Süni İmmun Sistemlərinin Kibertəhlükəsizlik Problemlərinin Həllində Tətbiqi İmkanları və Perspektivləri

Ramiz Şıxəliyev
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shikhramiz61@gmail.com

***Xülasə*— Rəqəmsal transformasiya və şəbəkə texnologiyalarının intensiv inkişafı müasir informasiya sistemlərində kibertəhlükələrin həm mürəkkəbliyini, həm də miqyasını əhəmiyyətli dərəcədə artırmışdır. Xüsusilə dinamik və sürətlə dəyişən hücum vektorları fonunda ənənəvi, imza əsaslı kibertəhlükəsizlik mexanizmləri yeni və naməlum təhdidlərin vaxtında aşkarlanmasında yetərli effektivlik nümayiş etdirmir. Bu kontekstdə məqalədə bioloji immun sisteminin prinsiplərinə əsaslanan süni immun sistemlərinin kibertəhlükəsizlik sahəsində tətbiqi imkanları araşdırılır. Süni immun sistemlərinin əsas alqoritmik mexanizmləri, tətbiq sahələri, üstünlükləri, məhdudiyyətləri və aktual elmi-nəzəri problemləri təhlil edilir, həmçinin perspektiv inkişaf istiqamətləri müəyyənləşdirilir.**

Açar sözlər*— *süni immun sistemləri; kibertəhlükəsizlik; anomaliyaların aşkarlanması; neqativ seçim alqoritmi; klonal seçim alqoritmi; hibrid modellər.

I. GİRİŞ

Son illərdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı rəqəmsal transformasiya proseslərinin genişlənməsinə və cəmiyyətin müxtəlif sahələrində rəqəmsal həllərin tətbiqinin intensivləşməsinə səbəb olmuşdur. Sənaye, maliyyə, səhiyyə, nəqliyyat və dövlət idarəçiliyi kimi sahələrdə rəqəmsal platformaların geniş yayılması informasiya sistemlərinin funksional imkanlarını artırmaqla yanaşı, onları kibertəhlükələr qarşısında daha həssas vəziyyətə gətirmişdir. Bunun nəticəsində kibercinayətkarlığın miqyası genişlənmiş, hücumların texniki mürəkkəbliyi və adaptivliyi isə əhəmiyyətli dərəcədə artmışdır. Müasir kibermühitdə müşahidə olunan hücumlar çoxvektorlu, dinamik və kontekstdən asılı xarakter daşıyır, eyni zamanda sistemlərin müxtəlif zəifliklərindən istifadə etməyə yönəlir. İnkişaf etmiş davamlı təhdidlər (APT – Advanced Persistent Threat), sıfır-gün zəifliklərindən istifadə edən hücumlar və süni intellekt (Sİ) texnologiyalarına əsaslanan zərərli proqram təminatları bu cür kibertəhlükələrə aid edilə bilər.

Mövcud kibermüdafiə vasitələri, o cümlədən şəbəkələrarası ekran sistemləri, müdaxilələrin aşkarlanması və qarşısının alınması sistemləri (IDS/IPS - Intrusion Detection System/ Intrusion Prevention System), eləcə də antivirus proqramları əsasən əvvəlcədən müəyyən edilmiş siqnatura və qaydalara əsaslanan yanaşmalar üzərində qurulmuşdur. Bu sistemlər məlum hücum nümunələrinin aşkarlanmasında müəyyən effektivlik nümayiş etdirsə də, yeni və modifikasiya olunmuş kibertəhdidlərin aşkarlanmasında məhdud imkanlara malikdir. Bundan əlavə, bu sistemlərin statik təbiəti onların dəyişən kibermühitə operativ uyğunlaşmanı və real zaman rejimində çevik müdafiə mexanizmlərinin formalaşdırılmasını çətinləşdirir. Buna görə də müasir kibertəhlükəsizlik problemlərinin həlli üçün adaptiv, özüöyrənən və dinamik qərarvermə qabiliyyətinə malik yanaşmaların tətbiqi zəruri hesab olunur. Bu baxımdan, bioloji immun sisteminin mexanizmlərinə əsaslanan yanaşmalar, xüsusilə süni immun sistemləri (SİS), perspektivli istiqamətlərdən biri kimi diqqəti cəlb edir.

Bioloji immun sistemi canlı orqanizmi müxtəlif patogenlərdən qoruyan mürəkkəb, paylanmış və yüksək adaptiv müdafiə mexanizmi kimi fəaliyyət göstərir. Bu sistem "özününkü" və "yad" elementlərin fərqləndirilməsi, antigenlərin tanınması, immun yaddaşın formalaşdırılması və qeyri-müəyyən şəraitdə effektiv qərarların qəbul edilməsi kimi xüsusiyyətləri ilə seçilir. Adaptivlik, nümunələrin tanınması, paylanmış aşkarlama, küylü məlumatlara davamlılıq və dayanıqlılıq kimi xüsusiyyətlər kibertəhlükəsizlik sahəsində daha səmərəli müdafiə mexanizmlərinin qurulması üçün mühüm nəzəri əsas yaradır [1].

SİS bioloji immun mexanizmlərinin riyazi və alqoritmik modelləşdirilməsinə əsaslanan yanaşmadır. Bu yanaşma anomaliyaların aşkarlanması, nümunələrin tanınması, adaptiv qərar qəbuletmə, özü öyrənmə və dəyişən mühitə uyğunlaşma kimi funksiyaların həyata keçirilməsinə imkan verir. SİS əsaslı metodların müdaxilələrin aşkarlanması sistemlərində, zərərli fəaliyyətlərin müəyyənləşdirilməsində və risklərin qiymətləndirilməsində tətbiqi onların kibertəhlükəsizlik sahəsində yüksək potensiala malik olduğunu göstərir.

Məqalənin məqsədi SİS-nin kibertəhlükəsizlik sahəsində tətbiq imkanlarının, üstün cəhətlərinin və mövcud məhdudiyyətlərinin sistemli şəkildə təhlil edilməsi, həmçinin bu texnologiyanın gələcək inkişaf perspektivlərinin müəyyənləşdirilməsidir.

II. SÜNİ İMMUN SİSTEMLƏRİNİN ƏSAS ALQORİTMLƏRİ

SİS çərçivəsində bir neçə fundamental alqoritm formalaşmışdır ki, bunlara neqativ seçim, klonal seçim, immun şəbəkə və təhlükə nəzəriyyəsinə əsaslanan yanaşmalar daxildir. Neqativ seçim alqoritmi bioloji immun sistemində T-limfositlərin timusda yetişməsi prosesi zamanı baş verən

DOI: 10.25045/forensic.gov.2026.05

seleksiya mexanizminə əsaslanır. Bu prosesdə orqanizmin "öz" hüceyrələrinə qarşı reaksiya verən T-hüceyrələr məhv edilir, yalnız özünə qarşı tolerant olan hüceyrələr fəaliyyət qabiliyyətini saxlayır [2]. Süni immun sistemlərində (SİS) bu prinsip formal şəkildə modelləşdirilərək normal davranışın təsviri yaradılır və bu modeldən kənara çıxan nümunələr anomaliya kimi identifikasiya olunur.

Neqativ seçim alqoritmi xüsusilə anomaliya əsaslı müdaxilələrin aşkarlanması sistemlərində geniş tətbiq edilir. Bu yanaşmanın əsas üstünlüyü əvvəlcədən məlum olmayan hücumların aşkarlanması potensialıdır. Bununla belə, böyük verilənlərdə "özününkü"-nün dəqiq müəyyən edilməsi və yanlış pozitivlərin idarə olunması kimi problemlər alqoritmin praktiki tətbiqində əsas çətinliklərdən hesab olunur.

Klonal seçim alqoritmi immun sistemində antigenlərə qarşı yüksək yaxınlığa malik B-limfositlərin seçilərək sürətlə çoxaldılması və mutasiyaya uğraması prinsipinə əsaslanır [3]. Bu proses nəticəsində immun sistemi zaman keçdikcə daha spesifik və effektiv anticisimlər formalaşdırır, yəni öyrənmə və adaptasiya baş verir.

SİS-də klonal seçim mexanizmi optimallaşdırma və təsnifat problemlərinin həllində geniş istifadə olunur. Alqoritm yüksək uyğunluğa malik həllərin seçilməsi, onların klonlaşdırılması və mutasiya yolu ilə daha yaxşı həllərin axtarılması prinsipi üzərində qurulur. Bu xüsusiyyətlər onu xüsusilə mürəkkəb axtarış məkanlarında qlobal optimallaşdırma problemləri üçün effektiv edir. Eyni zamanda, klonal seçim mexanizmi sistemin adaptivliyini artıraraq dəyişən mühitlərdə məhsuldarlığının təmin edilməsinə imkan verir.

İmmun şəbəkə alqoritmi 1974-cü ildə Niels Jerne tərəfindən irəli sürülmüş immun şəbəkə nəzəriyyəsinə əsaslanır [4]. Bu nəzəriyyəyə görə, immun sistemi yalnız antigen-anticisim qarşılıqlı təsirindən ibarət deyil, eyni zamanda anticisimlər bir-biri ilə qarşılıqlı əlaqədə olaraq mürəkkəb, dinamik və özünü tənzimləyən şəbəkə strukturu yaradır.

SİS kontekstində bu alqoritm anticisimlər (detektorlar) arasında stimullaşdırma və fəaliyyətin məhdudlaşdırılması mexanizmlərini modelləşdirir. Nəticədə sistem daxilində müxtəlifliyin qorunması təmin olunur və həddindən artıq uyğunlaşmanın qarşısı alınır. İmmun şəbəkə yanaşması xüsusilə klasterləşdirmə, məlumatların analizi və adaptiv yaddaş mexanizmlərinin yaradılmasında effektiv hesab olunur.

Təhlükə nəzəriyyəsi 1994-cü ildə Polly Matzinger tərəfindən təklif edilmiş və klassik "özününkü" və "yad" fərqləndirməsinə alternativ konsepsiya kimi formalaşdırılmışdır [5]. Bu nəzəriyyəyə əsasən, immun cavabı yalnız "yad" obyektlərə qarşı deyil, hüceyrə və toxumaların zədələnməsi nəticəsində yaranan "təhlükə siqnalları"na cavab olaraq aktivləşir.

Süni immun sistemlərində bu yanaşma daha kontekst-əsaslı qərar qəbuletmə mexanizmlərinin formalaşdırılmasına imkan verir. Xüsusilə, kibertəhlükəsizlik sahəsində təhlükə nəzəriyyəsi yalnız anomal davranışın deyil, həm də onun yaratdığı potensial risk və təsirin qiymətləndirilməsinə imkan verir. Bu isə yanlış pozitivlərin azaldılması, prioritetləşdirmə və adaptiv müdafiə strategiyalarının qurulması baxımından mühüm üstünlüklər təmin edir.

III. KİBERTƏHLÜKƏSİZLİKDƏ TƏTBİQ SAHƏLƏRİ

SİS-lər özünün adaptivliyi, paylanmış strukturu və qeyri-müəyyən mühitlərdə effektiv işləmə qabiliyyəti sayəsində kibertəhlükəsizlik sahəsində geniş tətbiq imkanlarına malikdir. Müxtəlif tədqiqatlar göstərir ki, immun əsaslı yanaşmalar həm ənənəvi metodları tamamlayır, həm də yeni nəsil hücumların aşkarlanması və qarşısının alınmasında yüksək effektivlik nümayiş etdirir.

SİS-in ən geniş tətbiq sahələrindən biri müdaxilələrin aşkarlanması sistemləridir. Bu sistemlərdə bioloji immun sisteminin "özününkü/yad" fərqləndirmə prinsipi və paylanmış aşkarlama mexanizmləri formal şəkildə modelləşdirilir. Harmer və başqaları [6] tərəfindən təklif olunmuş yanaşma immun sisteminin iyerarxik arxitekturasına əsaslanan paylanmış agent əsaslı müdafiə modelinə əsaslanır. Bu modeldə müxtəlif səviyyələrdə fəaliyyət göstərən agentlər lokal qərarlar qəbul edərək ümumi təhlükəsizlik vəziyyətini qiymətləndirir. Eksperimental nəticələr göstərir ki, bu yanaşma virusların aşkarlanması və sistemə müdaxilələrin müəyyən edilməsi baxımından yüksək effektivlik nümayiş etdirir. Boukerche və başqaları [7] isə antigen-anticisim uyğunluğu və immun yaddaş prinsiplərinə əsaslanan IDS modeli təqdim etmişdir. Bu modeldə əvvəlki hücum nümunələri yadda saxlanılır və gələcəkdə oxşar fəaliyyətlərin daha sürətli aşkarlanması təmin edilir. Bundan əlavə, sistem loq fayllarının həcmini optimallaşdıraraq yalnız əhəmiyyətli hadisələrin saxlanmasını təmin edir və real-vaxt rejimində anomaliyaların monitorinqinə imkan yaradır. Bu xüsusiyyətlər böyük həcmli verilənlərin emalı baxımından xüsusi əhəmiyyət kəsb edir.

Anomaliyaların aşkarlanması SİS-in əsas tətbiq sahələrindən biri olmaqla, sistemin normal davranış modelindən kənara çıxmaları müəyyən etməyə yönəlmişdir. Bu yanaşma xüsusilə sıfır-gün hücumlarının aşkarlanmasında mühüm rol oynayır. Dandıl [8] tərəfindən təklif edilmiş C-NSA (Clonal–Negative Selection Algorithm) hibrid modeli neqativ seçim və klonal seçim alqoritmlərinin üstünlüklərini birləşdirir. Bu modeldə əvvəlcə normal davranış sahəsi müəyyən edilir, daha sonra isə klonal seçim vasitəsilə detektorların uyğunluğu artırılır. Aparılmış təcrübələr nəticəsində 94.30% orta aşkarlama dəqiqliyi və aşağı səviyyədə yalan pozitiv göstəricilər əldə edilmişdir. Bu isə modelin praktik tətbiq üçün yararlı olduğunu göstərir.

Elektron poçt və mesajlaşma sistemlərində spamların aşkarlanması da SİS-in tətbiq olunduğu mühüm istiqamətlərdən biridir. Haggag və Fattoh [9] tərəfindən təklif edilmiş model neqativ seçim alqoritmini antigen-anticisim yaxınlıq ölçüsü ilə birləşdirərək effektiv spam filtrasiya mexanizmi formalaşdırır. Bu yanaşmada spam mesajlar "yad" kimi modelləşdirilir və uyğun detektorlar vasitəsilə aşkarlanır. Təklif olunan model yüksək aşkarlama dəqiqliyi və aşağı yalançı pozitiv göstəriciləri ilə seçilir ki, bu da istifadəçi təcrübəsinin yaxşılaşdırılması baxımından mühüm əhəmiyyət daşıyır.

Əşyaların İnterneti (IoT) mühitində resurs məhdudiyyətləri, qeyri-bircinslik və yüksək paylanma səbəbindən təhlükəsizlik məsələləri daha mürəkkəb xarakter daşıyır. Bu səbəbdən adaptiv və yüngül hesablama modellərinə ehtiyac yaranır. Rosset və başqaları [10] tərəfindən təklif edilmiş Fed-Active modeli federativ təlim və aktiv təlim yanaşmalarını birləşdirərək IoT

mühitində müdaxilələrin aşkarlanmasını həyata keçirir. Bu model mərkəzləşdirilməmiş şəkildə öyrənərək məlumatların məxfiliyini qoruyur və eyni zamanda yüksək aşkarlama dəqiqliyi təmin edir. Tədqiqat nəticələri göstərir ki, təklif olunan yanaşma ənənəvi mərkəzləşdirilmiş modellərlə müqayisədə oxşar məhsuldarlıq nümayiş etdirir, lakin daha az təlim vaxtı tələb edir ki, bu da real zaman tətbiqləri üçün mühüm üstünlükdür.

Son illərdə SİS-in digər Sİ metodları ilə inteqrasiyası geniş yayılmışdır. Bu cür hibrid yanaşmalar müxtəlif metodların üstünlüklərini birləşdirərək daha yüksək məhsuldarlıq əldə etməyə imkan verir. Nguyen və başqaları [11] tərəfindən təklif edilmiş modeldə süni immun sistemi və DBN (Deep Belief Networks) şəbəkələri inteqrasiya edilərək virusların aşkarlanması üçün istifadə edilir. Bu yanaşmada SİS ilkin filtrasiya və xüsusiyyət seçimi funksiyasını yerinə yetirir, DBN isə mürəkkəb nümunələrin öyrənilməsi və təsnifatı üçün istifadə olunur. Nəticədə 98.8% orta aşkarlama dəqiqliyi əldə edilmişdir ki, bu da hibrid modellərin yüksək potensialını nümayiş etdirir.

Beləliklə, süni immun sistemlərinin müxtəlif kibertəhlükəsizlik sahələrində tətbiqi onların çevikliyi, adaptivliyi və yüksək aşkarlama qabiliyyəti sayəsində perspektivli yanaşma olduğunu göstərir. Bu sistemlərin xüsusilə hibrid modellərlə inteqrasiyası gələcək tədqiqatlar üçün mühüm istiqamətlərdən biri hesab olunur.

IV. MÜQAYİSƏLİ ANALİZ

Müasir kibertəhlükəsizlik mühitində müxtəlif yanaşmaların, o cümlədən, SİS, Sİ (xüsusilə dərin təlim (DT) metodları) və ənənəvi təhlükəsizlik mexanizmlərinin üstünlükləri və məhdudiyyətlərinin müqayisəli şəkildə təhlili onların tətbiq sahələrinin daha dəqiq müəyyənləşdirilməsi baxımından mühüm əhəmiyyət kəsb edir. Hər bir yanaşma fərqli nəzəri əsaslara, hesablama modellərinə və praktik tətbiq xüsusiyyətlərinə malik olduğundan, onların effektivliyi konkret istifadə ssenarilərindən asılı olaraq dəyişir (Cədvəl 1).

CƏDVƏL I. SİS, Sİ VƏ ƏNƏNƏVİ MEXANİZMLƏRİN MÜQAYİSƏSİ

Xüsusiyyətlər	**SİS**	**SI (Dərin Təlim)**	**Ənənəvi mexanizmlər**
Adaptivlik	Yüksək	Çox yüksək	Çox aşağı
Naməlum hücumlara davamlılıq	Yüksək	Orta	Qaydalara əsaslanan
Öyrənmə növü	Təkamül	Statistik	Öyrənmə qabiliyyəti yoxdur
Hesablama mürəkkəbliyi	Orta	Yüksək	Aşağı

Cədvəl 1-də göstərildiyi kimi, adaptivlik baxımından SİS və Sİ yanaşmaları ənənəvi metodları əhəmiyyətli dərəcədə üstələyir. SİS bioloji immun sistemindən qaynaqlanan təkamül və özünü tənzimləmə mexanizmləri sayəsində dəyişən mühitə uyğunlaşa bilir. DT modelləri isə böyük həcmli verilənlər üzərində öyrənərək mürəkkəb nümunələri aşkar etmək qabiliyyətinə malikdir və buna görə "çox yüksək" adaptivlik səviyyəsi ilə xarakterizə olunur. Ənənəvi mexanizmlər (məsələn, qayda və siqnatura əsaslı sistemlər) isə statik struktura malik olduqlarından adaptivlik baxımından məhduddur.

Naməlum hücumlara qarşı davamlılıq xüsusiyyəti müasir kibertəhlükəsizlik sistemləri üçün kritik göstəricilərdən biridir. SİS bu baxımdan yüksək məhsuldarlıq nümayiş etdirir, çünki o, "özününkü" davranış modelindən kənara çıxmaları aşkarlayaraq əvvəllər məlum olmayan hücumları müəyyən edə bilir. DT modelləri də müəyyən hallarda anomaliyaları aşkar edə bilsə də, onların effektivliyi təlim verilənlərinin keyfiyyəti və müxtəlifliyindən asılıdır. Bu səbəbdən bu göstərici "orta" səviyyədə qiymətləndirilir. Ənənəvi mexanizmlər isə yalnız məlum siqnaturalara əsaslandığından naməlum hücumlara qarşı demək olar ki, qeyri-effektivdir.

Təlim növü baxımından bu yanaşmalar arasında əsaslı fərqlər mövcuddur. SİS təkamül və immun mexanizmlərə əsaslanan adaptiv təlim prinsiplərini tətbiq edir (məsələn, klonal seçim, neqativ seçim). Sİ, xüsusilə DT modelləri statistik və optimallaşdırma əsaslı təlim mexanizmlərindən istifadə edir. Ənənəvi sistemlər isə əsasən əvvəlcədən müəyyən edilmiş qaydalar və ekspert biliklərinə əsaslanır ki, bu da onların çevikliyini məhdudlaşdırır.

Hesablama mürəkkəbliyi də mühüm müqayisə meyarlarından biridir. SİS alqoritmləri adətən orta səviyyəli hesablama resursları tələb edir və paralel işləmə qabiliyyətinə malikdir. DT modelləri isə böyük verilənlər və çoxsaylı parametrlər səbəbindən yüksək hesablama gücü və xüsusi avadanlıq (məsələn, GPU/TPU) tələb edir. Ənənəvi mexanizmlər isə nisbətən sadə struktura malik olduqlarından aşağı hesablama mürəkkəbliyi ilə seçilir.

İzahlılıq baxımından ənənəvi sistemlərdə qərar qəbuletmə prosesi aydın və şəffafdır, çünki qaydalara əsaslanır. SİS-də izahlılıq orta səviyyədədir; bəzi hallarda detektorların davranışı və qərar mexanizmi izah edilə bilər, lakin tam şəffaflıq təmin olunmur. DT modelləri isə "qara qutu" xarakteri daşıdığından onların qərarlarının izahı çətindir və bu, xüsusilə kritik tətbiqlərdə məhdudiyyət yaradır.

Yuxarıdakı üç yanaşmanın müqayisəsi göstərir ki, universal və bütün hallarda optimal olan vahid həll mövcud deyil. Əksinə, ən effektiv nəticələr çox vaxt bu metodların hibrid şəkildə inteqrasiyası ilə əldə olunur. Xüsusilə SİS-in adaptivliyi ilə Sİ-in yüksək təlim qabiliyyətinin birləşdirilməsi gələcək kibertəhlükəsizlik sistemlərinin inkişafında perspektivli istiqamət kimi qiymətləndirilə bilər.

V. ELMİ-NƏZƏRİ PROBLEMLƏR VƏ GƏLƏCƏK TƏDQİQAT İSTİQAMƏTLƏRİ

SİS-in kibertəhlükəsizlik sahəsində tətbiqi mühüm üstünlüklər təqdim etməklə yanaşı, bir sıra elmi-nəzəri və praktik problemlərlə də müşayiət olunur. Bu problemlərin sistemli şəkildə təhlili və aradan qaldırılması istiqamətində aparılan tədqiqatlar SİS-in daha geniş tətbiqinə və effektivliyinin artırılmasına zəmin yaradır. Eyni zamanda, bu sahədə mövcud boşluqlar gələcək tədqiqat istiqamətlərinin formalaşdırılmasında mühüm rol oynayır. İlk növbədə, parametrlərin optimal seçimi məsələsi SİS modellərinin effektivliyinə birbaşa təsir edən əsas problemlərdən biridir. İmmun sistemlərdə istifadə olunan detektorların sayı, uyğunluq həddləri, mutasiya dərəcəsi və seleksiya mexanizmləri kimi parametrlərin düzgün tənzimlənməsi sistemin effektivliyini müəyyən edir. Lakin dinamik və qeyri-stasionar kibermühitlərdə

bu parametrlərin adaptiv şəkildə optimallaşdırılması üçün vahid formal metodologiyanın olmaması ciddi elmi boşluq kimi qalmaqdadır [12].

Digər mühüm problem yüksək hesablama mürəkkəbliyi ilə bağlıdır. SİS alqoritmləri, xüsusilə populyasiya əsaslı yanaşmalar, çoxsaylı detektorların idarə olunması və onların giriş verilənləri ilə uyğunluğunun hesablanmasını tələb edir. Bu isə böyük həcmli və yüksək sürətli şəbəkə trafikinin analizində hesablama yükünü artırır və sistemin miqyaslanma qabiliyyətini məhdudlaşdırır. Bu baxımdan, paralel hesablama, paylanmış arxitekturalar və optimallaşdırılmış alqoritmlərin işlənməsi aktual tədqiqat mövzularındandır.

SİS əsaslı anomaliya aşkarlama sistemlərində yalan pozitiv nəticələrin yüksək olması da mühüm problemlərdən hesab olunur. Bunun əsas səbəbi normal sistem davranışlarının zamanla dəyişməsi və müxtəlif kontekstlərdə fərqli təzahür etməsidir. Nəticədə, bəzi hallarda qanuni fəaliyyətlər səhvən anomaliya kimi qiymətləndirilə bilər ki, bu da sistemin etibarlılığına mənfi təsir göstərir və əlavə analiz yükü yaradır.

Bundan əlavə, real-vaxt tətbiqləri üçün tələb olunan aşağı gecikmə şərtləri ilə SİS modellərinin hesablama mürəkkəbliyi arasında ziddiyyət mövcuddur. Xüsusilə yüksək sürətli şəbəkələrdə və kritik infrastrukturlarda təhlükələrin dərhal aşkarlanması tələb olunduğu halda, mürəkkəb immun alqoritmlərinin istifadəsi əlavə vaxt tələb edə bilər [13]. Bu isə SİS-in real-vaxt sistemlərində tətbiqini məhdudlaşdıran amillərdən biridir.

Elmi və nəzəri baxımdan digər mühüm problem hücum-müdafiə təkamülünün formal modellərinin kifayət qədər inkişaf etməməsidir. Bioloji immun sistemində olduğu kimi, kibermühitdə də hücum və müdafiə mexanizmləri arasında dinamik qarşılıqlı təsir mövcuddur. Lakin bu qarşılıqlı təsirin riyazi və alqoritmik modelləşdirilməsi hələ də tam formalaşmamışdır. Bu sahədə aparılacaq tədqiqatlar adaptiv və proqnozlaşdırıcı təhlükəsizlik sistemlərinin yaradılmasına töhfə verə bilər.

Yuxarıda qeyd olunan problemlər SİS-in inkişaf istiqamətlərini də müəyyənləşdirir. Gələcək tədqiqatlarda SİS-in digər Sİ metodları ilə, xüsusilə DT yanaşmaları ilə inteqrasiyası mühüm yer tutur. Bu cür hibrid modellər SİS-in adaptiv və təkamül əsaslı xüsusiyyətlərini DT-in yüksək təsnifat qabiliyyəti ilə birləşdirərək daha effektiv təhlükəsizlik həlləri yarada bilər.

Eyni zamanda, kiber-immun arxitekturaların işlənməsi perspektivli istiqamətlərdən biridir. Bu arxitekturalar paylanmış, çoxsəviyyəli və özünü tənzimləyən müdafiə mexanizmlərini əhatə etməklə mürəkkəb şəbəkə mühitlərində daha dayanıqlı təhlükəsizlik təmin edə bilər. Bununla yanaşı, özünü bərpa edən sistemlərin inkişafı da mühüm əhəmiyyət kəsb edir. Belə sistemlər yalnız hücumları aşkar etməklə kifayətlənmir, həm də zədələnmiş komponentləri avtomatik şəkildə bərpa edərək sistemin davamlılığını təmin edir.

Avtonom qərar qəbuletmə mexanizmlərinin inkişafı da SİS-in gələcək tədqiqat istiqamətləri sırasında mühüm yer tutur. Bu yanaşma insan müdaxiləsini minimuma endirərək sistemlərin müstəqil şəkildə təhlükələri qiymətləndirməsinə və müvafiq cavab tədbirləri görməsinə imkan verir. Bununla yanaşı, SİS-in real zaman rejimində adaptasiyası və böyükmiqyaslı şəbəkələrdə (məsələn, bulud infrastrukturları və IoT ekosistemləri) tətbiqi də prioritet istiqamətlər kimi çıxış edir.

SİS-in kibertəhlükəsizlik sahəsində effektiv tətbiqi üçün mövcud elmi-nəzəri problemlərin həlli və qeyd olunan istiqamətlər üzrə tədqiqatların dərinləşdirilməsi zəruridir. Bu yanaşma gələcəkdə daha çevik, adaptiv və intellektual kibermüdafiə sistemlərinin yaradılmasına imkan verəcəkdir.

NƏTİCƏ

Aparılmış təhlillər göstərir ki, SİS-lər müasir kibertəhlükəsizlik çağırışlarına cavab verən perspektivli və innovativ yanaşma kimi çıxış edir. Bioloji immun sistemi mexanizmlərinə əslanan bu modellər adaptivlik, özüöyrənən və paylanmış qərar qəbuletmə xüsusiyyətləri ilə ənənəvi siqnatura əsaslı metodların məhdudiyyətlərini qismən aradan qaldırır. Tədqiqat nəticələri SİS-in müdaxilələrin və anomaliyaların aşkarlanması, həmçinin IoT mühitlərində effektiv tətbiq oluna bildiyini göstərir. Bununla yanaşı, DT metodları ilə inteqrasiya aşkarlama dəqiqliyini artırır. Lakin hesablama mürəkkəbliyi, parametr optimallaşdırılması və real zaman tələbləri kimi problemlər əlavə araşdırmalar tələb edir. Beləliklə, SİS gələcək intellektual kibertəhlükəsizlik sistemlərinin formalaşmasında mühüm rol oynaya bilər.

ƏDƏBİYYAT

[1] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection – a review," Natural Computing, vol. 6, no. 4, pp. 413-466, 2007.

[2] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in Proceedings of the 1994 IEEE Symposium on Security and Privacy, 1994, pp. 202-212.

[3] L. N. de Castro and F. J. Von Zuben, "Learning and optimization using the clonal selection principle," IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 239-251, 2002.

[4] N. K. Jerne, "Towards a network theory of the immune system," Annales d'Immunologie, vol. 125C, no. 1-2, pp. 373-389, 1974.

[5] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger Theory: The Link between AIS and IDS," in Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS), Edinburgh, United Kingdom, 2003, pp. 147–155.

[6] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An Artificial Immune System Architecture for Computer Security Applications," IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 252-280, 2002.

[7] A. Boukerche, K. R. L. Jucá, J. B. Sobral, and M. S. M. A. Notare, "An artificial immune based intrusion detection model for computer and telecommunication systems," Parallel Computing, vol. 30, no. 5-6, pp. 629–646, 2004.

[8] E. Dandıl, "C-NSA: a hybrid approach based on artificial immune algorithms for anomaly detection in web traffic," IET Information Security, vol. 14, no. 6, pp. 683-693, 2020.

[9] M. H. Haggag and I. E. Fattoh, "Artificial immune system for spam filtering," in Conference Proceedings, vol. 9, no. 2, pp. 117-129, 2009.

[10] V. Rosset, M. B. de Almeida, and A. C. P. de L. F. de Carvalho, "A distributed security approach based on artificial immune systems for intrusion detection in Internet of Things," Research Article, 2024.

[11] V. T. Nguyen, L. H. Dung, and T. D. Le, "A combination of artificial immune system and deep learning for virus detection," International Journal of Applied Engineering Research, vol. 13, no. 22, pp. 15622-15628, 2018.

[12] P. Widuliński, "Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies," Applied Cybersecurity & Internet Governance, vol. 2, no. 1, pp. 1-24, 2023.

Application Opportunities and Prospects of Artificial Immune Systems in Solving Cybersecurity Problems

Ramiz Shikhaliyev
Institute of Information Technology, Baku, Azerbaijan
shikhramiz61@gmail.com

Abstract– Digital transformation and intensive development of network technologies have significantly increased both the complexity and scale of cyber threats in modern information systems. Especially against the background of dynamic and rapidly changing attack vectors, traditional, signature-based cybersecurity mechanisms do not demonstrate sufficient effectiveness in the timely detection of new and unknown threats. In this context, the article examines the possibilities of applying artificial immune systems based on the principles of the biological immune system in the field of cybersecurity. The main algorithmic mechanisms, application areas, advantages, limitations and current scientific and theoretical problems of artificial immune systems are analyzed, and prospective development directions are also identified.

Keywords – artificial immune systems; cybersecurity; anomaly detection; negative selection algorithm; clonal selection algorithm; hybrid models.