraq işçilərin vaxtını və resurslarını azad edən təhlükəsizlik avtomatlaşdırılması üçün mühərrik rolunu oynaya bilər. Süni intellekt həmçinin insanları bir vəzifədən və ya prosesdən kənarlaşdırmaqla insan səhvlərinin baş verməsini azalda bilər. [6]

AI kibertəhlükəsizliyi fərqi

Süni intellektlə kibertəhlükəsizliyin qorunması heç vaxt təhlükəsizlik mütəxəssislərini tam əvəz etməyəcək, çünki iş yerində yaradıcı problemlərin həllinə və daha mürəkkəb problemlərə həmişə ehtiyac olacaq. Bununla belə, süni intellekt böyük həcmdə məlumatı təhlil edərək, nümunələri tanıyaraq və böyük həcmdə təhlükəsizlik məlumatlarına əsaslanaraq anlayışlar yaratmaqla insan təhlükəsizliyi mütəxəssislərinə kömək edə bilər və artıq edir. Bunun ənənəvi təhlükəsizlik prosesləri ilə tamamlanması saatlar, bəzən həftələr çəkə bilər.
Süni intellektdən əvvəl təhlükəsizlik mütəxəssisləri potensial kibertəhlükələri müəyyən etmək üçün imza əsaslı aşkarlama alətləri və sistemlərindən istifadə edirdilər. Bu təhlükəsizlik alətləri daxil olan şəbəkə trafikini məlum təhlükələrin və ya zərərli kod imzalarının verilənlər bazası ilə müqayisə edir. Aşkar edildikdə, sistem xəbərdarlıq verir və təhlükəsizlik mütəxəssisinə təhlükənin qarşısını almaq və ya karantinə almaq üçün tədbir görməyi təklif edir. [5]
Bu imza əsaslı təhlükəsizlik yanaşması məlum təhdidlərə qarşı kifayət qədər effektiv olmuşdur. Bununla belə, imzaya əsaslanan aşkarlama yanaşmasının yeni (Zero-Day) və ya naməlum təhlükələrə qarşı qeyri-adekvat olduğu sübut edilmişdir. Çox tez-tez bu alətlər, həmçinin təhlükəsizlik mütəxəssislərini "vəhşi qaz təqibinə" göndərən yalan pozitivlərin daha yüksək tezliyi ilə nəticələndi.
Ənənəvi kibertəhlükəsizlik də əsasən əl analizinə əsaslanır. Təhlükəsizlik analitikləri potensial təhlükəsizlik pozuntusunun göstəriciləri kimi xidmət edən hər hansı müəyyən edilə bilən nümunələri axtarmaq üçün təhlükəsizlik xəbərdarlıqlarını və hadisə qeydlərini əl ilə araşdırmalıdırlar. Qeydləri və hadisələri araşdırmaq çox vaxt apara bilər və yalnız bir təhlükəsizlik analitikinə etibar etmək şirkətlərin edə bilməyəcəyi bir səhvdir.
Süni intellekt ənənəvi kibertəhlükəsizliyin bu çatışmazlıqlarını və daha çoxunu aradan qaldırmaq gücünə malikdir. Bu texnologiya inkişaf etməyə davam etdikcə kibertəhlükəsizlik proseslərinə və insanlara böyük təsir göstərəcək.

Kibertəhlükəsizlikdə AI vacibliyi

Kiber cinayət təşkilatları təşkilatlara qarşı irimiqyaslı, məqsədyönlü kiberhücumlar həyata keçirmək üçün artıq maşın öyrənməsi, avtomatlaşdırma və süni intellektə sərmayə qoyublar. Təhdidlərin sayı və şəbəkələrə təsir edən ransomware potensialı artmaqda davam edir.
Süni intellekt və maşın öyrənməsi böyük həcmdə məlumatı emal etməklə, təhlil əsasında sürətli fikirlər təqdim etməklə və gündəlik təhlükəsizlik xəbərdarlığı və yalan pozitiv səs-küyü aradan qaldırmaqla

təhlükəsizlik analitiklərinə oyun sahəsini bərabərləşdirməyə kömək edir. Bu isə öz növbəsində, komandanın səmərəliliyini və məhsuldarlığını əhəmiyyətli dərəcədə yaxşılaşdırır və onlara potensial kibercinayətkarlar üzərində üstünlük verir. [8,9]

Polimorfik zərərli proqramlar, skriptlər və "yerdən kənarda yaşamaq" adlanan hücumlar kimi daha mürəkkəb hücum vektorlarının artması ilə kibercinayətkarlar üçün ənənəvi, fayl skanına əsaslanan antivirus müdafiəsini keçmək asanlaşdı. Zərərli proqramların bu təkamülündən qorunmaq üçün davranış təhlili kimi daha müasir yanaşmalar kibertəhlükəsizlikdə daha populyarlaşır. Davranış təhlili və aşkarlama yanaşmaları güclüdür, çünki bütün zərərli proqramlar nəticədə uğur qazanmaq üçün zərərli davranış nümayiş etdirməlidir. Süni intellekt düzgün layihələndirildikdə, bu zərərli davranışları insanlardan daha sürətli izləyə, onları aşkar edə və onlara cavab vermək qabiliyyətinə malik olacaq

Kibertəhlükəsizlikdə AI-nin üstünlükləri

Bugünkü AI sistemləri potensial kibertəhlükələri aşkar etmək, yeni hücum vektorlarını müəyyən etmək və şirkətlərin həssas məlumatlarını qorumaq üçün öyrədilir. Süni intellektlə idarə olunan kibertəhlükəsizlik alətlərindən istifadənin üç əsas faydasına aşağıdakılar daxildir: [5]

1. Böyük həcmli məlumatların sürətlə təhlili
2. Anomaliyaların və zəifliklərin aşkarlanması
3. Təkrarlanan proseslərin avtomatlaşdırılması

Kibertəhlükəsizlikdə süni intellektdən istifadə potensialı demək olar ki, sonsuzdur. Təhdidin aşkarlanması və cavab reaksiyasının sürəti və dəqiqliyi real vaxta mümkün qədər yaxındır. Süni intellekt mümkün qədər tez bir zamanda təhlükəsizlik komandasına şübhəli davranışı qeyd etməklə, ransomware hücumunun təsirini minimuma endirməyə kömək edə bilər. Və nəhayət, süni intellekt avtomatlaşdırma vasitəsilə kibertəhlükəsizlik əməliyyatlarını daha səmərəli edir, təhlükəsizlik komandasının qiymətli vaxtını və resurslarını digər, daha vacib vəzifələr üzərində işləmək üçün azad edir.

Kibertəhlükəsizlikdə AI-nin riskləri

Bir texnologiya olaraq AI-nin hələ ilk günlərində olduğunu xatırlamaq vacibdir. Süni intellekt hələ də insan müdaxiləsini tələb edir, təkcə süni intellekt mühərriklərini öyrətmək üçün deyil, həm də mühərrik səhv olarsa işə qarışmaq üçün insan müdaxiləsi tələb olunur. Süni intellektlə işləyən təhlükəsizlik sistemləri tarixi məlumatlardan öyrənən maşın öyrənmə alqoritmlərinə əsaslanır. Bu, sistem mövcud nümunələrə uyğun gəlməyən yeni, naməlum təhlükələrlə qarşılaşdıqda yanlış nəticələrə səbəb ola bilər. Digər artan narahatlıq, hakerlərin inandırıcı fişinq e-poçtları yaratmaq və hətta zərərli proqram yaratmaq da daxil olmaqla, zərərli məqsədlər üçün AI-dan necə istifadə edə bilməsidir. [8]

Kibertəhlükəsizlikdə AI tətbiq etmək üçün bacarıqlar

Süni intellekt və kibertəhlükəsizlik hər zamankindən daha çox bağlıdır. Hər ikisində bacarıq və qabiliyyətə malik şəxslərə bu gün yüksək tələbat var. Müəssisələr və texnologiya şirkətləri həm kibertəhlükəsizliyi, həm də AI texnikalarını kibertəhlükəsizlik iş axınlarına nə vaxt və necə tətbiq edəcəyini başa düşmək üçün kifayət qədər kibertəhlükəsizliyi başa düşə bilən insanları axtarırlar. Məlumat alimləri, analitiklər və kibertəhlükəsizlik sahəsində təcrübəsi olan mühəndislər vacibdir. Bu rollar maşın öyrənmə məlumatlarının modelləşdirilməsi, dərin neyron şəbəkələri, dil modelləşdirilməsi və davranış təhlili sahəsində təhsil və təcrübə tələb edir. Bundan əlavə, onlar kibertəhlükəsizlik prinsiplərini yaxşı başa düşməlidirlər. Süni intellekt üzrə kibertəhlükəsizlik üzrə mütəxəssis şəbəkə təhlükəsizliyi, kompüter ekspertizası və kriptoqrafiya, zərərli proqramların aşkarlanması və müdafiəsi və məlumatların mühafizəsi sahələrində güclü biliyə malik olmalıdır.

Kibertəhlükəsizlikdə AI ilə bağlı alt xətt

Sophos Süni İntellekt 2017-ci ildə xüsusi olaraq kibertəhlükəsizlik üçün məlumat elmində və maşın öyrənməsində qabaqcıl texnologiyalar istehsal etmək üçün yaradılıb. Yüksək təcrübəli məlumat alimləri, mühəndislər və təhlükəsizlik ekspertlərindən ibarət Sophos X-Ops komandası maşın öyrənməsi, genişmiqyaslı elmi hesablama arxitekturası, insan-AI qarşılıqlı əlaqəsi və məlumatın

vizuallaşdırılmasına diqqət yetirir. Süni intellekt təhdidləri aşkar etmək və sistemlərinizi, məlumatlarınızı və tətbiqlərinizi qorumaq üçün maşın öyrənməsinin sərhədlərini irəliləyir. [7,9,10]

Nəticə.

İstənilən məkanda və istənilən sistemdə kibertəhlükəsizliyi təmin edə bilmək üçün ən yaxşı üsul və vasitə seçilmədir. Bu cür təhlükələrdən qoruna bilmək üçün əvvəlcədən onu müəyyənləşdirməyi bacarmaq lazımdır. Doğru qəbul edilmiş qərarla və düzgün seçilmiş qorunma üsulu ilə kibertəhlükəsizliyi təmin etmək mümkündür. Düzgün seçilmiş qorunma üsuluna süni intellekt sistemlərini misal göstərə bilərik. Məqalədə süni intellektlə kibertəhlükəsizliyi təmin etməyin yolları araşdırılmışdır.

Ədəbiyyat

[1] Hadis Karimipour, Hany Farag, Jin Wei – Kocsis, Pirathayini Srikantha "Security of Cyber – physical systems", 2020.

[2] B.S.Prashanth, M.V.Manoj Kumar, S.L. Shiva Darshan, Vishnu Srinivasa Murthy "Malware analysis and intrusion detection in cyber – physical systems", 2023.

[3] T. Pushpalatha, Dr. Yogesh Kumar Sharma, M. Krishna, Dr. S. Nagaprasad "Introduction to cyber security", 2020.

[4] James Graham, Rick Howard, Ryan Olson "Cyber security essentials", 2016.

[5] Ashish Kumar Luhach, Atilla Elçi "Artifical intelligence paradigms fors mart cyber – physical systems ", 2020.

[6] Daniel Mikelsten, Vasil Teigens, Peter Skalfist "Yapay zeka: Dördüncü sanayi devrimi", 2020.

[7] Sedat Akleylek, Aykut Karakaya, Yavyz Canbay ve b. "Siber güvenlik ve savunma: Biyometrik ve kriptografik uygulamalar", 2020.

[8] https://dergipark.org.tr/en/download/article-file/1883680

[9] https://www.researchgate.net/publication/343926839_Artificial_intelligence_in_cyber_physical_systems

[10] https://www.aimspress.com/article/doi/10.3934/era.2023097

KORPORATİV İDARƏETMƏDƏ BULUD TEXNOLOGİYALARI

Babazadə Gülnar

Rəhimova Nazilə

Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı, Azərbaycan 2024

Xülasə

Bu məqlədə İKT-nin inkişafı nəticəsində dayanmadan inkişaf etdirilən Korporativ idarəetmədə Cloud Computing(Bulud Hesablama) və onun sayəsində işlərimizin asanlaşmasından, eləcə də niyə bulud texnologiyalarından istifadə etməliyik və onun üstünlükləri, çatışmazlıqları nələrdir, bu haqda bəhs olunub.

Açar sözlər-Cloud Computing(Bulud Hesablama), üstünlüklər, çatışmazlıqlar, təhlükəsizlik.

Giriş

Korporativ idarəetmədə dedikdə, qarşıya qoyulan bir məqsəd üçün bir çox resurlardan birgə istifadə nəzərdə tutulur. Dövlət qurumları vətəndaşlara ən yaxşı keyfiyyəti daha az xərclə xidmət etməyi, özəl şirkətlər isə mənfəət əldə etmək üçün müştərilərinə mal və xidmətlər təqdim edir.

İnformasiya Texnologiyaları çox sürətlə inkişaf edir və bu inkişafı kənardan izləmək, tamaşaçı kimi qalmaq ölkəmizin gələcəyi üçün olduqca ciddi problemlər yarada bilər. İnformasiya cəmiyyətinə yönəlmiş İKT-nin ölkəmizdə dayanmadan inkişaf etməsi eyni zamanda dövlət tərəfindən maraq yaradan hərtərəfli diqqət və qayğı bu sahənin qeyri-neft sektorundakı rolunun ildən ilə artacağını deməyə əsas