DOI: https://www.doi.org/10.36719/2663-4619/79/50-54

Rəsmiyyə İsrayıl qızı Əmiraslanova
Mingəçevir Dövlət Universiteti
dissertant
amiraslanova.ras@mail.ru

SÜNİ İNTELLEKTİN TƏTBİQİLƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ RİSKLƏRİNİN QİYMƏTLƏNDİRİLMƏSİ METODİKASI

Xülasə

Müasirdə informasiya təhlükəsizliyinin təmini hər bir müəssisənin idarəetmə fəaliyyətində vacib rol oynayır. Bu da verilənlərin toplanması, saxlanması, emalı və tətbiqi texnologiyalarının əsasını təşkil edir. Bu proseslər informasiya riskləri səviyyələrinin kəmiyyət və keyfiyyət şkalalarına görə vaxtaşırı təhlilinə əsaslanır. Bunlar da, informasiya təhlükəsizliyi təhdidlərinin, zəifliklərinin vaxtında müəyyən edilməsi, zərərsizləşdirilməsi üçün müvafiq tədbirlər kompleksini həyata keçirməyə imkan verir. Təqdim olunan məqalədə, informasiya təhlükəsizliyi risklərinin analitik təhlili süni intellekt texnologiyalarının bir istiqaməti olan neyro-qeyri-səlis şəbəkəyə əsaslanan metodika ilə qiymətləndirilməsi aparılmışdır.

Açar sözlər: *kompüter riyaziyyatı sistemləri, informasiya təhlükəsizliyi riski, süni intellekt, neyron şəbəkə, risklərinin qiymətləndirilməsi metodikası*

Rasmiyya Israil Amiraslanova

Methodology for assessing information security risks with the use of artificial intelligence

Abstract

Today, information security plays an important role in the management of every enterprise. It is the basis of data collection, storage, processing and application technologies. These processes are based on periodic analysis of information risk levels on quantitative and qualitative scales. They also allow for the implementation of a set of appropriate measures to identify and neutralize information security threats and vulnerabilities in a timely manner. In the presented article, the analytical analysis of information security risks was assessed using a neuro-fuzzy network-based methodology, which is one of the directions of artificial intelligence technologies.

Key words: *computer mathematical systems, information security risk, artificial intelligence, neuro network, risk assessment methodology*

Giriş

Kompüter riyaziyyatı sistemlərinin (KRS) rəqəmsal texnologiyalara tətbiqi cəmiyyətin informasiyalaşdırılması prosesini sürətləndirərək bir növ strateji resursa çevirmişdir. Beləki, informasiya sistemləri ölkəmizin, eləcədə dunyanın bir çox iqtisadi, ekoloji, enerji, nəqliyyat, ərzaq, səhiyyə, təhsil və s. sahələrində ən dəyərli və təhlükəli resurs hesab olunur. Beləliklə, informasiya sistemləri müasir cəmiyyətin əsas amillərindən biri olub müəssisə və təşkilatlarda informasiyanın qorunması və təhlükəsizliyinin təmini məsələsini ön plana çıxarır (Amiraslanoava, 2019: s.17-19).

Təqdim olunan məqalənin əsas məqsədi informasiyanın mühafizə metodologiyalarını təhlil edib, kompüter riyaziyyatı sistemlərinin tətbiqilə ilə davamlığı, dayanıqlığı və səmərəliliyi təmin edən metodoloji sxemin hazırlanmasıdır (Hümbətəliyev, 2021: 283).

Məlumdur ki, qloballaşdırılmış rəqəmsal transformasiyaya keçid dövründə süni intellektin tətbiqi imkanları durmadan artmaqdadır və etibarlı, çevik və dayanıqlı təhlükəsiz informasiya sistemlərinin formalaşmasında vacib rol oynayır. Bu məqsədlə, məqalədə informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodikası Neyron şəbəkədən istifadə edərək, kompüter riyaziyyatının ən geniş istifadə olunan Matlab proqram paketinin Neural Network Toolbox paketinin köməyilə yerinə yetirilmişdir. Sonda kəmiyyət və keyfiyyət göstəricilərinə görə adekvat nəticələrin əldə olunmasına dəstək verən işləmə mexanizmi təklif olunmuşdur.

1. İnformasiya təhlükəsizliyi sahəsində risklərin rolu

Risk sözün ümumi mənasında müəyyən qərarlar və ya hərəkətlər nəticəsində mənfi və ya müsbət nəticələri olan hadisələrin baş vermə ehtimalı və ya prosesi kimi başa düşülür. Bu proses məlumat risklərinin vaxtaşırı təhlilinə əsaslanır ki, bu da vaxtında informasiya təhlükəsizliyinə təhdidləri, informasiya sisteminin zəifliklərini müəyyən etmək, onların zərərsizləşdirilməsi üçün müvafiq tədbirlər görmək və nəticədə əvvəlki təcrübəni və yeni təhdid və zəiflikləri nəzərə alaraq təşkilatda informasiya təhlükəsizliyinin vəziyyətinə daim nəzarət etmək imkanı verir (Amiraslanova, 2020: 39-40). Bütün risklər təsadüfi hadisələrdir ki, bu da çox vaxt onlar haqqında keyfiyyətli məlumatın olmaması ilə bağlıdır. Bütün zəruri məlumatların əldə edilməsi müvafiq alətlərin olmaması, məlumatların toplanması və emalı üçün vaxt, xarici qüvvələrin hərəkəti, habelə risk proseslərinin və ya hadisələrinin təbiəti haqqında tam elmi biliklərin olmaması ilə məhdudlaşır (Mustafayeva, 2022: 57-59).

Risk insan fəaliyyətinin istənilən sahəsinə xasdır ki, bu da insanların qərarlarının nəticələrinə təsir edən bir çox şərait və amillərlə bağlıdır.

Riskin qiymətləndirilməsi ən çox iqtisadi, təbii, siyasi və hərbi fəaliyyət sahələrində istifadə olunur. İnformasiya təhlükəsizliyi sahəsində risklər keçən əsrin sonlarında kompüter texnologiyalarının inkişafı nəticəsində emal olunan məlumatların həcminin artması ilə əlaqədar olaraq diqqəti cəlb etməyə başladı. İnformasiya təhlükəsizliyi sahəsində risklərin idarə edilməsi özünəməxsus xüsusiyyətlərə malikdir. Bununla belə, normativ sənədlərdə və metodiki ədəbiyyatlarda istifadə olunan terminologiyada, standart risklərin qiymətləndirilməsi prosedurlarının tərkibində və qiymətləndiriləcək parametrlər toplusunda tez-tez uyğunsuzluqlar olur. Bu, informasiya sistemlərinin süni 51ntellektin tətbiqilə təhlükəsizlik riskinin qiymətləndirilməsinin mövzu sahəsini təhlil etməyi zəruri edir.

2. Problemin qoyuluşu

Rəqəmsallaşdırılmış cəmiyyətdə "informasiya təhlükəsizliyi riski" və ya "informasiya riski" termini çox geniş istifadə olunur. Lakin hələ də əksər alim və tədqiqadçılar tərəfindən qəbul edilən ümumi vahid konsepsiyanın şərhi yoxdur. Elmi işdə araşdırılan aktual problemlər aşağdakıları əhatə edir:

- müəssisənin informasiya sistemində onun fəaliyyətinin pozulmasına, məlumatın keyfiyyətinin aşağı düşməsinə səbəb olan təsadüfi hadisənin baş verməsi, nəticədə ziyan vurması ehtimalı;
- informasiya texnologiyalarından istifadə nəticəsində itki və ya zədələnmə riski;
- informasiya təhlükəsizliyinin pozulması ilə bağlı zərərin mümkünlüyünü nəzərdə tutan qeyri-müəyyənlik;
- aktivin zəifliyindən istifadənin potensial təhlükəsi, bununla da təşkilata zərər vurması (Ajmuxamedov, 2012: 59).

Təhdid - informasiya təhlükəsizliyinin pozulmasının potensial və ya real təhlükəsini yaradan şərait və amillər məcmusu kimi başa düşülür. İS-in təhlükəsizliyinə təhdid məlumatın məxfiliyini, bütövlüyünü və əlçatanlığını pozmaq üçün üçüncü şəxslər tərəfindən ona icazəsiz daxil olmaqdan ibarət ola bilər. İnformasiya sistemlərinin təhlükəsizliyinə təhdidlərin həyata keçirilməsinin nəticələrinin müəyyən edilməsi, dəf edilməsi və aradan qaldırılmasına yönəlmiş mühafizə tədbirlərinin, habelə onlara əsaslanan fəaliyyətlərin məcmusu *informasiya təhlükəsizliyi sistemi* adlanır.

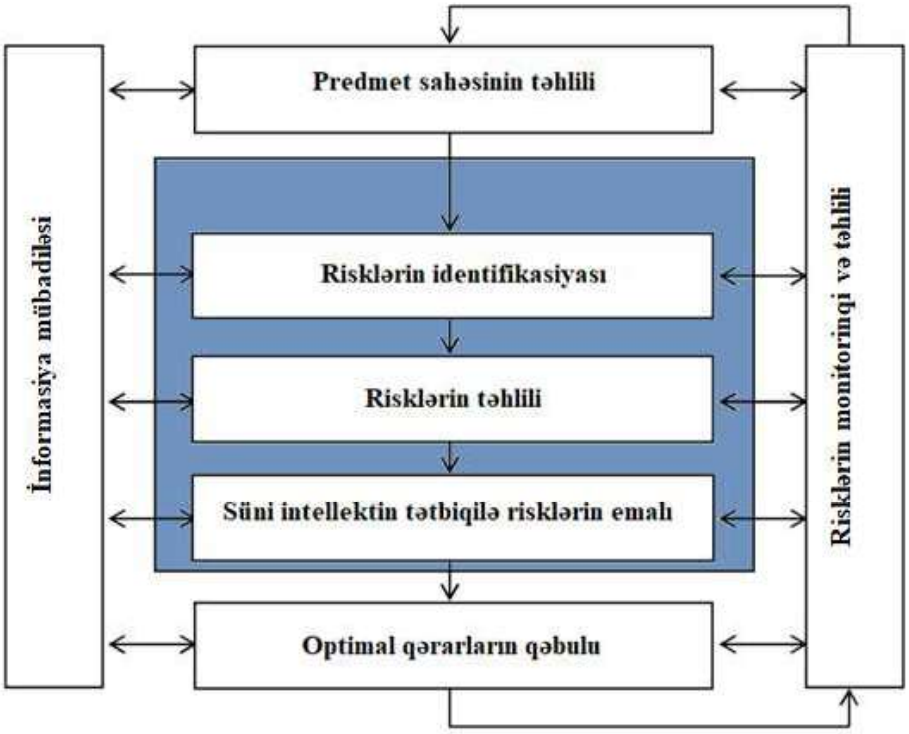
Klassik idarəetmə sistemlərində informasiya təhlükəsizliyinin qorunması mexanizmi – qoruyucu tədbirlər toplusu, yəni, təhlükəsizliyi təmin edə bilən, zəifliyi azalda bilən, təhlükəsizlik sistemində insidentin təsirini məhdudlaşdıran hərəkətlər, prosedurlar və mexanizmlərdir. Qoruyucu tədbirlər həm təhdidlərin reallaşma ehtimalını azaltmağa (zəifliklərı aradan qaldırmaq və ya istifadəsini çətinləşdirməklə), həm də təhdidlərin həyata keçirilməsinin nəticələrinin (zərərin) miqyasını azaltmağa yönəldilə bilər (Baranova, 2016: 91-93).

Nəticələr dedikdə, risk hadisəsi (təhlükənin reallaşması) nəticəsində müəssisənin üzləşə biləcəyi müxtəlif maddi və qeyri-maddi itkilər başa düşülür. Riskli hadisənin bütün nəticələrinin keyfiyyət və ya kəmiyyət (xərc) qiymətləndirilməsi zərərin məbləği adlanır.

Ancaq praktikada ən geniş yayılmış risk qiymətləndirilməsi, mahiyyəti əvvəlcədən formalaşmış keyfiyyət şkalaları üzrə risk parametrlərinin (təhlükənin yaranması ehtimalı, zəiflikdən istifadə ehtimalları və zərərin məbləği) dəyərlərinin kompüter riyaziyyatı sistemlərinin bir istiqaməti olan süni intellekt proqramlarının tətbiqi ilə müəyyənləşdirilməsindən ibarətdir (Buldakova, 2013: 298-305).

Klassik nümunə "yüksək", "orta" və "aşağı" dəyərləri ilə risk parametrlərinin qiymətləndirilməsi üçün üç səviyyəli ölçüyə malikdir. Risk səviyyəsi xüsusi matrislə müəyyən edilir, hansında ki, mümkün risk səviyyəsi onun parametrlərinin qəbul etdiyi dəyərlərin kəsişmələrində qoyulmuşdur.

Süni intellektin tətbiqilə riskin qiymətləndirilməsi daxil olan məlumatların (aktivlər, təhlükələr, zəifliklər və s. haqqında məlumat) çıxış məlumatlarına (siyahı və risk qiymətləri) çevirən bir alt prosesdir. Riskin qiymətləndirilməsi prosesi ardıcıl prosedurlardan ibarət olub riskləırin müəyyən edilməsi, təhlili və müqayisəsini əhatə edir (şəkil 1).



Şəkil 1. Süni intellektin tətbiqilə risklərin qiymətləndirilməsi metodikası

Riskin identifikasiyası aktivlər (mühafizə obyektləri), zəifliklər, həyata keçirilən qoruyucu tədbirlər, təhdidlər, təhlükə mənbələri və nəticələri haqqında məlumat toplamaq məqsədi ilə həyata keçirilir. Risklərin təhlili zamanı parametrlərin dəyərləri müəyyən edilir: təhlükə ehtimalı, zəiflikdən istifadə ehtimalı, zərərin miqyası və s. Risklərin əhəmiyyətini müəyyən etmək üçün müəyyən edilmiş səviyyələrlə risklərin müqayisəli qiymətləndirilməsi proseduru həyata keçirilir.

3. İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodikası

Riskin qiymətləndirilməsi prosesi İnformasiya təhlükəsizliyi sisteminin həyat dövrünün bütün mərhələlərində tətbiq oluna bilər. Riskin kəmiyyət və keyfiyyət qiymətləndirilməsi prosesinə əlavə olaraq, risklərin idarə edilməsi çərçivəsində aşağıdakı proseslər fərqləndirilir (He, 2011: 778).

- əhatə dairəsinin (kontekstinin) müəyyən edilməsi risklərin qiymətləndirilməsi və qəbul edilməsi meyarlarını, habelə risklərin idarə edilməsi prosesinin sərhədlərini və əhatə dairəsini müəyyənləşdirilməsi;
- risk müalicəsi riskin dəyişdirilməsi tədbirlərinin seçilməsi və həyata keçirilməsi prosesi;
- risklər haqqında məlumat mübadiləsi risklərin idarə edilməsi prosesinin bütün aspektləri üzrə iştirak edən tərəflər arasında razılığın əldə edilməsinə yönəldilməsi;
- risklərin qiymətləndirilməsinə və risklərin müalicəsi ilə bağlı qərarların qəbul edilməsinə təsir edən amillərdə dəyişikliklərə nəzarət etmək məqsədilə risklərin monitorinqi və təhlilin aparılması (Mustafayeva, 2022: 58).

İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodikası kompüter riyaziyyatının ən geniş istifadə olunan Matlab proqram paketinin köməyilə yerinə yetirilmişdir (Qluşenko, 2013: 37). Qiymətləndirmə Matlab proqramına daxil olan NEURAL Network Toolbox proqram modulundan istifadə etməklə daxili prosedurlar şəklində, müəyyən biliklər bazasının formalaşması əsasında aparılmışdır. Sonda kəmiyyət və keyfiyyət göstəricilərinə görə əldə olunmuş adekvat nəticələr sistemin təhlükəsizliyinin təmini risklərini yüksəldir və nəzarətdə saxlamağa imkan verir (Sakhno, 2018: 32).

Müxtəlif neyropaketlərin təhlil nəticələrinə görə, informasiya sisteminin təhlükəsizliyini təhlil etmək üçün Matlab sisteminin NEURAL Network Toolbox paketi seçilmişdir. O, qoyulmuş məsələnin həlli üçün optimal sistemin axtarış prosesini avtomatlaşdırmaq imkanına malikdir. Neyron şəbəkədən istifadə edərək, informasiya sisteminin təhlükəsizliyinin qiymətləndirilməsi mərhələləri aşağıdakı kimi təsvir olunur (Qaluşkin, 2011: 38).

1. *Neyron şəbəkənin tətbiqi probleminin qoyuluşu.* Problemin həlli üçün neyron şəbəkədən istifadənin məqsədəuyğunluğu haqqında ilkin fərziyyələrin irəli sürülməsi.
2. *Şəbəkə topologiyasının seçimi.* Problem və təlim üçün mövcud verilənlərə əsaslanaraq şəbəkə tipini seçilməsi
3. *Şəbəkə xüsusiyyətlərinin seçilməsi.* Şəbəkə parametrləri eksperimental olaraq seçilir: təbəqələrin sayı, gizli təbəqələrdəki blokların sayı, giriş əlaqələrinin olması və ya olmamasının təyini, neyronların ötürmə funksiyaları və s.
4. *Verilənlərin seçilməsi, təlim nümunəsinin formalaşdırılması*. Təlim nümunəsinə neyrosistemin gələcək istifadəsi şərtlərinə yaxın olan şərtləri təsvir edən məlumatlar daxildir.
5. *Təlim parametrlərinin seçilməsi*. Təlim parametrlərinin dəyərləri təlimin tamamlanması meyarına (məsələn, xətanın minimuma endirilməsi və ya məşq vaxtının məhdudlaşdırılması) əsaslanaraq eksperimental olaraq seçilir.
6. *Neyron şəbəkənin öyrədilməsi*. Neyron şəbəkənin təlimi təlim məlumatlarının şəbəkə sisteminə təqdim edilməsi prosesindən ibarətdir.
7. *Təlimin adekvatlığının yoxlanılması.* Neyron şəbəkənin təlim keyfiyyətinin yoxlanılması onun təlimində iştirak etməyən nümunələr üzrə aparılır. Əldə edilən nəticələr gözlənilənlərdən əhəmiyyətli dərəcədə fərqlənirsə, problemin qoyuluşuna qayıtmaq lazımdır (Schrieber, 2014: 642)

Süni intellektin müdafiəsini qiymətləndirərkən ekspert qiymətləndirmələrindən istifadə etmək lazımdır. Qiymətləndirmə aşağıdakı tələbləri ödəməlidir:

- yoxlanılan təşkilatın daxili normativ sənədləri və zərurət olduqda təşkilatın informasiya təhlükəsizliyinin təmin edilməsinə aid üçüncü şəxslərin sənədləri;
- aparılan sorğular zamanı yoxlanılan təşkilat əməkdaşlarının şifahi fikirləri;
- ekspert qrupu üzvlərinin yoxlanılan təşkilatın əməkdaşlarının fəaliyyətinə dair müşahidələrinin nəticələri;
- yoxlanmış təşkilatın IP ekspertləri tərəfindən sorğunun nəticələri;
- ekspertlər tərəfindən təhlükəsizliyin təhlili üçün instrumental vasitələrdən istifadənin nəticələri.

Nəticə

İnformasiya təhlükəsizliyi riskinin qiymətləndirilməsi risklərin qəbulu meyarlarına və təşkilata aid olan məqsədlərə uyğun olaraq riskləri müəyyən etməyə, kəmiyyətləndirməyə və prioritetləşdirməyə kömək edən müəssisələrin idarəetmə təcrübələrinin mühüm hissəsidir. Risklərin idarə edilməsi məlumat sisteminə potensial olaraq təsir göstərə bilən təhlükəsizlik risklərini azaltmaq üçün informasiya sisteminin resurslarına mənfi təsir göstərə biləcək proseslər araşdırılmış və müəyyən təkliflər verilmişdir.

Kibertəhlükəsizlikdə süni intellektin rolu və təşkilatların kibertəhlükəsizlikdə süni intellektdən necə faydalanması ilə bağlı tövsiyələr təklif edilmiş və Neyron şəbəkənin tətbiqilə bağlı alqoritmlərin təhlili verilmişdir.

İnformasiya təhlükəsizliyinin qiymətləndirilməsinin ümumi sxemi əsasında mərhələlər üzrə təhlükəsizliyinin təhlili metodologiyası hazırlanmışdır ki, onun istifadəsi nəinki təhlükəsizlik səviyyəsini, habelə effektivliyini qiymətləndirməyə imkan verir.

Ədəbiyyat

1. Hümbətəliyev, R. (2021), Kompüter riyaziyyatı sistemlərinin tətbiqilə informasiyanın mühafizəsi metodologiyası // The XXI International Scientific Symposium "Science and Culture in the Modern World" dedicated to the Day of Solidarity of World Azerbaijanis, İnternational Scientific Center «Elger», Stokholm /Sweden, s.282-285.
2. Amiraslanova, R. (2020), Features of computer math // XVI İnternational Correspondence scientific specialized conference "İnternational Scientific reviewof the technical sciences, mathematics and computer sciences // Boston. USA: Boston Massachusetts. p.38-44.
3. Ajmuxamedov, I. (2012), Otsenka povrojdeniy bezopasnosti informatsionnoy sistemy na osnove necotko-koqnotiqnogo podkhoda // Voprosy zashchity informatsii. №1.s. 57–60
4. Amiraslanova, R. (2019), Metody i sposoby obrabotki i primeneniya dannix v komputernoy matematike // Moskva: Yevraziyskiy Soyuz Uchenyx (ECY), №10 (67). s. 16-20
5. Baranova, K. (2016), Metody analiza riskov informatsionnoy bezopasnosti s ispolzovaniyem logiki na baze instrumentaiya Matlab // Obrazovatelnie resursy i texnologii. №1 (13). s. 88–96.
6. Buldakova, T. (2013), Otsenka informatsionnykh riskov v avtomatizirovannix sistemax s pomosyu neyron-noçotkix modeley // Nauka i obrazovaniye: MGTU. N.E. Baumana. № 11. s. 295–310.
7. Glushchenko, S. (2013), Primeneniye sistem MATLAB dlya otsenki riskov informatsionnoy bezopasnosti organizatsii // Biznes-informatika. № 4 (26). s.35–42.
8. Galushkin, A. (2011), Neyrokomputery v reshenii zadachi obespecheniya informatsionnoy bezopasnosti // Informatsionnyye texnologii. №1. s.34–38.
9. Dolzhenko, A. (2009), Model analiza riska potrebitelskogo kacestva proyektov ekonomiceskix informatsionnix sistem // Vestnik Severo-Kavkazskogo gosudarstvennogo texnicheskogo universiteta. №1 (18). s.129-134.
10. Mustafayeva, A. (2022), Analiz riskov informatsionnoy bezopasnosti. Innovatsionnyye naucnyiye issledovaniya. Setevoye izdaniye, Naucniy jurnal. № 1-1 (15), ISSN 2713-0010, s.56-62.
11. Sakhno, V. (2018), Primeneniye metodov nelogicheskoy logiki dlya resheniya zadachi obespecheniya informatsionnoy bezopasnosti / Molodoy issledovatel. Dona №4(13) Rostov-na-Donu: Izdatelskiy sentr DGTU, s.28-35
12. Schrieber, M. (2014), Hardware Implementation of a Novel Inference Engine for Interval Type-2 Fuzzy Control on FPGA // IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Beijing, China. - USA, Piscataway, NJ: IEEE. p. 640-646.
13. He, Y. (2011), Risk assessment of urban network planning in china based on the matter-element model and extension analysis /International Journal of Electrical Power & Energy Systems. p.775-782

Rəyçi: tex.ü.f.d. Aidə Mustafayeva

Göndərilib: 06.04. 2022 Qəbul edilib: 12.05. 2022