Rəqəmsal Dövlət Mühitində İnzibati İdarəetmə Sistemlərinə Yönəlmiş Kibertəhlükəsizlik Təhdidlərinin Analizi

Gülnarə Nəbibəyova[1], Fidan Ellazova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*gnabibayova@gmail.com*, [2]*fidan.ellazova94@gmail.com*

***Xülasə*— Müxtəlif informasiya sistemlərindən, sensor mənbələrdən, dövlət reyestrlərindən və rəqəmsal platformalardan daxil olan məlumatların həcminin artması həm təhlil üçün yeni imkanlar yaradır, həm də yeni kibertəhlükələrin meydana çıxmasına səbəb olur. Müasir kibertəhdidlər yüksək mürəkkəblik, gizlilik və adaptivlik səviyyəsi ilə xarakterizə olunur. Bu isə onların vaxtında aşkarlanması üçün məlumatların intellektual analizi metodlarından istifadəni tələb edir. Məqalədə çoxölçülü məlumatların analizi və rəqəmsal dövlətin inzibati idarəetmə sistemlərinə yönəlmiş kibertəhlükəsizlik təhdidlərinin aşkar edilməsi məqsədilə OLAP texnologiyalarının neyron şəbəkələri ilə inteqrasiya olunmuş şəkildə istifadəsinin potensialı araşdırılır.**

Açar sözlər*— *rəqəmsal dövlət; OLAP; neyron şəbəkələri; kibertəhlükəsizlik; təhdidlər.

I. GİRİŞ

Rəqəmsal dövlət (RD) mühitində inzibati idarəetmə sistemləri dövlət infrastrukturunun kritik əhəmiyyətli elementlərinə çevrilir. İdarəetmə proseslərinin rəqəmsallaşdırılması informasiya sistemlərinin, qurumlararası inteqrasiyaların və məlumat mübadiləsi kanallarının sayının artması ilə müşayiət olunur. Bu isə öz növbəsində hücum səthinin genişlənməsinə və inzibati sistemlərin müxtəlif kibertəhdidlərə qarşı həssaslığının artmasına səbəb olur.

İnzibati idarəetmə sistemlərinin fəaliyyətinin pozulması ciddi nəticələrə, o cümlədən idarəetmənin effektivliyinin azalması və milli təhlükəsizlik üçün təhlükə yaranmasına gətirib çıxara bilər. Bu səbəbdən RD-in inzibati sistemlərinin kibertəhlükəsizliyinin təmin olunması müasir dövlət idarəçiliyinin əsas vəzifələrindən birinə çevrilir.

RD-in xüsusiyyətlərindən biri müxtəlif mənbələrdən daxil olan məlumatların həcminin sürətli artmasıdır. Böyük həcmli məlumatlar potensial təhlükələri aşkar etmək üçün intellektual analiz metodlarının tətbiqini zəruri edir. Ənənəvi təhlükəsizlik monitorinqi və analiz metodları çoxölçülü və dinamik məlumatlarla işləyərkən kifayət qədər effektiv deyil. Bu şəraitdə məlumatların intellektual analizi texnologiyaları, o cümlədən OLAP texnologiyaları və maşın öyrənmə metodları xüsusi rol oynayır [1].

OLAP texnologiyaları məlumatların çoxölçülü analizini aparmağa, qanunauyğunluqları aşkar etməyə və idarəetmə məlumatlarının müxtəlif kəsimlərində anomaliyaları müəyyən etməyə imkan verir. Neyron şəbəkələri isə sistemin özünüöyrənmə qabiliyyətini təmin edir, gizli asılılıqları aşkar edir və yeni kibertəhlükə növlərinə uyğunlaşmağa imkan yaradır.

Tədqiqatın məqsədi RD-in inzibati idarəetmə sistemlərinə yönəlmiş kibertəhlükəsizlik təhdidlərinin təhlil edilməsi, eləcə də bu təhdidlərin aşkarlanması üçün OLAP və neyron şəbəkə texnologiyalarının imkanlarının araşdırılmasıdır.

II. İNZİBATİ İDARƏETMƏ SİSTEMLƏRİNƏ YÖNƏLMİŞ KİBERTƏHLÜKƏSİZLİK TƏHDİDLƏRİNİN XARAKTERİSTİKASI

RD şəraitində inzibati idarəetmə sistemləri potensial kibercinayətkarların artan diqqət obyektinə çevrilir. Bu, həmin sistemlərin idarəetmə qərarlarının qəbulunu təmin etməsi, kritik əhəmiyyətli məlumatların emalı və dövlət proseslərinin koordinasiyasını həyata keçirməsi ilə bağlıdır. Bu baxımdan, inzibati idarəetmə sistemlərinə yönəlmiş kibertəhlükəsizlik təhdidlərinin əsas növlərinin təhlili xüsusi aktuallıq kəsb edir. Əsas təhdidlərə aşağıdakılar aid edilir:

- İcazəsiz giriş;
- Zərərli proqram təminatı hücumları;
- Xidmətdən imtina (DDoS) hücumları;
- Daxili təhdidlər;
- Sosial mühəndislik hücumları;
- Məlumat sızması təhdidləri.

A. İcazəsiz giriş

Ən geniş yayılmış təhdidlərdən biri inzibati idarəetmə informasiya sistemlərinə icazəsiz girişdir. Bu təhdid müvafiq hüquq və səlahiyyətlərə malik olmayan şəxslərin sistemlərə daxil olmasını nəzərdə tutur. İcazəsiz giriş proqram təminatındakı zəifliklərdən istifadə, zəif autentifikasiya mexanizmləri, həmçinin sosial mühəndislik üsulları vasitəsilə həyata keçirilə bilər. Belə halların nəticəsi kimi məxfi məlumatların sızması, idarəetmə məlumatlarının dəyişdirilməsi və inzibati proseslərin pozulması baş verə bilər [2].

B. Zərərli proqram təminatı hücumları

Digər ciddi təhdidlərdən biri zərərli proqram təminatından istifadə ilə həyata keçirilən hücumlardır. Bu hücumlara viruslar,

DOI: 10.25045/forensic.gov.2026.56

troyan proqramları, fidyə proqramları (ransomware) və casus proqram təminatı daxildir. Zərərli proqramlar inzibati idarəetmə sistemlərinə elektron poçt, xarici yaddaş daşıyıcıları və ya zəif qorunan şəbəkə xidmətləri vasitəsilə daxil ola bilər. Nəticədə dövlət informasiya sistemlərinin fəaliyyəti bloklana, məlumatlar itirilə və inzibati idarəetmənin dayanıqlığı pozula bilər [3].

C. Xidmətdən imtina (DDoS) hücumları

Xidmətdən imtina tipli hücumlar inzibati idarəetmə sistemlərinə çoxsaylı sorğular göndərərək onların fəaliyyətini iflic etməyə yönəldilir. Nəticədə sistemlər qanuni istifadəçilər üçün əlçatmaz olur. Bu isə dövlət orqanlarının fəaliyyətində fasilələrə, idarəetmə qərarlarının qəbulunda gecikmələrə və dövlət xidmətlərinin göstərilməsində problemlərə səbəb ola bilər [4].

D. Daxili təhdidlər

Daxili təhdidlər də mühüm rol oynayır və dövlət orqanlarının əməkdaşlarından və ya podratçı təşkilatlardan qaynaqlana bilər. Bu təhdidlər həm qəsdən edilən hərəkətlərlə, həm də insan səhvləri ilə bağlı ola bilər. İşçilərin təhlükəsizlik üzrə hazırlıq səviyyəsinin aşağı olması, təhlükəsizlik qaydalarının pozulması və informasiya sistemlərindən düzgün istifadə edilməməsi məlumat sızmasına və inzibati proseslərin **ləngiməsinə** gətirib çıxara bilər [5].

E. Sosial *mühəndislik* hücumları

Sosial mühəndislik informasiya sistemlərinin istifadəçilərinə təsir göstərərək məxfi məlumatların əldə edilməsinə yönəlmiş üsuldur. Bu hücumlara fişinq, saxta mesajlar, texniki dəstək adından edilən telefon zəngləri və digər manipulyasiya üsulları daxildir. Uğurlu sosial mühəndislik hücumları istifadəçi hesablarının ələ keçirilməsinə və inzibati idarəetmə sistemlərinə icazəsiz girişə səbəb ola bilər [6].

F. Məlumat sızması təhdidləri

Məlumat sızması inzibati idarəetmə sistemləri üçün ən kritik təhdidlərdən biridir. Bu hal kibercinayətkar hücumları, insan səhvləri və ya informasiya resurslarının zəif qorunması nəticəsində baş verə bilər. Məlumat sızması dövlət məlumatlarının, vətəndaşların şəxsi məlumatlarının və strateji idarəetmə qərarlarının açıqlanmasına səbəb ola bilər [7].

G. Ənənəvi müdafiə metodlarının problemləri

Kibertəhlükəsizliyin təmin edilməsi üçün ənənəvi metodlar, o cümlədən girişə nəzarət sistemləri, antivirus həlləri və müdaxilələrin aşkarlanması vasitələri RD-in inzibati idarəetmə sistemlərinin qorunmasında bir sıra məhdudiyyətlərə malikdir. Əsas problemlərdən biri bu metodların əvvəlcədən məlum olan təhdidlərə və siqnatura əsaslı analizə yönəlməsidir. Yeni növ hücumların və adaptiv təhdidlərin meydana çıxması şəraitində ənənəvi metodlar daha az effektiv olur. Onlar gizli hücumları, mürəkkəb sızma ssenarilərini və istifadəçilərin davranışındakı tədrici dəyişiklikləri vaxtında aşkar etmək qabiliyyətinə malik deyildir [2]. Bu baxımdan RD şəraitində inzibati idarəetmə sistemləri geniş spektrli kibertəhdidlərə məruz qalır. Bu təhdidlərin vaxtında aşkarlanması və təhlili dövlət idarəçiliyinin dayanıqlığının və təhlükəsizliyinin təmin edilməsinin əsas şərtlərindən biridir.

Beləliklə, RD-in fəaliyyətinin müasir şəraiti inzibati sistemlərin kibertəhlükəsizliyinin təmin edilməsi üçün məlumatların intellektual analiz metodlarının tətbiqini tələb edir. İntellektual metodlar böyük həcmli məlumatların təhlili əsasında gizli qanunauyğunluqları, anomaliyaları və potensial təhdidləri aşkar etməyə imkan verir. OLAP texnologiyalarının istifadəsi məlumatların çoxölçülü analizini təmin edir ki, bu da təhdidləri zaman, ərazi və funksional aspektlər daxil olmaqla müxtəlif kontekstlərdə araşdırmağa imkan yaradır. Öz növbəsində, neyron şəbəkələr gizli asılılıqları aşkar etməyə, mümkün hücumları proqnozlaşdırmağa və dəyişən şəraitə uyğunlaşmağa imkan verir. İntellektual analitika və adaptiv müdafiə metodlarının inteqrasiyası inzibati idarəetmə sistemlərinin kiberdavamlılıq səviyyəsini artırmağa imkan verir.

III. OLAP TEXNOLOGİYALARI İNZİBATİ MƏLUMATLARIN ANALİZİNDƏ

OLAP (On-Line Analytical Processing) böyük həcmli məlumatların çoxölçülü analizini təmin edən və qərarların qəbuluna dəstək verən texnologiyadır. RD mühitində OLAP texnologiyaları inzibati məlumatların, o cümlədən kiber təhlükəsizliklə bağlı məlumatların analizində mühüm rol oynayır.

Çoxölçülü məlumatların analizi informasiyanı müxtəlif baxış bucaqlarından qiymətləndirməyə imkan verir. Bu zaman ölçülər (dimensions) və göstəricilər (measures) istifadə olunur.

OLAP texnologiyalarının tətbiqi böyük həcmli məlumatların təhlilini asanlaşdırır, gizli əlaqələrin aşkarlanmasına imkan yaradır, müqayisəli analiz aparmağa, meyilləri və qanunauyğunluqları müəyyən etməyə və qərarvermə prosesinin effektivliyini artırmağa şərait yaradır. Beləliklə, OLAP texnologiyaları RD-in inzibati idarəetmə sistemlərində kiber təhlükəsizlik təhdidlərinin intellektual analizinin əsasını təşkil edir.

E. Təhlükəsizlik hadisələrinin analizi üçün OLAP-kubların qurulması

Kiber təhlükəsizlik təhdidlərinin analizi üçün təhlükəsizlik hadisələrini əhatə edən xüsusi OLAP kubları formalaşdırılır. Bu kublar məlumatların strukturlaşdırılmasına və çoxölçülü analizinə imkan verir.

OLAP kubunun ölçüləri kimi zaman, hücum mənbəyi, hücumun növü, giriş səviyyəsi, istifadəçi və qurum kimi parametrlərdən, həmçinin giriş cəhdlərinin sayı, təhlükəsizlik insidentlərinin miqdarı, risk səviyyəsi, anomaliya hadisələrinin tezliyi və bloklanan əməliyyatların sayı kimi göstəricilərdən istifadə oluna bilər.

OLAP kublarının qurulması təhlükəsizlik hadisələrinin operativ analizini aparmağa, tendensiyaları aşkar etməyə və təhdidlərin detallı şəkildə araşdırılmasına imkan verir.

F. Şübhəli fəaliyyət nümunələrinin aşkarlanması

OLAP texnologiyalarının tətbiqi inzibati sistemlərdə şübhəli davranış nümunələrinin (davranış şablonlarının) aşkarlanmasına imkan yaradır. Çoxölçülü məlumatların analizi istifadəçi

davranışında anomaliyaların və potensial təhlükələrin müəyyən edilməsini təmin edir.

Əsas aşkarlanan nümunələrə istifadəçilərin qeyri-adi aktivliyi, iş vaxtından kənar giriş cəhdləri, çoxsaylı uğursuz giriş cəhdləri, əməliyyat həcminin qəfil artması, eləcə də qeyri-adi məlumatlara giriş aid edilir. Bu cür nümunələrin aşkarlanması təhlükələrin vaxtında müəyyən olunmasına və onların qarşısının alınmasına imkan verir.

Nəticə etibarilə, OLAP texnologiyalarının inzibati məlumatların analizində tətbiqi kiber təhlükəsizlik təhdidlərinin effektiv aşkarlanmasını təmin edir və RD infrastrukturunun dayanıqlığını artırır.

IV. KİBERTƏHDİDLƏRİN AŞKARLANMASI ÜÇÜN NEYRON ŞƏBƏKƏLƏRİN TƏTBİQİ

Neyron şəbəkələr insan beyninin iş prinsipini imitasiya edən riyazi modellərdir və böyük həcmli məlumatlarda mürəkkəb asılılıqları aşkar etməyə, həmçinin öyrənmə qabiliyyətinə malikdir. Kiber təhlükəsizlik sahəsində neyron şəbəkələr anomaliyaların aşkarlanması və potensial təhdidlərin proqnozlaşdırılması üçün istifadə olunur.

Neyron şəbəkələrin əsas üstünlüyü onların özünüöyrənmə və adaptasiya qabiliyyətidir. Sistem yeni növ hücumlarla qarşılaşdıqda davranış modelini yeniləyə bilir ki, bu da onları dinamik və mürəkkəb informasiya sistemlərinin qorunması üçün effektiv edir.

A. Gizli təhdidlərin aşkarlanması

Gizli təhdidlər ənənəvi metodlarla aşkar edilməsi çətin olan və birbaşa görünməyən hücum növləridir. Neyron şəbəkələr böyük həcmli tarixi və cari məlumatları analiz edərək anomaliyaları və gizli qanunauyğunluqları müəyyən edə bilir.

Dərin öyrənmə metodları (RNN, CNN və s.) hadisə ardıcıllıqlarının, şəbəkə trafikinin və istifadəçi fəaliyyət jurnallarının analizində istifadə olunur. Bu yanaşma potensial təhlükələrin əvvəlcədən proqnozlaşdırılmasına imkan yaradır.

B. OLAP ilə inteqrasiya

Neyron şəbəkələrin OLAP texnologiyaları ilə inteqrasiyası hibrid analiz yanaşması yaradır. OLAP məlumatların strukturlaşdırılmış və çoxölçülü analizini təmin edir, neyron şəbəkələr isə bu məlumatlar üzərində intellektual emal və proqnozlaşdırma həyata keçirir.

Bu inteqrasiya nəticəsində daha dəqiq monitorinq sistemləri yaradılır və mürəkkəb kibertəhlükələrin aşkarlanması imkanı artır.

C. Neyron şəbəkələrin üstünlükləri

Neyron şəbəkələrin əsas üstünlüklərinə aşağıdakılar aid edilir:

- yeni növ kibertəhlükələrə adaptasiya olunma qabiliyyəti;
- gizli anomaliyaların və qeyri-aşkar qanunauyğunluqların aşkarlanması;
- böyük həcmli verilənlərin real-vaxt rejiminə yaxın şəraitdə intellektual təhlili;
- monitorinq və operativ reaksiya mexanizmlərinin effektivliyinin artırılması;
- inzibati idarəetmə sistemlərində risk səviyyəsinin azaldılması.

Nəticə olaraq, OLAP texnologiyaları ilə neyron şəbəkələrin birlikdə istifadəsi kibertəhlükəsizlik sahəsində intellektual analiz imkanlarını genişləndirir və RD infrastrukturunun təhlükəsizliyini əhəmiyyətli dərəcədə gücləndirir.

V. KİBERTƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİ ÜÇÜN OLAP TEXNOLOGİYALARI İLƏ NEYRON ŞƏBƏKƏLƏRİNİN İNTEQRASİYA MODELİ

RD-in müasir inzibati idarəetmə sistemləri kibertəhlükəsizliyin təmin edilməsi üçün inteqrasiya olunmuş analitik həllərin tətbiqini tələb edir. Məlumatların həcminin artması və kiber təhdidlərin çoxalması şəraitində informasiya axınlarının intellektual analiz metodlarından istifadə xüsusi aktuallıq kəsb edir. Effektiv yanaşmalardan biri OLAP texnologiyaları ilə neyron şəbəkələrin vahid analitik sistemdə birləşdirilməsidir.

OLAP texnologiyaları ilə neyron şəbəkələrin inteqrasiyası çoxölçülü məlumat analizi imkanlarını maşın öyrənmə metodları ilə birləşdirməyə imkan verir. Yuxarıda qeyd edildiyi kimi, belə inteqrasiya rəqəmsal dövlətin inzibati idarəetmə sistemlərində verilənlərin analizi üçün hibrid yanaşmanı formalaşdırır. Təklif olunan modeldə hibrid yanaşma verilənlərin emalının kaskad arxitekturası şəklində həyata keçirilir. Bu arxitekturada OLAP sistemi verilənlərin ilkin emalını, aqreqasiyasını və strukturlaşdırılmasını təmin edərək informasiya axınlarının çoxölçülü analizini yerinə yetirir. Neyron şəbəkələri isə verilənlərin intellektual analizini həyata keçirir, gizli qanunauyğunluqları aşkar edir, anomaliyaları müəyyənləşdirir və kibertəhlükəsizlik təhdidlərini proqnozlaşdırır.

Belə kompleks yanaşma RD-in inzibati sistemlərinin monitorinqinin effektivliyini artırmağa, təhlükələrin vaxtında aşkarlanmasını təmin etməyə və dövlətin rəqəmsal infrastrukturunun müasir kiberhücumlara qarşı dayanıqlığını yüksəltməyə imkan verir.

Şəkil 1-də OLAP texnologiyaları və neyron şəbəkələrin inteqrasiya modeli təqdim olunur. Bu model RD-in inzibati idarəetmə sistemlərində kibertəhlükəsizlik təhdidlərinin aşkarlanması və analiz edilməsi üçün nəzərdə tutulmuşdur.

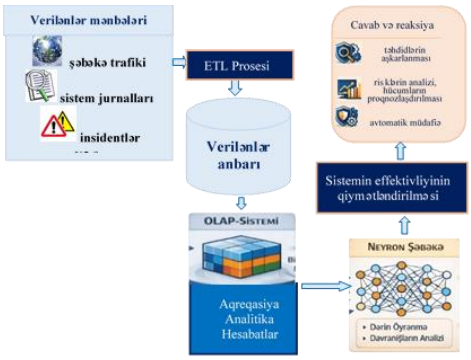
Təklif olunan OLAP texnologiyaları və neyron şəbəkələrin inteqrasiya modeli RD infrastrukturunda kibertəhlükəsizlik təhdidlərinin intellektual analizini təmin etmək üçün nəzərdə tutulmuşdur. Model verilənlərin toplanması, analitik emalı, intellektual analiz və avtomatik reaksiya mexanizmlərindən ibarət çoxsəviyyəli arxitekturaya əsaslanır.

Modelin arxitekturası yeddi əsas funksional blokdan ibarətdir.

Birinci blok verilənlər mənbələridir. Bu mənbələrə dövlət informasiya sistemlərinin şəbəkə trafiki, təhlükəsizlik hadisələri

jurnalları, sistem jurnalları, istifadəçi aktivliyi məlumatları, sistemə giriş jurnalları, təhlükəsizlik insidentləri haqqında məlumatlar və s. daxildir.

İkinci blok ETL prosesidir [8]. Bu mərhələdə paylanmış dövlət və şəbəkə mənbələrindən verilənlərin çıxarılması, onların təmizlənməsi, normallaşdırılması, transformasiyası və sonradan verilənlər anbarına yüklənməsi həyata keçirilir.



Şəkil 1. Rəqəmsal dövlət mühitində kibertəhlükəsizlik təhdidlərinin analizi üçün OLAP texnologiyaları ilə neyron şəbəkələrinin inteqrasiya modeli

Üçüncü blok verilənlər anbarıdır. Bu mərhələdə böyük həcmli çoxölçülü verilənlər sonrakı analiz üçün hazırlanır.

Dördüncü blok OLAP sistemindən ibarətdir və verilənlərin çoxölçülü analitik emalını həyata keçirir. Bu blokun əsas funksiyalarına verilənlərin aqreqasiyası, çoxölçülü analiz, tendensiyaların aşkar edilməsi, təhdidlərin dinamikasının təhlili və hesabatların formalaşdırılması daxildir.

OLAP texnologiyaları verilənlərin zaman, dövlət orqanları, təhdid növləri, kritik səviyyə və hücum mənbələri kimi ölçülər üzrə analizinə imkan verir.

Bu mərhələdə strukturlaşdırılmış verilənlər beşinci blok — neyron şəbəkələri blokuna ötürülür.

Beşinci blok kibertəhlükəsizlik təhdidlərinin intellektual analizini həyata keçirir. Bu blokun əsas funksiyalarına istifadəçi davranışının analizi, anomaliyaların aşkar edilməsi, naməlum təhdidlərin müəyyən olunması, hücumların proqnozlaşdırılması və təhdidlərin klassifikasiyası daxildir. Neyron şəbəkələri böyük həcmli verilənlər massivlərində gizli qanunauyğunluqları aşkar etməyə və yeni növ kibertəhdidləri müəyyən etməyə imkan verir.

Altıncı blok sistemin effektivliyinin qiymətləndirilməsini həyata keçirir.

Yeddinci blok aşkar edilmiş təhdidlərə avtomatik reaksiya verilməsini təmin edir. Bu blokun əsas funksiyalarına təhdidlərin aşkarlanması, risklərin təhlili, hücumların proqnozlaşdırılması, avtomatik müdafiə, administratorların məlumatlandırılması və müdafiə mexanizmlərinin işə salınması daxildir.

Bu mərhələdə sistem idarəetmə qərarları qəbul edir və təhlükəsizlik tədbirlərini həyata keçirir.

Təklif olunan modeldə Multilayer Perceptron (MLP) tipli çoxqatlı süni neyron şəbəkəsinin istifadəsi nəzərdə tutulur. Şəbəkənin arxitekturası ilkin olaraq giriş qatı, iki gizli qat və çıxış qatından ibarət hesab olunur.

Giriş qatının informasiya sisteminin analiz edilən xüsusiyyətlərinə uyğun olaraq 64 neyrondan ibarət olması nəzərdə tutulur. Bu xüsusiyyətlərə şəbəkə trafiki parametrləri, istifadəçi aktivliyi göstəriciləri, təhlükəsizlik hadisələri və sistem jurnalları aid edilir.

Birinci gizli qatda 128 neyronun istifadəsi nəzərdə tutulur. Bu mərhələdə neyronların sayının artırılması giriş verilənləri arasındakı mürəkkəb və gizli asılılıqların aşkarlanması, həmçinin xüsusiyyətlər fəzasının genişləndirilməsi məqsədi daşıyır.

İkinci gizli qatda 64 neyronun istifadəsi nəzərdə tutulur. Bu mərhələdə ölçünün azaldılması verilənlərin ən mühüm xüsusiyyətlərinin seçilməsinə və modelin həddindən artıq öyrənməsinin qarşısının alınmasına imkan verir.

Çıxış qatında sistemin vəziyyətinin binar təsnifatı — kibertəhdidin mövcudluğu və ya təhlükəsiz vəziyyətin müəyyən edilməsi üçün iki neyronun istifadəsi nəzərdə tutulur.

Gizli qatlarda qeyri-xətti asılılıqların effektiv emalını təmin edən ReLU (Rectified Linear Unit) aktivləşdirmə funksiyasının tətbiqi nəzərdə tutulur. Çıxış qatında isə analiz olunan hadisələrin uyğun siniflərə aid olma ehtimallarını müəyyən etməyə imkan verən Softmax funksiyasının istifadəsi planlaşdırılır.

Optimallaşdırma alqoritmi kimi Adam metodunun, itki funksiyası kimi isə categorical cross-entropy funksiyasının istifadəsi nəzərdə tutulur. Neyron şəbəkəsinin konkret arxitektur parametrləri və modelin effektivlik göstəriciləri gələcək eksperimental tədqiqatlar çərçivəsində dəqiqləşdirilə bilər.

VI. RƏQƏMSAL DÖVLƏTİN KİBERTƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ ÜÇÜN OLAP VƏ NEYRON ŞƏBƏKƏLƏRİNİN İNTEQRASİYASININ EFFEKTİVLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

Şəkil 1-də göstərilir ki, inteqrasiya olunmuş sistemin effektivlik metriklərinin hesablanması üçün əsas kimi neyron şəbəkələrinin çıxış nəticələri istifadə olunur. İdarəetmə sistemlərinin qorunması üçün təklif edilən OLAP və neyron şəbəkələrinin inteqrasiya olunmuş yanaşmasının effektivliyi bir neçə əsas göstərici vasitəsilə qiymətləndirilə bilər. Bu göstəricilər təhdidlərin aşkarlanmasının dəqiqliyini, tamlığını və sürətini [9], eləcə də sistemin ümumi effektivliyini kəmiyyət baxımından müəyyən etməyə imkan verir. Tədqiqat çərçivəsində eksperimental qiymətləndirmə aparılmadığından, aşağıda kibertəhlükəsizlik sistemləri üçün praktikada qənaətbəxş və yüksək effektiv hesab olunan göstəricilərin optimal dəyərləri təqdim olunur.

D. Təhdidlərin aşkarlanma dəqiqliyi (Accuracy)

Dəqiqlik düzgün identifikasiya edilmiş hadisələrin (həm təhdidlər, həm də təhlükəsiz hadisələr) ümumi hadisələr sayına nisbətini göstərir:

$$A = \frac{TT+TS}{TT+TS+FP+MT} \quad (1)$$

burada:

TT — düzgün aşkarlanmış təhdidlər;

TS — düzgün müəyyən edilmiş təhlükəsiz hadisələr;

FP — yanlış siqnallar (false positive);

MT — buraxılmış təhdidlər.

90%-dən yuxarı Accuracy göstəricisi adətən yaxşı nəticə, 95%-dən yuxarı göstərici isə yüksək effektivlik səviyyəsi hesab olunur.

E. Təhdidlərin aşkarlanma tamlığı (Recall)

Tamlıq sistem tərəfindən aşkarlanmış real təhdidlərin payını göstərir:

$$R = \frac{TT}{TT+MT} \quad (2)$$

Recall göstəricisinin 90%-dən yuxarı olması effektiv nəticə hesab olunur.

F. Aşkarlamanın dəqiqliyi (Precision)

Precision sistemi tərəfindən aşkar edilən təhdidlərin nə qədər dəqiq olduğunu, yəni yanlış siqnalların minimuma endirilməsini göstərir:

$$P = \frac{TT}{TT+\mathrm{FP}} \quad (3)$$

Praktiki sistemlərdə 90%-dən yuxarı Precision göstəricisi qənaətbəxş hesab edilir.

G. Effektivliyin F-ölçüsü

F-ölçü effektivliyi (F_1-ölçü) təhdidlərin aşkarlanmasının dəqiqliyini (Precision) və tamlığını (Recall) eyni zamanda nəzərə alan göstəricidir.

F_1-ölçüsü aşağıdakı kimi hesablanır:

$$F_1 = \frac{2*P*R}{\mathrm{P+R}} \quad (4)$$

Bu göstərici sistemin keyfiyyətinin kompleks qiymətləndirilməsi üçün istifadə olunur, xüsusilə də buraxılmış təhdidlər və yanlış siqnalların hər ikisi vacib olduqda, 0,9-dan yuxarı olması modelin balanslaşdırılmış və keyfiyyətli işlədiyini göstərir.

H. Təhdidin aşkarlanma vaxtı

Sistemin reaksiya sürəti hücumun başlanğıcı ilə onun aşkarlanması arasındakı zamanla müəyyən edilir:

$$T_{detect}=t_{alert}-t_{attack} \quad (5)$$

burada:

t_{alert} — təhdidin başlanma vaxtı;

t_{attack} — hücumun aşkarlanma vaxtı.

Müasir kibertəhlükəsizlik monitorinq sistemləri üçün təhdidlərin real-vaxta yaxın rejimdə, yəni bir neçə saniyə ərzində aşkarlanması üstün hesab olunur.

I. Sistemin inteqral effektivliyi

Sistemin ümumi effektivliyi dəqiqlik, tamlıq, aşkarlama dəqiqliyi və aşkarlama vaxtını birləşdirən çəkili göstərici vasitəsilə qiymətləndirilə bilər:

$$E=w_1A+w_2R+w_3P-w_4T_{detect} \quad (6)$$

burada w_1, w_2, w_3, w_4 — tədqiqatçı tərəfindən müəyyən edilən çəki əmsalları;

E — sistemin ümumi effektivliyi.

Sistemin inteqral effektivliyi formulunda T_{detect} aşkarlama vaxtı çıxılır, çünki aşkarlama vaxtının az olması sistem üçün daha yaxşıdır, vaxtın çox olması isə daha pis hesab olunur. Hücum tez aşkar edilərsə, sistem daha effektiv hesab olunur; hücum gec aşkar edilərsə isə sistemin effektivliyi azalır.

Bu yanaşma OLAP texnologiyaları və neyron şəbəkələrinin inteqrasiyasının RD-in inzibati sistemlərinin təhlükəsizliyinin təmin edilməsində effektivliyini kompleks şəkildə qiymətləndirməyə imkan verir.

NƏTİCƏ

Kibertəhlükəsizliyin təmin olunması üçün OLAP texnologiyaları və neyron şəbəkələrin inteqrasiya olunmuş şəkildə tətbiqi mühüm əhəmiyyət kəsb edir. OLAP texnologiyaları böyük həcmli məlumatların çoxölçülü analizini, strukturlaşdırılmasını və aqreqasiyasını təmin edərək analitik prosesin ilkin mərhələsini formalaşdırır. Neyron şəbəkələr isə bu məlumatlar əsasında gizli qanunauyğunluqları aşkar edir, anomaliyaları müəyyənləşdirir və potensial kibertəhlükələri əvvəlcədən proqnozlaşdırır.

Bu inteqrasiya olunmuş yanaşma təhlükələrin vaxtında aşkarlanmasına, qərarvermə prosesinin effektivliyinin artırılmasına və inzibati sistemlərin dayanıqlığının gücləndirilməsinə imkan yaradır. Beləliklə, OLAP texnologiyaları və neyron şəbəkələrin birgə tətbiqi RD-in kibertəhlükəsizliyinin təmin edilməsində effektiv və perspektivli analitik yanaşma kimi qiymətləndirilə bilər.

ƏDƏBİYYAT

[1] P. O. Obitade, "Big data analytics: a link between knowledge management capabilities and superior cyber protection," Journal of Big Data, vol. 6, no. 71, 2019.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," Cybersecurity, vol. 2, no. 20, 2019.

[3] L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability," Journal of Cybersecurity, vol. 6, no. 1, p. tyaa023, 2020.

[4] Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Impact of Ransomware Attacks on Government Infrastructure and Potential Mitigation Strategies: A Systematic Review," Applied Sciences, vol. 12, no. 23, p. 12441, Dec. 2022.

[5] S. Prabhu and N. Thompson, "A primer on insider threats in cybersecurity," Information Security Journal: A Global Perspective, vol. 30, no. 6, pp. 341–353, 2021.

[6] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," Cybersecurity, vol. 4, no. 1, p. 28, 2021.

[7] I. H. Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, and J. J. P. Rodrigues, "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat," Cluster Computing, vol. 26, pp. 1913–1929, 2023.

[8] S. Sajida and S. Ramakrishna, "A Study of Extract-Transform-Load (ETL) Processes," ResearchGate, 2025. https://www.researchgate.net/publication/391846398_A_Study_of_Extract-Transform-Load_ETL_Processes

[9] C. D. Manning, P. Raghavan, and H. Schütze, An Introduction to Information Retrieval. Cambridge University Press, 2008. https://nlp.stanford.edu/IR-book/pdf/irbookonlinereading.pdf

Analysis of Cybersecurity Threats Targeting Administrative Management Systems in the Digital Government Environment

Gulnara Nabibayova[1], Fidan Ellazova[2]

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

[1]gnabibayova@gmail.com, [2]fidan.ellazova94@gmail.com

Abstract- In the context of the formation of a digital state, cybersecurity issues are of particular importance, especially for administrative management systems that ensure the functioning of government institutions and support governmental decision-making processes. The increasing volume of data originating from various information systems, sensor sources, state registries, and digital platforms creates new opportunities for analysis while simultaneously leading to the emergence of new cyber threats. Modern cyber threats are characterized by high levels of complexity, stealth, and adaptivity, which necessitates the use of intelligent data analysis methods for their timely detection. This article explores the potential of using OLAP technologies in conjunction with neural networks for multidimensional data analysis and for detecting cybersecurity threats targeting the administrative management systems of a digital government. Within the framework of the study, approaches to evaluating the effectiveness of the proposed integrated system are also considered. For the quantitative analysis of the model's performance, it is proposed to use a set of metrics that make it possible to determine the accuracy, completeness, and speed of threat detection, as well as the overall effectiveness of the cybersecurity system**.**

Keywords- digital state; OLAP; neural networks; cybersecurity; threats**.**