Süni İmmun Sistemləri Əsasında Tibbi Təyinatlı Proqram Sisteminin Kibertəhlükəsizliyinin Təmin Edilməsi Alqoritmi

Şəfəqət Mahmudova
ETN İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shafagat@gmail.com

***Xülasə*— Məqalədə süni immun sistemləri əsasında tibbi təyinatlı proqram sisteminin (PS) kibertəlükəsizliyini təmin etmək üçün alqoritm işlənilmişdir. Süni immun sistemi nəzəri immunologiyada problemlərin həlli üçün istifadə olunan modellərdən, prinsiplərdən, mexanizmlərdən və funksiyalardan istifadə edən adaptiv hesablama sistemidir. Onun müxtəlif elm sahələrinə tətbiqi araşdırılmışdır. Süni immun sistemlərinin proqram sistemi üçün oynadığı rol əvəzsizdir. Süni immun sistemi sahəsində olan bəzi ədəbiyyatların təhlili aparılmış, həll olunası məsələlər müəyyənləşdirilmişdir. Bayes metodu müəyyən şərt daxilində hər hansı bir hadisənin olma ehtimalını dəqiq hesablamağa icazə verir. İşdə süni immun sistemlərdən istifadə etməklə tibbi təyinatlı proqram sisteminə Bayes metodunun tətbiqi bununla əlaqədardır. Bunun üçün alqoritm işlənilmişdir. Eksperimentlərin nəticəsi qənaətbəxş olmuşdur.**

***Açar sözlər*— süni immun sistemi; tibbi təyinatlı; proqram sistemi; kibertəhlükəsizlik; Bayes metodu; ziyanlı proqramlar**

I. GİRİŞ

İnformasiya texnologiyalarının inkişafı bir çox elm sahələrinin inkişafına səbəb oldu. İnsan orqanlarının işləmə prinsiplərinə əsaslanan texnologiyalar geniş vüsət aldı: süni intellekt metodları, vizual görüntülərin işlənmə vasitələri, süni torlu qişa, bütün növ genetik alqoritmlər və s. İmmun sistemlərinin iş prinsipləri əsasında qurulmuş informasiya sistemləri bir çox sahələrdə böyük potensiala malikdir [1].

Tibdə immun sistemi uyğunlaşdırıla bilən mürəkkəb müdafiə mexanizmlərinin kompleksidir, onun əsas funksiyası bədəni zərərli və xarici maddələrdən, toksinlərdən, mikroorqanizmlərdən və zərərli hüceyrələrdən müdafiə etməkdir.

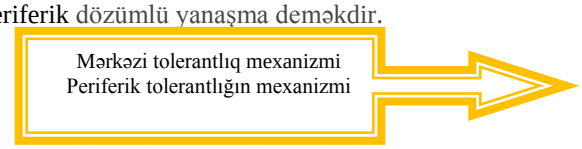
Canlı orqanizmin təhlükəli xarici və daxili amillərə davamlı təsirindən müdafiəsi immun sisteminin inkişafını təmin edir. İmmunitet sistemi endogen maddələrə dağıdıcı cavab verir və bədənin öz toxumalarına mənfi təsir göstərmir [2].

Endogen intoksikasiya (Eİ) onların yaranma mənbəyinə çevrilmiş xəstəlikdən (zədə, radiasiya, infeksiya, iltihab), orqanizmdə toksiki məhsulların yığılmasına gətirən fizioloji sistemdən (bağırsaq, böyrək) asılı olaraq təsnif edilir.

İmmunoloji reaksiyaların çoxu qısa ömürlüdür və çox güclü reaksiyaya mane olan tənzimləyici mexanizmlər tərəfindən idarə olunur.

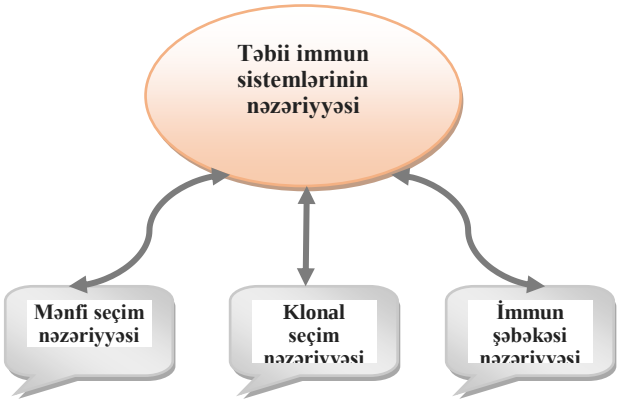
Dözümlülük immun sisteminin öz vücuduna qarşı yönəldilən dağıdıcı reaksiyalara yol vermədiyi mexanizmlər kompleksidir.

Tolerantlığın iki mexanizmi şəkil 1-də göstərilmişdir. Periferik dözümlü yanaşma deməkdir.



Şəkil 1. Tolerantlığın iki mexanizmi.

Bütün ibtidai limfoid orqanlarda yerləşən və bədənin öz antigenlərinə qarşı hərəkət edən əksər limfositlər mərkəzi dözümlülük mexanizmləri ilə məhv edilir. İmmunologiya, immun sisteminin quruluşu və işləmə qaydaları, xəstəlikləri və immunoterapiya üsulları elmidir. Bədənin hər hansı bir xarici maddəyə qarşı özünümüdafiəsinin bioloji mexanizmlərini öyrənir. Süni immun sistemi (SİS) nəzəri immunologiyada təsvir və tətbiq olunan problemlərin həlli üçün istifadə olunan modellərdən, prinsiplərdən, mexanizmlərdən və funksiyalardan istifadə edən adaptiv hesablama sistemidir. Təbii immun sistemlərinin tam öyrənilməməsinə baxmayaraq, bu gün immun sisteminin fəaliyyətini və onun elementlərinin qarşılıqlı təsirini izah edən ən azı üç nəzəriyyə mövcuddur (şəkil 2):



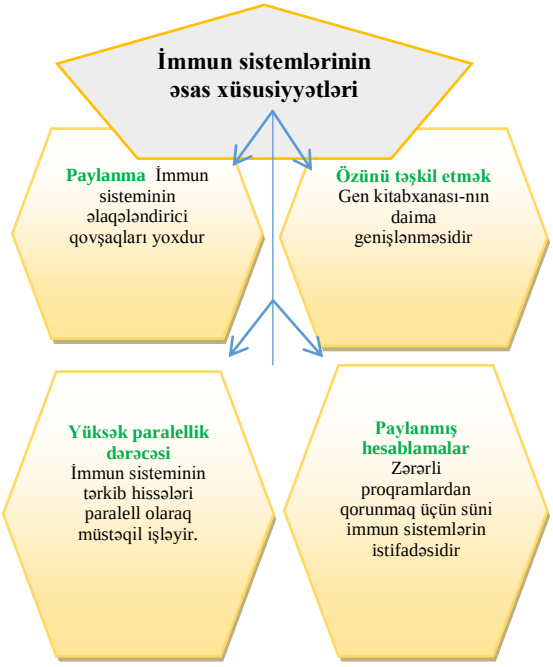
Şəkil 2. Təbii immun sistemlərinin nəzəriyyəsi.

SİS 1980-ci illərin ortalarında Fermer, Packard Perelson 1986, Bersini, Varela 1990-cı ildə immunitet şəbəkələrinə aid yazdıqları məqalələrdə ortaya çıxdı. Bununla birlikdə SİS-in əsasları yalnız 1990-cı illərin ortalarında qoyuldu. Forrest və

DOI: 10.25045/SPCDH4.0.2025.41

Kephart [3] SİS haqqında ilk məqalələrini 1994-cü ildə nəşr etdilər və Dasgupta mənfi seçim nəzəriyyəsi ilə bağlı geniş araşdırma apardı. Hun Cooke 1995-ci ildə immun şəbəkəsi nəzəriyyəsi üzərində işə başladı. Timmis və Neal bu işi davam etdirdi və işi daha da təkmilləşdirdilər. Süni immun sistemlərinə dair ilk kitab 1999-cu ildə Dasqupta tərəfindən redaktə edilmişdir [4].

İnsanların orqanları kimi eyni prinsiplərə əsaslanan texnologiya bu gün geniş yayılmışdır: neyronşəbəkələrə əsaslanan süni intellekt, vizual görüntünün emal vasitələri, süni torlu qişa, müxtəlif genetik alqoritmlər və s. İmmunitet prinsipləri əsasında qurulmuş informasiya sistemləri bir çox sahələrdə böyük potensiala malikdir. Hazırda süni immun sistemlər əsasən bir növ süni intellekt sistemlərindən istifadə edir, lakin kompüter viruslarına qarşı mübarizə üçün toxunulmazlıq prinsipi üzərində işləyən müdafiə sistemlərindən istifadə etdir, şəbəkə müdaxilələrini aşkar edir və s. Burada başqa bir prosesdə baş verir - klonal seleksiya antitellərin bir növ təbii seleksiyasının baş verdiyi yerdir: yalnız aşkar olan xarici cisim altında yaşayanların yalnız sağ qalmasıdır. Eyni zamanda, yaranan antikorlarla (immunitet sisteminin bədənə qarşı təhdidləri müəyyən edib yox etməsinə kömək edən zülallara deyilir) bağlı məlumatlar yuxarıda göstərilən gen kitabxanasına daxil edilir. Beləliklə, gen verilənlər bazası yalnız təhlükə ilə qarşılaşa bilən məlumatları ehtiva edir.Vacib olan immunitet sisteminin əsas xüsusiyyətləri şəkil 3-də göstərilmişdir.



Şəkil 3. İmmun sisteminin əsas xüsusiyyətləri.

Bu mərkəzləşdirilmiş yüksək səviyyədə paralel paylanmış məlumatların emalı və analiz sistemidir və xüsusilə paylanmış hesablama mühitlərinin qorunması üçün əlverişlidir. SİS-in aşağıdakı alqoritmləri vardır:

Klonal seçim alqoritmi - B və T lenfositlərin antigenlərə qarşı reaksiyasını zamanla yaxşılaşdırdıqlarını izah edən, əldə edilmiş toxunulmazlığın klon seçimi nəzəriyyəsinə əsaslanan alqoritmlər sinfidir. Bu alqoritmlər Darvin nəzəriyyəsinin atributlarına əsaslanmışdır, burada seçim antigenlərin və antitellərin qarşılıqlı təsirinə, hüceyrələrin bölünməsi prinsipinə və somatizasiyaya (stres kimi psixi faktorların fiziki simptomlara, daha çox ağrı, ürək bulanması, boğulma hissi və s. səbəb olması) əsaslanır.

Mənfi seçim alqoritmi - ən pis variantın seçimidir. Mənfi seçim, tibbi xidmətə ehtiyacı olan insanların sığorta almaq ehtimalı yüksək olduqda baş verir.

Immun .şəbəkəsi - İmmun sistemi orqanlar, ağ qan hüceyrələri, zülallar (antikorlar) və kimyəvi maddələrdən ibarət geniş bir şəbəkədir. Bu sistem insanı infeksiyalara, xəstəliklərə və narahatlığa səbəb olan xarici cisimlərdən (bakteriyalar, viruslar, parazitlər və göbələklər) qorumaq üçün şəbəkə şəklində işləyir.

SIS, immun sisteminin prinsipləri və proseslərinə əsaslanan avtomatlaşdırılmış hesablama sistemləri sinfidir. Tipik olaraq, bu cür alqoritmlər problemi həll etmək üçün immun sisteminin yaddaşından və öyrənmə qabiliyyətindən istifadə edir.

II. ƏDƏBİYYATLARIN MÜZAKİRƏSİ

İmmun sistemlərdən istifadə edərək kompleks texnoloji problemlərin həllinə yönəldilmiş bir çox tədqiqat işləri aparılmışdır. Onların arasında anormal aşkarlama, obrazların tanınması, sistem kibertəhlükəsizliyi və məlumatların toplanması bu strukturda həll olunmuş problemlərdən hesab olunur. Böyük həcmli proqram sistemlərini idarə və nəzarət etmək çətindir. Bir çox hallarda, bu sistemlərdə xüsusilə yeniləmə və ya onların ətraf mühitində dəyişikliklər baş verdikdən sonra (məsələn, əməliyyat sistemi yeniləndikdə və s.) gözlənilməz davranışlar baş verə bilir. Buna görə dəyişən mühitdə bunun qarşısını almaq üçün, özünü adaptiv metodlarla səhvin aşkarlanması və performansın monitorinqinə ehtiyac vardır [5]. Proqram səhvlərinin aşkarlanması ilə təbii immun sistemlərdə aşkar edilən patogen (hər hansı orqanizm sisteminə zərər verə bilən və xəstəliyin inkişafına səbəb ola biləcək bir ekoloji amil kimi başa düşülür) mikroorqanizmlərin aşkarlanması problemi arasında oxşarlıqlar vardır. Bu sistemlərdə müşahidə edilən peyvənd və mənfi klonal seçimlərdən istifadə edərək sistem resurslarının göstəricilərini təhlil edərək proqram təminatlarının monitorinqi üçün effektiv adaptiv model hazırlanmışdır.

Süni intellekt (Sİ) maşın və proqram təminatında insanın zəkasını əks etdirir. Bu, bir çox müasir tədqiqat sahələrində çox arzu olunan akademik sahədir. Sİ-nin aparıcı tədqiqatçıları bu sahəni "ağıllı agentləri öyrənmək və dizayn etmək" kimi təsvir edirlər. McCarthy termini 1955-ci ildə icad etdi və onu "ağıllı maşınların yaradılmasının elm və texnologiyası" olaraq təyin etdi. Sİ tədqiqatının əsas məqsədləri təfəkkür, bilik, planlaşdırma, təlim, təbii dildə işləmə (ünsiyyət), qavrayış və obyektlərin hərəkət və manipulyasiya etmək bacarığıdır. Əslində, Sİ -nin fənlərarası sahəsi olduqca genişdir və bir çox elm və peşəni, o cümlədən kompüter elmləri, psixologiya, dilçilik, fəlsəfə, nevrologiya və s. sahələri əhatə edir. Bu sahə insanların mərkəzi intellektual mülkiyyəti olaraq Homo

Sapiensin "intellekt zehni o qədər dəqiq təsvir edilə bilər ki, onu modelləşdirmək üçün bir maşın yaradıla bilər" fikri üzərində quruldu. Sİ böyük mövzu idi, eyni zamanda uğursuzluqlarla da üzləşdi [6].

Siqnallar ilə kəsişmələrdə aralıq trafikə nəzarət etmək və optimallaşdırma metodlarına və süni zəkaya əsaslanan bir neçə yol siqnalının idarəetmə sistemi hazırlanmışdır. Təklif olunan sistem, müasir trafik modelləşdirmə proqramı olan VISSIM-dən (dinamik sistemlərin modelləşdirilməsi üçün hazırlanmış vizual proqramlaşdırma dilidir) istifadə edərək modelləşdirilmiş kəsişməyə tətbiq olunur. Nəticələr təklif olunan sistemin rəqabət qabiliyyətli olduğunu və müxtəlif trafik ssenarilərini idarə etməyə qadir olduğunu və yüksək trafik axını ilə əlaqəli ekstremal vəziyyətlərdə istifadə üçün tövsiyə olunduğunu göstərir [7]. İnsan bədəninin immun sistemi bir çox zərərli virus və xarici cisimlərdən qorunmaq üçün böyük potensiala malikdir. Tarix boyu insanlar mikroorqanizmlərə (Mikroorqanizmlər və ya mikroblar adətən ölçüləri 0,1 mm-dən az, gözlə görünməyəcək qədər kiçik olan canlı orqanizmlərin ümumi adı) yoluxmuşdur. Bu mikrobial (mikroblarla bağlı çox kiçik canlılar, xüsusən də xəstəliyə səbəb olanlar) mikrob biotexnologiyasının ölçüsünü və intensivliyini məhdudlaşdırmaq üçün insanlar onlarla mübarizə etmək xüsusiyyətlərinə malikdir. İnsanın immun sistemi bədəni, dərini, hüceyrələri və toxumaları xarici maneələrdən qorumağa qadirdir. [8]-də adaptiv immun sistemlərinin riyazi modelləri vasitəsilə insanın immun sisteminin öyrənilməsinə dair nümunə təqdim olunur. Bədəndə bərpa mexanizmi meydana gəldikdə xarici hissəciklərin təsirini öyrənmək üçün geniş simulyasiyalar (tədqiq olunan sistemin həqiqi sistemi kifayət qədər dəqiqliklə təsvir edən bir modellə əvəz olunduğu tədqiqat metodu) aparılmışdır. Əldə olunan nəticələr insanın immunoloji riyazi modelinin etibarlılığını əsaslandırır. İnsan bədənində təhlükəsizlik və məxfiliyin olması güclü şəbəkə sisteminin yaradılmasına kömək edə biləcəyini müdafiə edir [8]. Dinamik risk identifikasiyası mümkün risk məlumatlarına əsaslanaraq gələcək riskləri proqnozlaşdırmaq üçün istifadə olunur. Qeyri-səlis istinad vektor sistemi (fuzzy support vector machine, FSVM) modelinə əsaslanan risk identifikasiya texnologiyasının təlim modelindən istifadə etməklə mümkün riskləri tam və avtomatik müəyyən edə bilir və bu texnologiya dinamik risk identifikasiyasının əsas metoduna çevrilmişdir. Tanınmanın səmərəliliyini və dəqiqliyini artırmaq üçün FSVM parametrlərinin seçilməsi çox vacibdir. Süni immun alqoritmi (artificial immune algorithm AIA), stoxastik qlobal optimallaşdırma üçün effektiv bir texnologiyadır və yüksək dəqiqlik, yaxınlaşma dərəcəsinin üstünlüklərinə malikdir. Buna görə, [9]-da FSVM və immun optimallaşdırma alqoritminin (immune optimization algorithm , IOA) inteqrasiyasına əsaslanan yeni bir dinamik risk identifikasiya modeli təklif edilmişdir. [10]-da şəbəkəyə müdaxilələrin aşkar edilməsi üçün hibrid modeli təqdim edilir, belə ki, informasiyanın qorunmasının ənənəvi metodlarıyla süni immun sistemi metodlarını uyğunlaşdırır. Anomaliyaların aşkar edilməsi funksiyasının köməyi ilə şəbəkədə təhlükələrinin tanınması, yanlış istifadə və immunoloji təhlükənin modelinə əsaslanan anadangəlmə immun funksiyasına şəbəkənin monitorinqi əsasında müdaxilələrin aşkar edilməsi üçün proqramları özünə daxil edir. Sınaqlar yanlış istifadə əsasında müdaxilələrin aşkar edilməsiylə müqayisədə aşkar etmənin yaxşılaşdırılmış dəqiqliyini müəyyən edir. Sonrakı tədqiqat və modelin yaxşılaşması üçün vacib olan sahələr müzakirə edilir. Ədəbiyyatların təhlilindən göründüyü kimi, süni immun sistemlərinin müxtəlif sahələrə tətbiqi çox əhəmiyyətlidir və effektiv nəticə verir. Süni immun sisteminə əsaslanan müdafiə sistemlərinin üstünlükləri və mənfi cəhətləri cədvəl I-də göstərilmişdir.

CƏDVƏL I. SÜNİ İMMUN SİSTEMİNƏ ƏSASLANAN MÜDAFİƏ SİSTEMLƏRİNİN ÜSTÜNLÜKLƏRİ VƏ MƏNFİ CƏHƏTLƏRİ

Üstünlükləri	Çatışmazlıqları
Çox sayda detektorun ((xüsusi maddə və ya hadisəni aşkar edən cihazlar) olması davamlılığa və sistemin etibarlılığına gətirib çıxarır.	Autoimmun (orqanizmdə immun sisteminin iş prinsipinin pozulması ilə əlaqədar meydana çıxan xəstəliklərdir) reaksiyası mümkündür.
İmtinanın (rəddin) vahid nöqtəsi yoxdur.	Mümkün autoimmun reaksiyasının olmasıdır.
Təklif olunan sistemdə paylanmış hesablama mühitinin düyün nöqtələrinin sayılarının artması təhlükəsizlik səviyyəsinin artmasına da səbəb olur.	İmmun çatışmazlığı xüsusilə paylanmış hesablama mühitində az sayıda qovşaqda mümkündür.
Dedektorların zərərli obyektlərlə bütün toqquşmaları yaddaşda saxlanılır. Bu detektorların təliminə imkan verir.	

III. ZİYANLI PROQRAM SISTEMİNİ AŞKARLAMAQ ÜÇÜN METODLAR

Sistemlərin informasiya təhlükəsizliyi üçün ən ciddi təhlükələrdən biri də ziyanlı proqram sistemləridir (ZPS). ZPS kompüterdən gizli məlumatları oğurlaya bilər, fayllara yoluxa bilər, kompüter və ya bütün lokal şəbəkə boyunca yayıla bilər, məxfi məlumatların itkisinə səbəb ola bilər, ziyanvericilik məqsədilə saxlanılan bütün məlumatları şifrləyə bilər, məlumat sahiblərinə iqtisadi cəhətdən çox zərər verə bilər və s. Zərərli proqramların fəaliyyətinin qarşısını almaq üçün ən qısa zamanda onlar kompüterdə aşkar edilməli və silinməlidir [11].

ZPS şərti olaraq viruslara, qurdlara, troyanlara, casus proqramlarına, reklam proqramlarına və s. bölünə bilir [12].

1. Gizlətmə metodları. Bu üsullar vasitəsilə proqramın semantikasını dəyişdirmədən onun sintaksisini dəyişdirir və bu zərərli kodları təhlil etmək və anlamaq daha çətin olur [13]. Bu, dəyişənlərin yerləşdirildiyi registrləri dəyişdirməklə əldə edilə bilər, proqramın kodu isə eyni olaraq qalır; təlimatları digər zərərli təlimatlarla işləyən prosesin icrası qaydasını mübadilə təlimatları ilə dəyişir və s.

2. Şifrələmə kodu. ZPS şifrələnməsinə parolu deşifrə / şifrələmə əməliyyatları, şifrələmə açarları və xüsusi şifrələnmiş zərərli kodun özü daxildir.

3. Şifrəli ZPS şərti olaraq aşağıdakı növlərə bölünə bilər:

- Oligomorfik (viruslu) proqramlar, şifrələmə, kodun bəzi xarakteristikalarını, məsələn, ZPS-nin sinyalizasiya (mərkəzləşdirilmiş) sistemləri tərəfindən aşkar edilməsini çətinləşdirən təsvirlər kimi kiçik bir dəyişiklik edir;

- Çox sayda şifrələmə alqoritmləri və açarlardan istifadə edərkən fərqli şifrələmə alqoritmi ilə şifrələndirilən və hər bir yeni infeksiyaya əsaslanan polimorfik proqramlar (proqramın bu obyektin xüsusi növü haqqında məlumat olmadan eyni interfeysə malik obyektlərdən eyni şəkildə istifadə etmək qabiliyyətidir.) belə ki, onların aşkarlanması çox çətindir və xeyli vaxt sərf edilir;
- Özünü tamamilə dəyişə bilən metamorfik (dəyişikliyə uğramış) proqramları özünü orijinalla heç bir əlaqəsi olmayan yeni bir vəziyyətə çevirir və bu da onları aşkarlamaq üçün ən çətin haldır.

ZPS-nin aşkarlama sistemləri, qorunan kompüter sisteminin adətən ilk kibermüdafiəsidir. Bu sistemlərə aid metodların əksəriyyəti aşağıdakı üç sinifə bölünə bilər.

1. İmza metodları ZPS-ni aşkar etmək üçün geniş istifadə olunur. Çox təsirli olmasına baxmayaraq, əgər, kodda çox kiçik dəyişiklik olarsa, bu da öz növbəsində imzanı dəyişir və təsirli olmur. Əlavə olaraq, bu metod yeni ZPS aşkar etmək üçün imza bazasının müntəzəm olaraq yenilənməsini tələb edir [14];
2. Davranış metodları proqramın zərərli olub, olmadığını müəyyən etmək üçün onun davranışının davamlı müşahidəsini təmin edir. Eksperimentlər göstərir ki, bu metodlar yüksək səviyyədə yalan pozitivlərə malikdir
3. Evristik (məsələ həllinə, öyrənməyə, yaxud kəşf etməyə hər hansı elə yanaşmadır ki, o, optimal, mükəmməl, məntiqli, yaxud rasional olduğuna zəmanət verilməyən, ancaq bilavasitə məqsədə çatmaq üçün kifayət edən praktik metoddan istifadə edir) metod proqramların davranışını müəyyən etmək üçün əsasən maşın təlimindən və verilənlərin intellektual analizindən istifadə edir [15].

IV. BAYES METODUNUN TƏTBİQİ İLƏ ALQORİTMİN İŞLƏNİLMƏSİ

Kibertəhlükəsizlik, bir sıra texnologiyaları, prosesləri, kompüter avadanlıqlarını, məlumatları, proqramları, xidmətləri, şəbəkələri istəmədən və ya icazəsiz girişdən, dəyişikliklərdən və məhv edilmədən, o cümlədən planlaşdırılmamış hadisələrdən və təbii fəlakətlərdən qorumaq metodlarını əhatə edir.

Kiber məkandakı aktivlər, şəxsiyyət, təşkilat və ya dövlət üçün dəyərli olan mənbələr maddi və qeyri-maddi ola bilər. Maddi aktivlərə müəssisə, binalar, avadanlıq, avtomobillər, xammalın əmlakı və s.daxildir. Qeyri-maddi aktivlər xidmətlərə və ya xidmətlərin verilməsinə, patentlərə və ya vacib məlumatlara sahib olmağa, ixtisarlar, təcrübələrin, işçilərin nüfuzuna sahibdir. Kibertəhlükəsizlik məsələlərində bir neçə problemi həll etmək lazımdır:.

- Obyektlərin mühafizəsini müəyyən etmək lazımdır;
- Təhlükələrin mənbəyini müəyyəetmək lazımdır;
- Əks təhdidlər üçün tədbirlər görmək lazımdır;
- Bütün aktivlərin həssaslığını izləmək lazımdır;
- Hərbi və dövlət orqanlarının kiber sistemlərinə bənzər sistemləri aşkarlamaq lazımdır və s.

Süni immun sistemlərinin PS üçün oynadığı rol barədə məlumat verdik. Bayes metodundan istifadə edərək immun sistemlərinin PS üçün nə dərəcədə qoruyucu olmasını müəyyən etmək olar. Bayes metodu haqqında məlumat verək.

Bayes teoremi (və ya Bayesa düsturu) — elementar ehtimal nəzəriyyəsinin əsas teoremlərindən biridir, hansı ki, müəyyən şərt daxilində hər hansı bir hadisənin ehtimalını dəqiq hesablamağa icazə verir. Bayes metodunun tətbiqi onunla nəticələnir ki, onun praktikada tətbiq edilməsi üçün böyük sayda hesablamalar tələb olunmur.

Buna görə Bayes qiymətləndirilmələri yalnız kompüter və şəbəkə texnologiyalarında baş verən yeniliklərdən sonra fəal istifadə edilməyə başlandı [16, 17].

Bayes düsturu aşağıda göstərilmişdir:

$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B)}$$

Burada

P(A) – A hadisəsinin olma ehtimalı;

P(A | B) – B hadisəsi baş verdikdə A hadisəsinin olma ehtimalı;

P(B | A) – A hadisəsi baş verdikdə B hadisəsinin olma ehtimalı;

P(B) – B hadisəsinin olma ehtimalı.

PS arasında virusun yayılma tezliyi 0,001, və immun sisteminin PS-ni qoruması metodu 0,9 ehtimalla virusu aşkara çıxarır. Bu halda müsbət nəticənin 0,01 səhv olma ehtimalı vardır. Burada proqramın immun sistem tərəfindən qorunması ehtimalını tapmaq lazımdır, yəni virusun yalan olduğunu sübut etmək lazımdır. Yoxlama zamanı virusun olduğu fərz edilən PS-nin təmiz olma ehtimalını tapmaq lazımdır.

İ – PS virusludur;

“İ” – yoxlama göstərdi ki, PS virusludur;

H – PS-nin təmiz olduğunu göstərir.

Onda verilən şərt belə yazılır:

P(«İ» | İ) = 0,8;

P(«İ» | H)= 0,02;

P(İ) = 0,002;

P(H) = 0,888.

Ehtimal edilir ki, PS təmizdir, əgər o viruslu hesab edilirdisə, onda o şərti ehtimala bərabərdir:

P(H | «İ»).

Onu tapmaq üçün, virusun tam olma ehtimalını hesablayaq:

P(«İ») = 0,888 × 0,02 + 0,002 × 0,8 = 0,01936.

Ehtimal edilir ki, PS təmizdir, nəticə etibarilə "viruslu" olduğu halda:

P(H | «İ») = 0,999 × 0,01 / (0,999 × 0,01 + 0,001 × 0,9) ≈ 0,917.

P(H | «İ») = 0,888 × 0,02 / (0,888 × 0,02 + 0,002 × 0,8) ≈ 0,917.

Beləliklə, 91,7%, PS-də, müayinə vaxtı “virusli” hesab edilən PS əslində təmizdir.

Əgər müayinənin nəticələrini təsadüfi səhv hesab etmək olarsa, onda həminki PS-nin təkrar müayinəsi birinci nəticədən asılı olmayaraq müstəqil olacaq. Bu halda nəticələrin yalan müsbət payının azaldılması üçün PS-nin təkrar müayinəsini keçirmək əhəmiyyət daşıyır, əgər “viruslu”

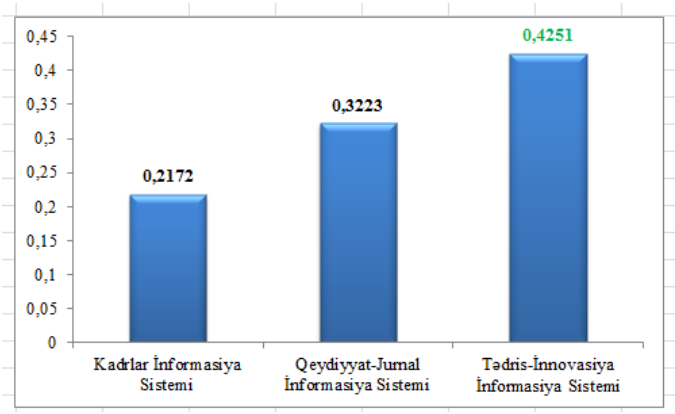
nəticəni almışlarsa. Ehtimal edilir ki, PS təkrar nəticənin "virusli" alınmasından sonra təmizdir, həmçinin Bayes düsturuna görə belə hesablamaq olar:

P(İ | «H», «H») = 0,888 × 0,02 × 0,02 / (0,888 × 0,02 × 0,02 + 0,002 × 0,8 × 0,8) ≈ 0,2172.

Eksperiment aparmaq üçün üç PS-dən istifadə edilmişdir. Göstərilən qayda hər bir PS üçün tətbiq edilmiş və nəticələr alınmışdır (cədvəl II) [18]. Nəticənin qrafik təsviri şəkil 4-də verilmişdir.

CƏDVƏL II. PS-LƏRİN BAYES DÜSTURUNA GÖRƏ TƏMİZ OLMA EHTİMALI

PS-lər	Bayes düsturuna görə alınan qiymətlər
Kadrlar İnformasiya Sistemi	0,2172
Qeydiyyat-Jurnal İnformasiya Sistemi	0,3223
Tədris-İnnovasiya İnformasiya Sistemi	**0,4251**



Şəkil 4. Bayes düsturuna görə eksperiment apar;lan proqram sisteminin təmiz olma ehtimalı.

V. NƏTİCƏ

Məqalədən göründüyü kimi SİS-in bütün elm sahələrində rolu böyük əhəmiyyətə malikdir. SİS-in müxtəlif alqoritmləri vardır və bunlardan müxtəlif məsələlərin həllində istifadə olunur. Proqramlaşdırmada SİS-dən istifadə edilməsi xüsusi əhəmiyyət kəsb edir. SİS-dən zərərli proqram sistemlərinin (viruslar, qurdlar, troyanlar, casus proqramları və s.) təmizlənməsində istifadə edilir. Bu məqalədə də SİS əsasında tibbi təyinatlı proqram sisteminin kibertəhlekəsizliyini təmin etmək üçün Bayes metodunun tətbiqi ilə yeni alqoritm işlənilmiş və eksperiment aparılmışdır. SİS-in özünün üstünlükləri və çatışmayan cəhətləri vardır. Çatışmayan cəhətləri aradan qaldırmaq üçün mükəmməl SİS-lər işlənilməlidir ki, bu da proqram sisteminin effektli və keyfiyyətli işləməsinə səbəb olsun. Təklif olunan metod istənilən optimallaşdırıcıdan (optimallaşdırıcı qurğular, həmçinin kibertəhlükəsizliyi təmin edən sistemlər) istifadə edərək optimallaşdırıla bilər.

İSTİNADLAR

[1] С. В. Гаврилюк, Б. Н. Оныкий и А. А. Станкевичус, “Применение искусственных иммунных систем для защиты сред распределенных вычислений от вредоносного программного обеспечения”. Информационные технологии, том.17, № 3, стр. 32-34, 2015.

[2] De Castro Leandro and Jon Timmis, “A Artificial immune systems: a new computational intelligence approach”, Book, Springer, Berlin, p. 398, 2002.

[3] J. Kephart, “A biologically inspired immune system for computers”, In: Fourth Int. Workshop on the Synthesis and Simulation of Living Systems. MA: MIT Press, Cambridge, p. 130, 1994.

[4] D. Dasgupta, “Artificial Immune Systems”, Artificial Immune System and Their Applications. Springer, Berlin, pp. 355-379, 2010. http:// doi.org/10.1007/978-1-4614-6940-7_7

[5] R. Ligeiro, “Monitoring applications: An immune inspired algorithm for software-fault detection”, Applied soft computing, vol. 24, no. 1095, 2014. http://dx.doi.org/10.1016/j.asoc.2014.08.021

[6] J. Sniecinski Seghatchian, Artificial intelligence: A joint narrative on potential use in pediatric stem and immune cell therapies and regenerative medicine. Trans and Aphaeresis Science, vol. 57 no. 3, p. 422, 2018. https://doi.org/10.1016/j.transci.2018.05.004

[7] S. Louati, S. Darmoul, S. Elkosantini, L. Ben Said, “An artificial immune network to control interrupted flow at a signalized intersection an arti”. Information Sciences, vol.433, no. 70, 2018. https://doi.org/10.1016/j.ins.2017.12.033

[8] H. Rathore, M. Guizani, A. Mohamed, “Mathematical Evaluation of Human Immune Systems For Securing Software Defined NetworksWireless Net.and Mob. Comm”. In: 6TH In. Conf. (IEEE, Morocco), p. 187, 2018.. https://doi.org/10.1109/WINCOM.2018.8629728

[9] Bo Yang, “Mathematical Evaluation of Human Immune Systems For Securing Software Defined Networks Safety Science”. In: 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), vol.118, no. 205, 2019. https://doi.org/10.1109/WINCOM.2018.8629728

[10] L. Fanelli Robert, “A hybrid model for immune inspired network intrusion detection artificial immune syst”. In: International conference on artificial immune systems, Springer-Verlag, Berlin Heidelberg, p. 107-118, 2008.https://doi.org/10.1007/978-3-540-85072-4_10

[11] В.Л. Токарев, А.А. Сычугов, “Обнаружение вредоносного программного обеспечения с использованием иммунных детекторов”. Вопросы защиты информации, стр. 1-15, 2017. https://cyberleninka.ru/article/n/obnaruzhenie-vredonosnogo-programmnogo-obespecheniya-s-ispolzovaniem-immunnyh-detektorov/viewer

[12] К.Н. Евдокимов, “К вопросу о совершенствовании угловой ответственности за создание, использование и распространение вредоносных программ для ЭВМ”. Право и законодательство, стр. 1-4, 2012. https://cyberleninka.ru/article/n/k-voprosu-o-sovershenstvovanii-ugolovnoy-otvetstvennosti-za-sozdanie-ispolzovanie-i-rasprostranenie-vredonosnyh-programm-dlya-evm-st-273/viewer

[13] A. Venkatesan, “Code obfuscation and virus detection master's projects”, p. 116, 2008, San Jose State University. https://doi.org/10.31979/etd.ez5v-x8jc

[14] А.А.Бирюков, “Информационная безопасность: защита и нападение”.DMK Press, Москва, стр. 516,2012 .https://dmkpress.com/catalog/computer/securuty/978-5-94074-647-8/?srsltid=AfmBOooQ90B-ggvl8yDmyXWCVfC6cXVVuJGIJdsUJyF1-SCLBHadPlYG

[15] К. Крис, “Компьютерные вирусы изнутри и снаружи” СбП, Питер, с. 527, 2011. https://www.litres.ru/book/kris-kasperski/komputernye-virusy-iznutri-i-snaruzhi-585385/

[16] В. Е. Гмурман, “Теория вероятностей и математическая статистика”, Высшее образование, с. 480, 2005. Москва. http://univer.nuczu.edu.ua/tmp_metod/142/Gmurman.pdf

[17] D. Stephen, “Judgment under Uncertainty: Heuristics and Biases”, Business Information Review, vol. 32, no. 2, pp. 93-99, 2015. https://doi.org/10.1177/0266382115592536

[18] R.M. Alguliyev, T.H. Kazimov, Sh.J. Mahmudova, R.S. Mahmudova, “Corporate Information System Educational Center” in Proc. Educational Technology: The Inter. Conf., ICTE', Budapest, Hungary, vol. 1, no. 8, pp. 1-8, 2005. https://www.researchgate.net/publication/273696130_Corporate_Information_System_Educational_Center