AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

KİBER-FİZİKİ SİSTEMLƏRİN KİBER DAYANIQLIĞININ TƏMİN EDİLMƏSİ ÜÇÜN METOD VƏ ALQORİTMLƏRİN İŞLƏNMƏSİ

İxtisas: 3338.01 – Sistemli analiz, idarəetmə və informasiyanın işlənməsi (informasiya texnologiyaları)

Elm sahəsi: Texnika elmləri

İddiaçı: **Suxostat Lyudmila Valentinovna**

Elmlər doktoru elmi dərəcəsi
almaq üçün təqdim olunmuş dissertasiyanın

A V T O R E F E R A T I

Bakı – 2025

Dissertasiya işi Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunda yerinə yetirilmişdir.

Elmi məsləhətçi: AMEA-nın həqiqi üzvü,
texnika elmləri doktoru, professor
Rasim Məhəmməd oğlu Əliquliyev

Rəsmi opponentlər: texnika elmləri doktoru, professor
Nailə Fuad qızı Musayeva
texnika elmləri doktoru, professor
Valeh Azad oğlu Mustafayev
texnika elmləri doktoru, dosent
Zərifə Qasım qızı Cəbrayılova
texnika elmləri doktoru, professor
Baləmi Qasım oğlu İsmayılov

Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun nəzdində fəaliyyət göstərən ED 1.35 Dissertasiya Şurası

Dissertasiya şurasının sədri:
AMEA-nın həqiqi üzvü, texnika elmləri doktoru, professor
Rasim Məhəmməd oğlu Əliquliyev

Dissertasiya şurasının elmi katibi:
texnika üzrə fəlsəfə doktoru, dosent
Fərqanə Cabbar qızı Abdullayeva

Elmi seminarın sədri:
texnika elmləri doktoru
Mütəllim Mirzəəhməd oğlu Mütəllimov

İŞİN ÜMUMİ XARAKTERİSTİKASI

Mövzunun aktuallığı və işlənmə dərəcəsi. Müasir informasiya texnologiyaları dövlətin və cəmiyyətin mühüm inkişaf vasitəsidir. Kiber-fiziki sistemlər (KFS) Sənaye 4.0 konsepsiyasının həyata keçirilməsində əsas texnologiya və insan fəaliyyətinin müxtəlif sahələrində geniş istifadə olunan intellektual obyektlərin əsas komponentidir.

KFS sistemlərinin əsasını təşkil edən mühüm texnoloji tendensiyalara aşağıdakılar daxildir: Əşyaların İnterneti (Internet of Things), ağıllı elektrik şəbəkələri, ağıllı istehsal sistemləri, bulud hesablamaları və s. KFS aşağıdakı sahələrin inkişafı üçün əsasdır: ağıllı istehsal, ağıllı tibb, ağıllı binalar və infrastrukturlar, intellektual nəqliyyat sistemləri, mobil sistemlər, müdafiə sistemləri və hava monitorinqi sistemləri [4].

KFS sistemlər iki texnologiyanın birləşməsidir: kiber səviyyədə informasiya texnologiyası (İT) və fiziki səviyyədə əməliyyat texnologiyası (ƏT). Kiber səviyyə serverlərdən, verilənlər bazası sistemlərindən, hostlardan və s. ibarətdir. Fiziki səviyyə istehsal müəssisələrini idarə edən sensorlar, aktuatorlar, əks əlaqə sistemləri və s. ibarətdir.

KFS ƏT və İT platformalarında böyük verilənlərin toplanması və mübadiləsi üçün bir çox cihaz və sistemlərin qoşulmasını tələb edir. Qarşıya qoyulmuş məsələlərə nail olmaq üçün birləşdirilməli olan müxtəlif avtomatlaşdırma protokolları mövcuddur. ISO 22301:2019 standartı isə təşkilatların müxtəlif gözlənilməz pozuntulara dayanıqlığını artırmaq, əməliyyatların və xidmətlərin davamlılığını təmin etmək üçün çox vacibdir.

Onların kibertəhlükəsizliyini təmin etmək üçün aktuallıq son illərdə bir sıra kiberhücumlardan sonra kəskin şəkildə artmışdır.

KFS kiberhücumlar insan sağlamlığı və təhlükəsizliyi üçün əhəmiyyətli risk yaradır və ətraf mühitə ciddi ziyan vurur. 2010-cu ildə Stuxnet kompüter virusu kiberhücumlarından sonra KFS informasiya təhlükəsizliyinə maraq kəskin artıb. Daim dəyişən kibertəhlükələrlə daxili və gizli kiberhücumların aşkarlanmasını tələb

edən, daha kiber dayanıqlı və təhlükəsiz kiberinfrastrukturu təmin edən daha yüksək səviyyəli metodologiya hazırlamaq lazımdır.

12 mart 2024-cü ildə Avropa Parlamenti təklif olunan "Kiber Dayanıqlıq Aktını" təsdiqlədi. O, Avropa bazarında yerləşdirilən rəqəmsal elementləri olan bütün məhsullara şamil ediləcək, istifadəsi məlumatların cihaz və ya şəbəkəyə birbaşa və ya dolayı məntiqi və ya fiziki qoşulmasını nəzərdə tutur.

KFS sistemlərinin fəaliyyətinin pozulması və onun komponentlərinin sıradan çıxması ciddi təhlükələrə səbəb ola bilər ki, bu da KFS sistemlərinin kiber dayanıqlığına prioritetlərdən biri kimi baxılması zərurətini yaradır.

Sənaye 4.0-a keçid bütün dünya kimi, Azərbaycan Respublikasının qarşısında da yeni vəzifələr və çağırışlar qoyub. Azərbaycan Respublikasında Dördüncü Sənaye İnqilabının inkişafı üçün bütün imkanlar vardır. Ölkədə mütərəqqi texnologiyalar daim inkişaf etdirilir. "Azərbaycan Respublikasının 2025–2028-ci illər üçün süni intellekt Strategiyası" təsdiq edilib.

Müasir dövrdə Respublikada bütün Sənaye 4.0 texnologiyaları müxtəlif kritik infrastrukturlarda, məsələn, neft-qaz platformalarında, nəqliyyat sistemlərində və s. istifadə olunur.

Dünya İqtisadi Forumu ilə fəal əməkdaşlıq Azərbaycan Respublikası Prezidentinin 6 yanvar 2021-ci il tarixli fərmanına uyğun olaraq "Dördüncü Sənaye İnqilabının Təhlili və Koordinasiya Mərkəzi"nin yaradılmasına səbəb olmuşdur. Mərkəzin fəaliyyəti süni intellektin və maşın təlimin inkişafının təmin edilməsinə, o cümlədən vətəndaşlara xidmətə, rəqəmsal iqtisadiyyatın inkişafına və ölkədə müxtəlif tədqiqat sahələrinin daha da təkmilləşdirilməsinə yönəlib.

"Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" 17 aprel 2021-ci il tarixli Fərmanı imzalanıb.

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə 27 may 2022-ci il tarixli Qanununa əsasən, "kritik informasiya infrastrukturu" anlayışları, onun obyekti və subyekti, habelə təhlükəsizliyinin təmin edilməsi qaydalarının hüquqi əsasları

əlavə edilir. Azərbaycan Respublikası Nazirlər Kabineti 29 noyabr 2024-cü ildə "Kritik informasiya infrastrukturu obyektlərinin Siyahısı"nı təsdiq edib.

Azərbaycan Respublikası Prezidentinin 16 yanvar 2025-ci il tarixli Fərmanı ilə "Azərbaycan Respublikasında Rəqəmsal İnkişaf Konsepsiyası" təsdiq edilib.

Müasir kiberhücumların aşkarlanması KFS sistemlərinin dayanıqlı fəaliyyəti üçün çox vacibdir. Ənənəvi müdafiə mexanizmləri kiberhücumçuların istifadə etdiyi üsullara görə daha az effektiv olur. Kiberhücum riskləri kiber və fiziki domenlərinin inteqrasiyasından, başqa sözlə, İT və OT domenlərinin inteqrasiyasından yaranır. Bu kontekstdə kiberhücumların aşkarlanması üçün adaptiv, daha effektiv üsulların işlənməsi İT və ƏT infrastrukturlarını bu cür təhlükələrdən qorumaq üçün təcili ehtiyacdır.

Kritik vəziyyətlər kibercinayətkarlar üçün idealdır, çünki onlar ən zəif halqadan – insan faktordan istifadə edə bilirlər. Kibercinayətkarlar icazəsiz giriş əldə etmək, etimadnamələri oğurlamaq və sistemləri zərərli proqramlarla yoluxdurmaq üçün insan faktordan istifadə edirlər.

Bütün məlum kiberhücumlar üçün aşkarlama alqoritmlərinin və əks tədbirlərin işlənməsi vacibdir. Bu, onların təsirini azaldacaq və sistemə zərəri minimuma endirəcəkdir. Araşdırmalar göstərir ki, KFS sistemlərinin kibertəhlükəsizliyinin daha dərin təhlili, xüsusən də süni intellektə əsaslanan yanaşmaların tətbiqi tələb olunur.

Bu məsələ ilə məşğul olan ilk beş tədqiqat universiteti sırasına Berkli Kaliforniya Universiteti (ABŞ), Pekin Elm və Texnologiya Universiteti (Çin), KTH Kral Texnologiya İnstitutu (İsveç), Politecnico di Milano (İtaliya) və Hamburq Texnologiya Universiteti (Almaniya) daxildir.

Sənaye 4.0-da doğru irəlilədikcə, KFS daha mürəkkəb, paylanmış və verilənlərə əsaslanan olur, bu da tədricən müdaxilə və anomaliyaların aşkarlanmasını böyük verilənlər probleminə çevirir. Çətinlik təbiətcə fərqli, minimal hesablama xərcləri ilə böyük həcmli verilənlərin təhlilinə ehtiyacdır.

KFS sistemlərdən məlumat toplamaq üçün sensorlar, aktuatorlar və digər cihazlardan istifadə onların təhlili üçün faydalı məlumat verir. Lakin bu gün saxlanılan verilənlərin həcmi ənənəvi alqoritmlərin işləməsi üçün çox mürəkkəbləşir. Tədqiqatçılar verilənlərin bölünməsi və aprior biliklərin istifadəsi kimi müxtəlif yanaşmalara müraciət etməlidirlər. Beləliklə, böyük verilənlərlə işləmək tədqiqatçıların istifadə etdiyi yeni metodların işlənməsini zəruri edir. Böyük həcmli və böyük ölçülü verilənlərlə işləmək üçün maşın təlimi metodlarının imkanlarından istifadə edən yeni alqoritmlər yaratmaq da lazımdır. Lakin mövcud alqoritmlər yüksək hesablama mürəkkəbliyinə görə həmişə effektiv olmur.

Maşın təlimi üsulları kiberhücumları aşkar edərkən KFS məlumatlarını təhlil etmək üçün geniş istifadə olunur. Nəzəriyyə olaraq, maşın təlimi alqoritmləri yüksək effektivliyinə nail ola bilər, yəni yanlış həyəcan siqnalını minimuma endirir və aşkarlama dəqiqliyini maksimum dərəcədə artırır [10]. Ancaq adətən, sonsuz sayda təlim nümunələri tələb olunur. Praktikada bu şərt məhdud hesablama gücü və real vaxt rejimində cavab tələbi səbəbindən mümkün deyil [10]. Buna görə də kibercinayətkarlar tez-tez ən zəif nöqtəni – KFS sistemlərdə ən həssas funksional komponenti axtarır və hədəfə alırlar. Ən həssas cihazlar təhlükəsizlik zəifliklərinin effektiv tədqiqi üçün yaxşı başlanğıc nöqtəsi ola bilər. Mövcud metodlar kiber-fiziki mühitində ümumi çoxmərhələli kiberhücumları hərtərəfli təhlil edə bilmir [30].

Tədqiq olunan problemlərin həlli mühüm vəzifədir, bununla əlaqədar müxtəlif metod və alqoritmlər işlənmiş və praktikada tətbiq edilmişdir. Onların əksəriyyəti ya yalnız İT mühitində kibertəhlükəsizliyi, ya da ƏT mühitində təhlükəsizliyi nəzərdə tutur. Kiber-fiziki hücumlardan qorunmanın təmin edilməsi ciddi problemdir. Bu, kiber dayanıqlığın qiymətləndirilməsi metodlarının işlənməsini tələb edir. Bu metodlar KFS sistemlərdə kiber və fiziki komponentlər arasında sıx qarşılıqlı əlaqə və asılılıqları öyrənməlidir. Bununla belə, mövcud metodlar bu spesifikliyi nəzərə almır.

Yuxarıda göstərilənləri nəzərə alaraq belə qənaətə gəlmək olar ki, hazırda kiber dayanıqlı və kibertəhlükəsiz KFS sistemlərinin layihələndirilməsinə vahid yanaşma yoxdur. Bu dissertasiya tədqiqatı İT komponentlərinin kibertəhlükəsizliyini və ƏT komponentlərinin dayanıqlılığını təmin etmək üçün metod və alqoritmlərin işlənməsinə yönəlib.

Tədqiqatın obyekti və predmeti. Tədqiqatın obyekti kiberfiziki sistemlərin İT kibertəhlükəsizliyi və ƏT mühafizəsidir. **Tədqiqatın predmeti** kiber-fiziki sistemlərin kiber dayanıqlığını təmin etmək üçün proseslərinin idarə edilməsinin model və metodlarıdır.

Tədqiqatın məqsəd və vəzifələri. Dissertasiya işinin məqsədi kiberhücumların və sistem nasazlıqlarının aşkarlanması ilə böyük verilənlərin intellektual təhlili əsasında kiber-fiziki sistemlərin kiber dayanıqlığın və informasiya təhlükəsizliyinin təmin edilməsi üçün metod və alqoritmlərin işlənməsidir.

Dissertasiya işində qarşıya qoyulmuş məqsədə çatmaq üçün aşağıdakı **vəzifələr** həll edilmişdir:

- KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün mövcud metod və alqoritmlərin təhlili və tədqiqi;
- KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün konseptual modelin işlənməsi;
- KFS sistemlərinin kiber dayanıqlığını təmin edən böyük verilənlərin intellektual emalı üçün metod və alqoritmlərin işlənməsi;
- KFS sistemlərinin informasiya texnologiyalarının kibertəhlükəsizliyinin təmin edilməsi üçün metod və alqoritmlərin işlənməsi;
- KFS sistemlərinin əməliyyat texnologiyalarının təhlükəsizliyinin təmin edilməsi üçün metodlarının işlənməsi;
- KFS sistemlərinin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metodun işlənməsi;
- KFS risklərinin qiymətləndirilməsi üçün metodun işlənməsi.

Tədqiqat metodları. Dissertasiya işində qarşıya qoyulmuş məsələni həll etmək üçün informasiya təhlükəsizliyi nəzəriyyəsi,

maşın təlimi, ehtimal nəzəriyyəsi, qeyri-səlis ədədlər nəzəriyyəsi, obrazların tanınması nəzəriyyəsi, risk təhlili və qərarların qəbul olunması texnologiyalarından istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar:

- KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün konseptual modeli;
- KFS sistemlərinin bloklanması risklərini azaltmaq üçün k-means metoduna əsaslanan böyük verilənlərdə kənar göstəricilərin aşkarlanması alqoritmi;
- Çəkili klasterləşdirmə əsasında KFS sistemlərinin böyük verilənlərin təhlili alqoritmi;
- KFS sistemlərinin uğursuzluq risklərini azaltmaq üçün paralel böyük verilənlərin emalı metodu;
- Konsensus ansamblı əsasında KFS sistemlərinin böyük verilənlərinin klaster analizi metodu;
- Ekstremal maşın təlimindən istifadə etməklə KFS sistemlərdə kiberhücumların təsnifatı metodu;
- Təsnifatçılar ansamblından istifadə etməklə DoS hücumlarının aşkarlanması metodu;
- Kiberhücumlarda vizual təsvirlərə əsaslanan KFS sistemlərdə zərərli proqram təminatının aşkarlanması alqoritmi;
- Su təmizləmə sistemi üçün iyerarxik gizli Markov modelləri əsasında KFS sistemlərinin əməliyyat texnologiyalarında anomaliyaların aşkarlanması metodu;
- Transfer təlimi istifadə etməklə KFS sistemlərinin akustik siqnallarında anomaliyaların aşkarlanması metodu;
- Su təmizləmə sistemi üçün dərin hibrid modeldən istifadə etməklə KFS cihazlarına hücumların aşkarlanması metodu;
- KFS sistemlərdə vizual təsvirlərə əsaslanan nasazlıqların təsnifat metodu;
- Təbii qaz boru kəmərinin nəqli üçün Bayes hücum qraf əsasında KFS sistemlərinin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metodu;

– Külək enerjisi istehsalı üçün qeyri-səlis Suqeno inteqralından istifadə edən risklərin qiymətləndirilməsi metodu.

Tədqiqatın elmi yeniliyi aşağıdakılardan ibarətdir:

– KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün bir sıra problemlərin həlliyinə üç səviyyəli konseptual model işlənmişdir;
– KFS sistemlərinin bloklanması risklərini azaltmaq üçün k-means metoduna əsaslanan böyük verilənlərdə kənar göstəricilərin aşkarlanması alqoritmi işlənmişdir;
– Çəkili klasterləşdirmə əsasında KFS sistemlərinin böyük verilənlərin təhlili alqoritmi işlənmişdir;
– KFS sistemlərinin uğursuzluq risklərini azaltmaq üçün paralel böyük verilənlərin emalı metodu işlənmişdir;
– Konsensus ansamblı əsasında KFS sistemlərinin böyük verilənlərinin klaster analizi metodu işlənmişdir;
– Ekstremal maşın təlimindən istifadə etməklə KFS sistemlərdə kiberhücumların təsnifatı metodu işlənmişdir;
– Təsnifatçılar ansamblından istifadə etməklə DoS hücumlarının aşkarlanması metodu işlənmişdir;
– Kiberhücumlarda vizual təsvirlərə əsaslanan KFS sistemlərdə zərərli proqram təminatının aşkarlanması alqoritmi işlənmişdir;
– Su təmizləmə sistemi üçün iyerarxik gizli Markov modelləri əsasında KFS sistemlərinin əməliyyat texnologiyalarında anomaliyaların aşkarlanması metodu işlənmişdir;
– Transfer təlimindən istifadə etməklə KFS sistemlərinin akustik siqnallarında anomaliyaların aşkarlanması metodu işlənmişdir;
– Su təmizləmə sistemi üçün dərin hibrid modelindən istifadə etməklə KFS cihazlarına hücumların aşkarlanması metodu işlənmişdir;
– KFS sistemlərdə vizual təsvirlərə əsaslanan nasazlıqların təsnifat metodu işlənmişdir;

- Təbii qaz boru kəmərinin nəqli üçün Bayes hücum qraf əsasında KFS sistemlərinin funksional komponentlərin zəifliklərinin kritikliyini müəyyən etmək üçün metodu işlənmişdir;
- Külək enerjisi istehsalı üçün qeyri-səlis Suqeno inteqralından istifadə edən risklərin qiymətləndirilməsi metodu işlənmişdir.

Tədqiqatın nəzəri və praktiki əhəmiyyəti ondan ibarətdir ki, işlənmiş metod və alqoritmlərdən ƏT təhlükəsizliyinin və İT kibertəhlükəsizliyinin təkmilləşdirilməsi məqsədilə kiber-fiziki sistemlərin kiber dayanıqlığını təmin etmək üçün istifadə oluna bilər. İşlənmiş metod və alqoritmlər elmi jurnallarda dərc edilmiş, beynəlxalq elmi konfranslarda məruzələr şəklində təqdim edilmiş və ictimaiyyətin istifadəsinə verilmişdir. Alınan nəticələrin elmi əsaslılığı və etibarlılığı müasir tədqiqat metodlarından istifadə etməklə, eləcə də onların effektivliyini təsdiq etmək üçün tədqiq olunan sahədə əvvəllər təklif edilmiş metod və alqoritmlərin nəticələri ilə müqayisə edilməklə təsdiqlənir.

Dissertasiya işində alınmış nəticələr praktiki əhəmiyyəti malikdir və aşağıdakı sahələrdə istifadə oluna bilər:

- KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün strategiya və proqramları üçün təkliflərin işlənməsi;
- KFS sistemlərinin etibarlılığını, kibertəhlükəsizliyini, kiber dayanıqlığını və effektivliyini təmin etmək üçün kiberhücumların aşkarlanması sistemlərində;
- İT kibertəhlükəsizliyi və ƏT mühafizəsini üçün KFS sistemlərinin kiber dayanıqlığının təhlilində ekspertlər tərəfindən tətbiqi.

İşin aprobasiyası və nəticələrin tətbiqi. Dissertasiyanın əsas elmi-nəzəri və praktiki nəticələri Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun seminarlarında təqdim edilmiş və müzakirə edilmişdir. Onlar bir sıra beynəlxalq və respublika səviyyəli konfranslarda məruzə edilmiş və müzakirə olunmuşdur: «Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları» III respublika elmi-praktiki konfransı (Sumqayit,

15-16 dekabr 2016-cı il); «Proqram mühəndisliyinin aktual elmi-praktiki problemləri» I respublika konfransı (Bakı, 17 may 2017-ci il); «Big data: imkanları, multidissiplinar problemləri və perspektivləri» I respublika elmi-praktiki konfransı (Bakı, 25 fevral 2016-cı il); XIII Международной научно-технической конференции «Распознавание-2017» (г. Курск, Россия, 16-19 мая 2017 г.); «İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri» IV respublika konfransı (Bakı, 14 dekabr 2018-ci il); X Международной конеренции «Application of Information and Communication Technologies» (AICT-2016) (г. Баку, 12-14 октября 2016 г.); «İnformasiya təhlükəsizliyinin aktual problemləri» III respublika elmi-praktiki konfransı (Bakı, 8 dekabr 2017-ci il) ; XV Международной научно-технической конференции «Распознавание-2019» (г. Курск, Россия, 14-17 мая 2019 г.); XIII Международной молодежной научной конференции «Technical Sciences. Industrial Management» (г. Боровец, Болгария, 11-14 марта 2020 г.); «Global Cyber Security Forum 2019» (г. Харьков, Украина, 14-16 ноября 2019); XIV Международной научно-технической конференции «Распознавание-2018» (г. Курск, Россия, 25-28 сентября 2018 г.); XIII Международной конеренции «Application of Information and Communication Technologies» (AICT-2019) (г. Баку, 23-25 октября 2019 г.); «İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri» V respublika konfransı (Bakı, 29 noyabr 2019-cu il); Международной конференции «Information Security: Problems and Prospects» (г. Баку, 29 октября 2021 г.); Международном научном семинаре NATO ARW «Cybersecurity of Industrial Control Systems (ICS)» (г. Баку, 27-29 октября 2021 г.); XI «Национальном Суперкомпьютерном Форуме (НСКФ-21)» (г. Переславль-Залесский, Россия, 30 ноября – 3 декабря 2021 г.); XVI Международной конференции «Application of Information and Communication Technologies» (AICT-2022) (г. Вашингтон, США, 12-14 октября 2022 г.); XVII Международной научно-технической конференции «Распознавание-2023» (г. Курск, Россия, 12-15 сентября 2023 г.).

İddiaçı dissertasiya işinin mövzusu üzrə Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişaf Fondu (EİF-11-1(3)-82/08/1, EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/18/1, EİF-KETPL-2-2015-1(25)-56/05/1, AEF-MCG-2023-1(43)-13/04/1-M-04), Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondu və Azərbaycan Milli Elmlər Akademiyası tərəfindən maliyyələşdirilən qrant layihələrinin icrasında iştirak etmişdir.

Dissertasiya işinin yerinə yetirildiyi təşkilatın adı. Azərbaycan Respublikası Elm və Təhsil Nazirliyi İnformasiya Texnologiyaları İnstitutu.

Elmi nəşrlər. Dissertasiyanın mövzusu üzrə 33 elmi iş nəşr edilmişdir. Onlardan 17 məqaləsi xarici jurnallarda, o cümlədən 2 məqalə Azərbaycan Respublikası Prezidenti yanında Ali Attestasiya Komissiyasının tövsiyə etdiyi resenziya olunan jurnallarda, 4 məqalə beynəlxalq Scopus və 11 əsər Web of Science bazalarında indeksləşən jurnallarda nəşr edilmişdir. 16 tezis isə beynəlxalq və respublika konfranslarının materiallarında nəşr edilmişdir.

İşin strukturu və həcmi. Dissertasiya işi giriş, 5 fəsil, nəticə və 409 ədəbiyyat siyahısından (o cümlədən 11 Azərbaycan dilində, 13 rus dilində və 385 ingilis dilində) ibarətdir. İşin ümumi həcmi 54 şəkil, 80 cədvəldən, 318 səhifədə ibarətdir.

DİSSERTASİYA İŞİNİN MƏZMUNU

Girişdə dissertasiya işinin mövzusunun aktuallığını əsaslandırılmış, tədqiqatın məqsəd və məsələləri müəyyən edilmiş, işin elmi yeniliyini, nəzəri və praktiki əhəmiyyəti və müdafiəyə çıxarılan əsas müddəaları, işin strukturunu və məzmununu göstərilmişdir.

Birinci fəsil KFS sisemlərinin kiber dayanıqlığını və nformasiya təhlükəsizliyini təmin etmək üçün mövcud metod və alqoritmlərin təhlili və tədqiqinə həsr edilmişdir. KFS sistemlərinin yaradılması insanların qarşısında yeni vəzifələr qoydu. KFS sistemlərinin informasiya təhlükəsizliyinin təmin edilməsi kiberhücumlardan müdafiə vasitələrinin geniş spektrində ən mürəkkəb problemlərdən biridir. Bu fəsil KFS sistemlərinin iş prinsipini təsvir edir. KFS üçün kiberhücumların və təhdidlərin əsas növləri nəzərdən keçirilir. KFS sistemlərinin böyük verilənlərinin intellektual emalı, İT kibertəhlükəsizliyinin təmin edilməsi, ƏT şəbəkədə anomaliyaların aşkarlanması və KFS sistemlərinin kiber dayanıqlığının qiymətləndirilməsi üzrə mövcud tədqiqat işlərinin təhlili aparılır. Fəsil altı paraqrafdan ibarətdir.

Birinci paraqrafda KFS sistemlərinin formalaşması və inkişafı xüsusiyyətləri təhlil edilir. KFS sistemlərinin ümumi strukturu təsvir edilir və sistemlərinin kiber dayanıqlığının qiymətləndirilməsi üçün faydalı alət kimi xidmət edə biləcək əsas standartlar təqdim olunur. Kiber-fiziki sistemlərinin kibertəhlükəsizliyinin təmin edilməsi sahəsində ən son tədqiqatları təhlil etmək üçün dörd tədqiqat kateqoriyası müəyyən edilmişdir: kiberhücumların nəticələrinin qiymətləndirilməsi, KFS sistemlərdə hücumların modelləşdirilməsi, KFS sistemlərdə hücumların aşkarlanması və təhlükəsizlik arxitekturasının işlənməsi.

İkinci paraqrafda KFS sistemlərinin böyük verilənlərinin intellektual emalı üçün metod və alqoritmlər təhlil edilir. KFS məlumatlarını toplamaq üçün sensorlar, aktuatorlar və digər cihazlardan istifadə onların təhlili üçün faydalı məlumat verir. Böyük verilənlərlə işləmək tədqiqatçıların istifadə etdiyi yeni metodların rəsmiləşdirilməsini və maşın təlimini metodlarının imkanlarından

istifadə edən yeni alqoritmlərin işlənməsini zəruri edir. Tədqiqatçılar DoS hücumlarının risklərini azaltmaq və KFS sistemlərinin İT domenlərinin fəaliyyətini bloklamaq üçün verilənlərin bölünməsi və aprior biliklərin istifadəsi kimi müxtəlif yanaşmalara müraciət etməlidirlər. Bununla belə, mövcud alqoritmlər yüksək hesablama mürəkkəbliyinə görə həmişə effektiv olmur.

Üçüncü paraqraf İT kibertəhlükəsizliyinin və KFS sistemlərinin ƏT mühafizəsinin təmin edilməsi metdlarının təhlili və tədqiqinə həsr edilmişdir. KFS sistemlərdə risk təhlili, kiberhücumlarının aşkarlanması, kiber dayanıqlıq və insidentlərə reaksiya sahəsində bəzi müasir həllər təsvir edilmişdir. Ənənəvi təhlükəsizlik mexanizmləri kiberhücumçular tərəfindən istifadə edildiyi üçün getdikcə daha az təsirli olur. Bu baxımdan kiberhücumların aşkarlanması üçün daha effektiv metodların işlənməsi KFS sistemlərinin İT və ƏT-ni kibertəhlükələrdən qorumaq üçün ən mühüm məsələdir. Təhlükəsizlik sahəsində mövcud tədqiqatların təhlili əsasında KFS sistemlərinin funksional modeli əsasında "hücum ağacı" və təhdidlər təklif olunur. "Ağac"ın budaqlarına aşağıdakı hücum növləri daxildir: a) sensor cihazlara hücumlar; b) aktuatorlara hücumlar; c) hesablama komponentlərinə hücumlar; d) rabitə vasitələrinə hücumlar; e) əks əlaqəyə hücumlar. Sənayedə anomaliyaların aşkarlanması vacibdir, çünki aşkarlanmamış nasazlıqlar kritik ziyana səbəb ola bilər. Anomaliyaların əvvəlcədən aşkarlanması nasazlığa meyilli sənaye avadanlıqlarının etibarlılığını artıra, istismar və texniki xidmət xərclərini azalda bilər.

Dördüncü paraqrafda KFS sistemlərinin kiber dayanıqlığının qiymətləndirilməsi metod və alqoritmləri təhlil və tədqiq edilir. Hazırda KFS sistemlərinin kiber dayanıqlığını təhlil etmək üçün çox yanaşma təklif edilmişdir. Bununla belə, cihazlar və zəifliklər arasında korrelyasiyaya az diqqət yetirilir. Mövcud metodlar KFS mühitində ümumi çoxmərhələli kiberhücumları hərtərəfli təhlil edə bilmir. Mövcud işlərin əksəriyyəti əsasən nəzəri tədqiqatlara yönəlib və maşın təlimi metodlarına əsaslanan KFS sistemlərinin kiber dayanıqlığının yalnız məhdud qiymətləndirilməsini təmin edir. Zəiflik qraf bir sıra eksploitlərdən istifadə edərək bütün mümkün

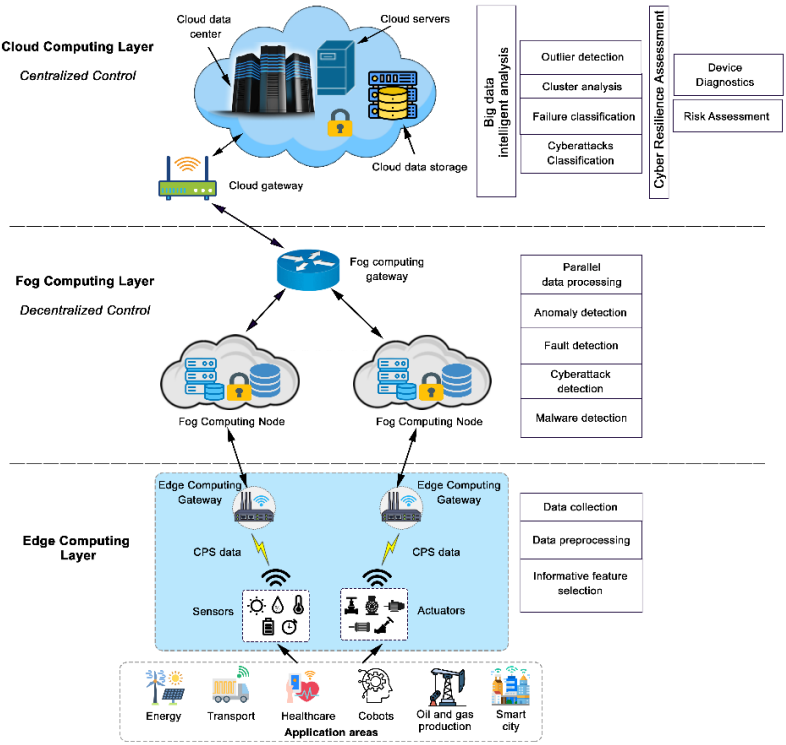
kiberhücum yollarını sadalayan perspektivli metoddur. Buna görə də, tədqiqatçılar və ekspertlər KFS sistemlərinin kiber dayanıqlığını qraflar əsasında təhlil etməkdə maraqlıdırlar. Kiber dayanıqlığın məqsədi bütün mövcud kiberresursları əhatə etməklə bütün KFS sistemini hərtərəfli təhlükəsizlikdir.

Beşinci paraqraf elmi tədqiqat məsələsini müəyyən edir. Dissertasiya işində istifadə olunan əsas anlayışlar və təriflər verilmişdir. Əsas diqqət KFS sistemlərinin kiber dayanıqlıq anlayışının təsvirinə verilir. KFS sistemlərdə kiberhücumların və kibertəhdidlərin əsas növləri nəzərdən keçirilir.

Altıncı paraqraf KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün konseptual modelin işlənməsinə həsr edilmişdir. Təklif olunan konseptual model üç əsas səviyyədən ibarət olan iyerarxik arxitekturadır: kənar hesablama səviyyəsi, duman hesablama səviyyəsi və bulud hesablama səviyyəsi (Şəkil 1). Kənar hesablama səviyyəsinə verilənlərin toplanması və real vaxt rejimində ilkin emal edilməsi üçün istifadə olunan sensorlar və aktuatorlar kimi ağıllı cihazlar daxildir. Bu səviyyə verilənləri müvəqqəti olaraq saxlayır və anormal vəziyyətin aşkarlanması ilə bağlı ilkin qərarlar yarada bilər. Kənar hesablama səviyyəsi həmçinin protokola əsaslanan kibertəhlükəsizlik autentifikasiyasını həyata keçirir. Baxmayaraq ki, bu səviyyə sensor və aktuator verilənlərini real vaxt rejimində ilkin emal edir, nəticələri dəqiqləşdirmək və qərarlar qəbul etmək üçün əlavə emal tələb edir. Bu məqsədlə əldə edilən verilənlər duman hesablama səviyyəsinə göndərilir.

Duman hesablama səviyyəsi şəbəkə keçidilər, duman hesablama xidmətləri, yönləndiricilər, erişim nöqtələri, baza stansiyaları və açarları ehtiva edən çoxlu paylanmış qovşaqlardan ibarətdir. Duman hesablamaları KFS sistemlərinin anormal işləməsini, kiberhücumlar nəticəsində yaranan sistem nasazlıqlarını və zərərli proqramların aşkarlanmasına yönəlmiş mərkəzləşdirilməmiş platforma təqdim edir. O, bulud xidmətlərini şəbəkə kənarının işlənməsi və təhlili üçün genişləndirir. Duman hesablama səviyyəsi şəbəkənin kənarında yerləşir, burada duman hesablama qovşaqları cihazlarda və bulud səviyyələrində yerləşdirilir. Bu, hesablama mürəkkəbliyini və enerji

istehlakını azaldır, daha az resurs və yüksək effektiv gücdən istifadəni təmin edir. Bu halda hesablamalar həm statik, həm də dinamik (mobil) ola bilər.



Şəkil 1. KFS sistemlərin kiber dayanıqlığını təmin etmək üçün konseptual modeli

Bulud hesablama səviyyəsi bir neçə serverdən, məlumat anbarından, bulud verilənlər mərkəzindən və şəbəkə keçidilərdən ibarətdir. Bu səviyyə yüksək məhsuldar hesablamalar həyata keçirir və enerji, nəqliyyat, səhiyyə, kobotlar, neft və qaz hasilatı, ağıllı şəhər və s. kimi sahələr üçün xidmətlər təqdim edir. Bulud hesablama səviyyəsi mərkəzləşdirilmiş idarəetməni həyata keçirir, böyük verilənlərin daimi saxlanmasını təmin edir və KFS sistemlərinin kiber dayanıqlığının qiymətləndirilməsi daxil olmaqla, onların intellektual

təhlilini həyata keçirir. Böyük verilənlərin intellektual təhlili axın və toplu emal imkanlarını təmin edir. Bu, istehsal prosesinə minimum insan müdaxiləsinə gətirib çıxarır və ekspert məlumatlarının qiymətləndirilməsi (paralel emal, kənar göstəricilərin aşkarlanması, klaster təhlili, uğursuzluq və kiberhücumların təsnifatı) real vaxt rejimində kiçik ekspertlər qrupu və ya maşın təlimi texnologiyalarından istifadə etməklə həyata keçirilə bilər. Bulud hesablama cihazları simli bağlantılar və simsiz mühitlər (Bluetooth, 5G, ZigBee, WiFi və simsiz LAN) vasitəsilə duman hesablama qovşaqlarına qoşulur. Bulud hesablama səviyyəsi dərin neyron şəbəkələrə əsaslanan böyük və mürəkkəb modelləri öyrənilir. Bu modellər tələb əsasında kənar və duman hesablama qovşaqlarına köçürülə bilər. Bu, duman və kənar hesablama səviyyələrində hesablama resurslarının istehlakını azaldır.

Təklif olunan arxitektura tədqiqatçılar, sənayeçilər və peşəkarlar üçün tələb olunan etibarlılığa, kibertəhlükəsizliyə, kiber dayanıqlığa və səmərəliliyə nail olmaq üçün sistemin modelləşdirilməsi, idarə edilməsi, monitorinqi, verilənlərin toplanması və təhlili nöqteyi-nəzərindən KFS arxitekturasının hər bir səviyyəsini təhlil etmək üçün lazımi təlimat verə bilər.

KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün proseslərin idarə edilməsi üçün mövcud metodların təhlili göstərir ki, aşağıdakı məsələlər aktualdır: böyük verilənlərin intellektual emalı üçün metod və alqoritmlərin işlənməsi; KFS sistemlərinin İT domenlərdə kibertəhlükəsizliyinin və KFS sistemlərinin ƏT təhlükəsizliyindən qorunmasının təmin edilməsi metod və alqoritmlərinin işlənməsi; KFS sistemlərinin funksional komponentlərinin zəifliklərinin müəyyən edilməsi üçün metodun və KFS risklərinin qiymətləndirilməsi metodunun işlənməsi.

İkinci fəsil KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün böyük verilənlərin intellektual emalı üçün metod və alqoritmlərin işlənməsinə həsr edilmişdir. Verilənləri təhlil edərkən məlumatın keyfiyyəti böyük əhəmiyyət kəsb edir. Bu məsələ toplanmış məlumatların böyük həcmdə artması ilə çətinləşir. Böyük verilənlərlə işləmək böyük hesablama resursları tələb edir. Bu

baxımdan tədqiqatçılar böyük verilənlərin intellektual təhlili üçün effektiv metod və alqoritmlərin işlənməsinə xüsusi diqqət yetirirlər. Həll olunan məsələlərin yüksək əhəmiyyəti bu sahədə çoxlu müxtəlif metodların meydana çıxmasına səbəb olmuşdur. Metodlar bir-birindən tətbiqi asanlığı, verilənlərin emalı üçün tətbiqi və əsas prinsipləri ilə fərqlənir. Fəsil dörd paraqrafdan ibarətdir.

Birinci paraqrafda KFS sistemlərinin bloklanması risklərini azaltmaq üçün k-means metoduna əsaslanan böyük verilənlərdə kənar göstəriciləri aşkarlanmaq üçün alqoritmi təqdim edilmişdir.

Böyük verilənlərin analitikası böyük hesablama resursları və yaddaş resursları tələb edir. Bu resurslar həmişə mövcud olmur və böyük hesablama xərcləri tələb edir. Bu baxımdan, böyük verilənlərin təhlili üçün yeni alqoritmlərin təklifi ən effektiv yanaşmalardan biridir. k-means alqoritmi sürətli yaxınlaşma dərəcəsinə malikdir və böyük hesablama resursları tələb etmir. Buna görə də, kiçik verilənlərinin klasterləşdirməsində məşhurdur. Lakin verilənlər dəstlərinin ölçüsü artdıqda böyük hesablama xərcləri tələb olunur.

Fərz edək ki, $x_i \in R^n$ $(i = \overline{1,n})$ verilənlər bazasından nöqtəsidir, burada n – verilənlər bazasında nöqtələrinin ümumi sayıdır, $x_i \in c_p \in R^k$ $(p = \overline{1,k})$ – klaster nömrəsidir və k – klasterlərin sayıdır. Klasterlərinin kompaktlığı (S_W), klasterlərinin ayrılmasını (S_{BW}) və klasterlərinin uzaqlığı (S_B) - hər bir klasterin mərkəzinin (O_p) giriş verilənlər bazasındaki bütün nöqtələrin mərkəzindən (O) məsafəsi aşağıdakı kimi hesablanır:

$$S_W = \sum_{p=1}^{k} \sum_{i=1}^{n} (x_i - O_p)(x_i - O_p)^T, \quad (1)$$

$$S_{BW} = \sum_{p=1}^{k-1} \sum_{q=p+1}^{k} (O_p - O_q)(O_p - O_q)^T, \quad (2)$$

$$S_B = \sum_{p=1}^{k} (O_p - O)(O - O_p)^T, \quad (3)$$

$$O = \frac{1}{n} \sum_{i=1}^{n} x_i, \quad O_p = \frac{1}{n_p} \sum_{x_i \in C_p} x_i, \quad n_p = |C_p|, \quad p = 1,2,\dots,k. \quad (4)$$

Klasterləşmədən istifadə edərək böyük KFS verilənlərində kənar göstəriciləri aşkarlanmaq üçün üç alqoritm təklif olunmuşdur. Birinci alqoritm üçün vəzifə aşağıdakı funksiyanı maksimuma çatdırmaqdır:

$$F_1(x) = \frac{S_B + S_{BW}}{S_W} \longrightarrow \max. \quad (5)$$

İkinci alqoritm üçün vəzifə aşağıdakı funksiyanı maksimuma çatdırmaqdır:

$$F_2(x) = \frac{S_B * S_{BW}}{S_W} \longrightarrow \max. \quad (6)$$

Üçüncü alqoritmdə vəzifə eksperimental olaraq təyin olunan nizamlanma parametri (α) ilə bağlı məqsəd funksiyasını maksimuma çatdırmaqdan ibarətdir:

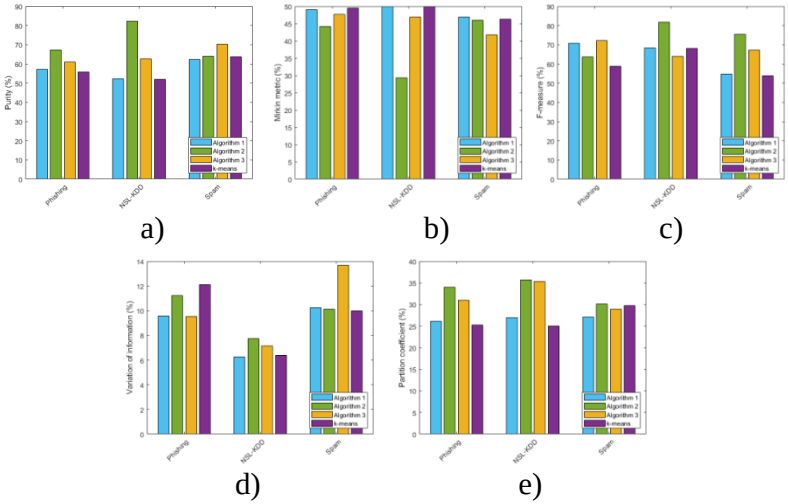
$$F_3(x) = \frac{1}{S_W}(\alpha S_B + (1-\alpha) S_{BW}) \longrightarrow \max. \quad (7)$$

Alqoritmlər klasterlərin kompaktlığını minimuma endirir və klasterlərin mərkəzləri arasındakı məsafələrə görə bir-birindən ayrılmasını maksimum dərəcədə artırır və klaster mərkəzlərini verilənlər bazasında seçilmiş ümumi nöqtə mərkəzindən çıxarır.

Eksperimentlər kiçik, orta və böyük real verilənlər bazaları üzərində aparılıb və təklif olunan alqoritmlərin effektivliyini nümayiş etdirib. UCI repozitoriyasından Phishing və Spam verilənlər bazaları və NSL-KDD verilənlər bazası daxil olmaqla üç verilənlər bazaları nəzərdən keçirilmişdir. NSL-KDD kiberhücum siqnaturası verilənlər bazası KDD-99 verilənlər bazası üzərində qurulub. Təlim (125973 nümunə) və test (22544 nümunə) verilənlər bazasından ibarətdir. Hər bir nümunə ya "anomaliya" və ya "normal" vəziyyət kimi etiketlənir. Bu tədqiqatda bütün nümunələr (148517) nəzərdən keçirilmişdir. Spam verilənlər bazası spam və qeyri-spam e-poçtları ehtiva edir. Müəyyən bir sözün və ya simvolun e-poçtda nə qədər tez-tez göründüyünü göstərən və böyük hərf ardıcıllığının uzunluğunu ölçən funksiyaları ehtiva edir. Verilənlər bazası iki sinifdən ibarətdir: spam ("anomaliya") və ya "normal". Phishing 11055 fişinq saytını əhatə edir. Buraya 30 əlamətlər daxildir (IP ünvanı, URL və anomal URL uzunluqları, vebsayt yönləndirmələri və s.). Verilənlər bazaları iki sinfə bölündü. İlkin emal zamanı verilənlər bazasındakı qiymətlər normallaşdırıldı.

α nizamlanma parametrinin üçüncü təklif olunan alqoritmin effektivliyinə təsiri müxtəlif verilənlər bazaları üçün nəzərdən keçirilmişdir. Təklif olunan alqoritmlərin səmərəliliyini

qiymətləndirmək üçün verilənlər nöqtələri cütləri arasındakı məsafəyə əsaslanan klasterləşmə ölçüləri, yəni Purity, Mirkin metrikası, PC (partition coefficient), VI (variation of information), F-measure və V-measure nəzərdən keçirilmişdir. Təklif olunan birinci, ikinci, üçüncü alqoritmlər və k-means alqoritmi üçün alınan nəticələr Şəkil 2-də daha aydın şəkildə təsvir edilmişdir. K-means alqoritmi ilə müqayisə təklif olunan yanaşmanın üstünlüyünü sübut etdi.



Şəkil 2. Təklif olunan alqoritmlərin metrikalar əsaslı k-means alqoritmi ilə müqayisəsi

Eksperimental nəticələrə əsasən belə qənaətə gəlmək olar ki, təklif olunan üç alqoritm Phishing verilənlər bazası üçün Purity, F-measure və PC metrikaları baxımından k-means alqoritmindən üstündür. NSL-KDD verilənlər bazası üçün yuxarıdakı üç metrikaları əsasən təklif olunan birinci və ikinci alqoritmləri tətbiq etməklə ən yaxşı nəticələr əldə edilmişdir. Bütün metrikaları görə, ikinci alqoritm Phishing verilənlər bazası üçün ən yaxşı nəticəni göstərdi. Eyni zamanda, Purity, Mirkin, F-measure və PC metrikalari ikinci alqoritmin tətbiqi zamanı NSL-KDD verilənlər bazası üçün yaxşı nəticələr göstərdi. Təklif olunan üçüncü alqoritm NSL-KDD və Spam verilənlər bazaları üçün ən yaxşı nəticələri göstərdi, ən aşağı

qiymətlər isə Phishing verilənlər bazası üçün müşahidə edildi. Belə nəticəyə gəlmək olar ki, üçüncü alqoritm kiçik və böyük ölçülü verilənlər bazalarında yaxşı işləyir, ikinci alqoritm isə orta ölçülü verilənlər bazalarında ən yaxşı nəticələri göstərmişdir.

İkinci paraqraf çəkili klasterləşdirməyə əsaslanan KFS böyük verilənlərin təhlilinin alqoritmini təqdim edir. Bu tədqiqatın məqsədi böyük verilənlərdə anomaliyaları aşkarlanması üçün klasterləşdirmə yanaşmasını işlənməsidir. Verilənlər bazaları hər bir nöqtənin çəkilərinin cəmlənməsi ilə əldə edilən çəkilər klasterlərə təyin edilmişdir. Çəkinin istifadəsi klasterləşdirmənin dəqiqliyini artırmağa imkan verir.

Fərz edək ki, $X = (x_1, x_2, \dots, x_n)$ verilənlər bazasındakı nöqtələr, burada n verilənlər bazasındakı nöqtələrin ümumi sayıdır, $x_i = (x_{i1}, x_{i2}, \dots, x_{im}) \in R^m$ – verilənlər bazasındakı nöqtə, m verilənlər nöqtələrinin ölçüsüdür, $C = (C_1, C_2, \dots, C_k)$ – klasterlər və k – klasterlərin sayıdır. Məsələ verilənlər bazasında anomaliyaları aşkarlanması üçün funksiyanı aşağıdakı kimi minimuma endirməkdir:

$$f(x) = \sum_{p=1}^{k} \sum_{x_i \in C_p} \left|C_p\right|_W * \left\|x_i - O_p\right\|^2 \longrightarrow \min, \qquad (8)$$

burada $\left|C_p\right|_W$ – p klasterin çəkisi.

Bu halda, klaster çəkisi klasterdəki bütün nöqtələrin çəkilərinin cəmi kimi müəyyən edilir:

$$\left|C_p\right|_W = \sum_{x_i \in C_p} w(x_i),\ p = 1,2, \dots, k, \qquad (9)$$

burada nöqtələrin çəkiləri verilənlər toplusunun bütün nöqtələrinin mərkəzindən məsafəsinə əsasən hesablanır

$$w(x_i) = \|x_i - O\|,\ O = \frac{1}{n}\sum_{i=1}^{n} x_i, \qquad (10)$$

və p klasterin mərkəzi (O_p) aşağıdakı kimi müəyyən edilir:

$$O_p = \frac{1}{n_p}\sum_{x_i \in C_p} x_i\,,\ n_p = \left|C_p\right|,\ p = 1,2, \dots, k. \qquad (11)$$

Alqoritmdə hər bir klaster öz mərkəzi ilə təmsil olunur və məqsəd hər bir nöqtə ilə onun təyin olunduğu klasterin mərkəzi arasındakı məsafəni minimuma endirən həll yolu tapmaqdır.

Eksperimental nəticələr eyni vaxtda həm klasterləşdirmə, həm də anomaliyaların aşkarlanması üçün təklif olunan yanaşmanın effek-

tivliyini göstərdi. k-means alqoritmi ilə müqayisə göstərdi ki, təklif olunan alqoritm KFS sistemlərdə anomaliyaları daha dəqiq aşkarlanır (Cədvəl 1). Təklif olunan yanaşmanın effektivliyini qiymətləndirmək üçün nisbi təkmilləşdirmədən istifadə edilmişdir:

$$\frac{\text{təklif olunan yanaşma} - \text{k-means}}{\text{k-means}} \times 100\%.$$

Cədvəl 1

k-means alqoritmi ilə təklif olunmuş alqoritmin performansının müqayisəsi

Metrikalar / Verilənlər bazası	Purity (%)	Mirkin (%)	F-measure (%)	VI (%)	PC (%)
NSL-KDD	3.78 (+)	0.44 (+)	0.66 (+)	13.03 (-)	10.55 (+)
Phishing	5.58 (+)	2.18 (+)	1.21 (-)	17.72 (+)	8.88 (+)

Eksperimental nəticələrə əsasən belə qənaətə gəlmək olar ki, təklif olunan yanaşma NSL-KDD verilənlər bazasında dörd metrikalarda (Purity, Mirkin, F-measure və PC) k-means alqoritmini üstələyir. Purity, Mirkin, PC və VI Phishing verilənlər bazasında yaxşı nəticələr göstərdi. F-measure metrika qiymətləri NSL-KDD və Phishing verilənlər bazasında hər iki yanaşma üçün olduqca yaxın idi. Təklif olunan yanaşma təhlil edilən verilənlər bazasının ölçüsünün artması ilə daha effektiv olur.

Üçüncü paraqraf KFS uğursuzluq riskini azaltmaq üçün böyük verilənlərin paralel işlənməsi metodunu təqdim edir. Böyük miqyaslı verilənlər bazalarının təhlili böyük hesablama gücü tələb edir ki, bu da həmişə mümkün olmur. Bu tədqiqat klasterləşmə prosesinin sürətləndirilməsi problemini həll etmək məqsədi daşıyır. Bu, k-means alqoritmin klasterləşdirilməsindən istifadə edərək verilənlər bazasını paralelləşdirmək və kiçik bloklara (batches) bölmək yolu ilə əldə edilmişdir.

Fərz edək ki, $X = \{x_1, x_2, \dots, x_n\}$ – m-ölçülü fəzada müəyyən edilmiş sonlu sayda nöqtə, q – blok ölçüsüdür, onun maksimum qiyməti $q(q < n)$ fərdi kompüter parametrləri ilə müəyyən edilir və eyni zamanda kifayət qədər tez işlənir, $C = \{C_1, C_2, \dots, C_k\}$ – klasterlər çoxluğur, burada $C_p^q(p = 1,2, \dots, k)$ — q blokun p klasteri,

k isə klasterlərin sayı və O_p^q — q blokdakı p klasterin mərkəzidir.

Məqsəd funksiyası aşağıdakı formaya malikdir:

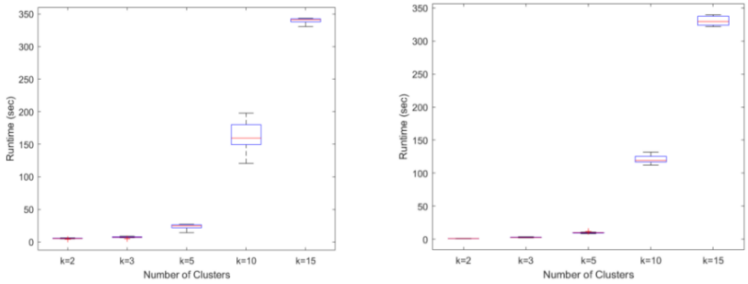
$$f(x) = \sum_{p=1}^{k} \sum_{x_i \in C_p} \left\| x_i - O_p^q \right\|^2 \longrightarrow \min, \qquad (12)$$

$$O_p^q = \frac{\sum_{x_i \in C_p^q} x_i}{\left| C_p^q \right|}, \; p = 1,2,\dots,k, \qquad (13)$$

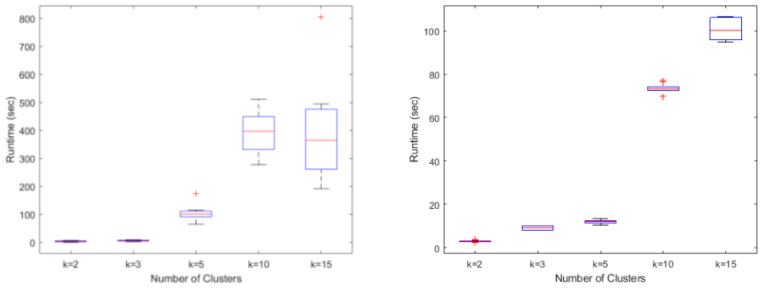
burada $\|.\|$ - $\mathfrak{R}^m$-da Evklid norması, $\left|C_p^q\right|$ isə C_p^q klasterindəki verilənlər nöqtələrinin sayıdır.

Bütün blokların mərkəzlər çoxluğuna k-means alqoritmini tətbiq etdikdən sonra alınan nəticə mərkəzi $O_p^* \, (p = 1,2,\dots,k)$ kimi işarələnir. Bu halda verilənlər bazası bir neçə bərabər bloka bölünür. Nəticədə klasterlər tam yaddaş yükləmədən paralel olaraq yaradılır ki, bu da klasterləşməni əhəmiyyətli dərəcədə sürətləndirir. Metod paralel və iterativ şəkildə işləyir. Tədqiqatın aktuallığı ondan ibarətdir ki, kiçik ölçülü blokların istifadəsi hesablama xərclərini azaldır və klasterləşdirmə alqoritminin yaxınlaşma dərəcəsini artırır.

Eksperimentlər iki verilənlər bazası üzərində aparılıb: Phone Accelerometer və Individual Household Electric Power Consumption (Şəkil 3). Phone Accelerometer verilənlər bazası 1048575 nümunə və 4 əlamətlərdən ibarətdir. İkinci verilənlər bazası üçün nümunələrin sayı 2075259 və 9 əlamətdir. Eksperimentlərdə bu verilənlər bazaları bərabər bloklara bölünür. Hər blok eyni ölçüyə malikdir (5000, 10000, 15000 və 20000 nümunə). Mərkəzləri işə salmaq üçün blokda k nümunə təsadüfi seçilir.



a) b)



c) d)

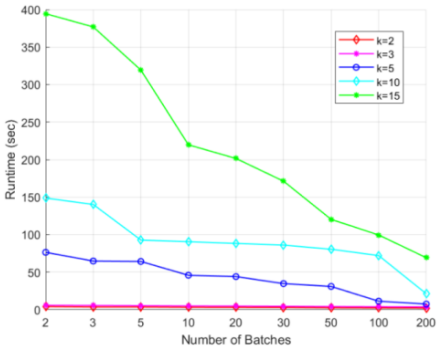
Şəkil 3. Phone Accelerometer (a, b) və Individual Household Electric Power Consumption (c, d) verilənlər bazalarında təklif olunmuş metodun və k-means alqoritminin performansının müqayisəsi

Mərkəzlər hər blokda k nümunə təsadüfi seçilir. Bu tədqiqatda təklif olunan yanaşma böyük verilənlərin paralel klasterləşdirilməsində effektivliyini sübut etmək üçün 2, 3, 5, 10 və 15-ə bərabər klaster sayına malik k-means alqoritmi ilə müqayisə edilmişdir. Təklif olunan yanaşmanın icra müddətinin və iki real verilənlər bazasında k-means alqoritminin müqayisəsi Şəkil 3-də göstərilmişdir.

Təklif olunan metodun əlavə qiymətləndirilməsi üçün nümunə kimi Individual Household Electric Power Consumption verilənlər bazasından istifadə etməklə müxtəlif sayda bloklarla təhlil aparılmışdır (Şəkil 4). k=2 və k=3 üçün təklif olunan metodu blokların sayının dəyişməsi az təsir edir. Təklif olunan yanaşma klasterlərin və blokların sayının artması ilə daha yaxşı təkmilləşdirmə təmin edir. Beləliklə, əvvəllər görülən blokların sayını (>200) artırmaq mümkündür.

Eksperimental nəticələr əsasında metodun hesablama effektivliyi k-means alqoritmi ilə müqayisədə sübut edilmişdir. Blok ölçüsünün funksiyanın orta qiymətinə və metodun orta icra müddətinə təsirini təhlil edərək belə nəticəyə gəlmək olar ki, hətta kiçik blok ölçüsü ilə də səmərəlilik əldə edilir. Klasterlərin sayının artmasına baxmayaraq, təklif olunan yanaşmanın sürəti k-means alqoritmi ilə müqayisədə xeyli yüksəkdir. Metod qısa müddətdə böyük KFS verilənlərini

klasterləşdırmağa qadirdir və sistemin nasazlığı riskini azaltmaq üçün böyük verilənləri təhlil etmək üçün istifadə edilə bilər.



Şəkil 4. Individual Household Electric Power Consumption verilənlər bazası üçün müxtəlif sayda bloklarla təklif olunmuş metodun effektivliyi

Dördüncü paraqraf konsensus ansamblına əsaslanan KFS böyük verilənlərinin klaster analizi metodunu təqdim edir. Konsensus yanaşması klaster analizi metodlarından birgə istifadənin mümkünlüyünə görə ardıcıl həll yolu tapmaqdır. Müəyyən bir oblast üçün ən uyğun klasterləşdirmə sxemi, üstünlüklərinə və fərqli xüsusiyyətlərinə görə müxtəlif alqoritm dəstlərinə konsensus yanaşması tətbiq etməklə qurula bilər. Yekun həll variantı hazırlanarkən müxtəlif baxışlar nəzərə alınır. Onlar nəinki ziddiyyət təşkil etmir, əksinə, hər bir metodun çatışmazlıqlarını kompensasiya edirlər. Konsensus qruplaşması "etibarlı" arakəsmələr yaratmağa, səs-küy və kənar göstəriciləri idarə etməyə kömək edir. Böyük KFS verilənlərinin klasterləşdirilməsi üçün perspektivli həll yolu kimi istifadə edir. Bu vəziyyətdə problem purity utility funksiyanı inkişaf etdirmək və onu səmərəli şəkildə optimallaşdırmaqdır.

Tədqiqatın məqsədi aşağıdakı optimallaşdırma problemini həll etməklə π-nin konsensus bölməsini tapmaqdır:

$$\pi^* = \underset{\pi}{\operatorname{argmax}}(w_i U(\pi, \pi_i)), \qquad (14)$$

burada π^* konsensus funksiyasıdır, U π ilə hər hansı π_i arasındakı oxşarlığı ölçən faydalı funksiyanı təmsil edir, π_i bölməsi əsas bölmədir ($1 \leq i \leq r$) və $w_i \in [0,1]$, $\sum_{i=1}^{r} w_i = 1$.
Çəkilər purity əsaslanan faydalı funksiyadan istifadə edərək fərdi klaster metodlarına təyin edilir:

$$f = (1-\lambda) \cdot \sum_{i=1}^{r} w_i U(\pi, \pi_i) + \lambda \cdot \|w\|^2 \longrightarrow \max \quad (15)$$

bir şərtlə ki,

$$\sum_{i=1}^{r} w_i = 1, w_i \geq 0, \forall i. \quad (16)$$

burada $0 \leq \lambda \leq 1$ – çəkili purity funksiyasını maksimuma çatdırmaq və w arasında uyğunluğu göstərən parametr.

Böyük verilənlərin klasterləşməsinin statistik təhlili etiketsiz KFS məlumatlarının təhlilinə çəkili konsensus klasterləşdirməsinin tətbiqinin mümkünlüyünü nümayiş etdirir. Bu məqsədlə Purity əsaslanan faydalılıq funksiyası Davies-Bouldin (DB) və Calinski-Harabasz (CH) indekslərinə əsaslanan funksiya ilə əvəz edilmişdir. DB indeksi çoxluqdaxili və çoxluqlararası məsafələrin nisbətinə əsaslanır. DB aşağıdakı kimi hesablanır:

$$DB = \frac{1}{k} \sum_{i=1}^{k} R_i \quad (17)$$

$$R_i = \max_{i \neq j} \left(\frac{\delta(C_i) + \delta(C_j)}{dist(C_i, C_j)} \right), \quad (18)$$

burada k – klasterlərin sayı, δ – klaster daxilində dispersiya, *dist* – i və j klasterləri arasındakı məsafədir. Məqsəd qiyməti indeksin minimumudur.

CH indeksi aşağıdakı funksiya ilə xarakterizə olunur:

$$CH = \frac{B(k)/(k-1)}{W(k)/(n-k)}, \quad (19)$$

burada

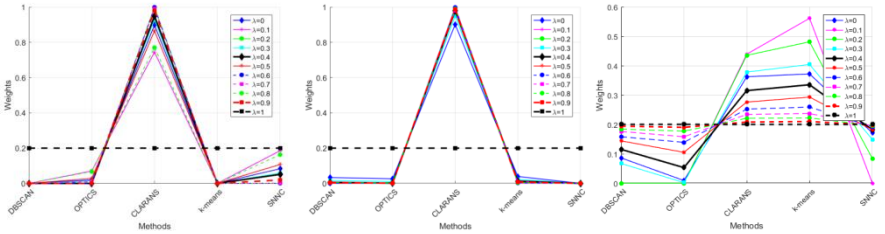
$$B(k) = \sum_{i=1}^{k} n_i \, dist^2(O_i, O), \quad (20)$$

$$W(k) = \sum_{i=1}^{k} \sum_{x \in C_i} dist^2(x, O_i), \quad (21)$$

k - klasterlərin sayı, n - nəzərdən keçirilən verilənlər bazasındakı D obyektlərin sayı, C_i – i-ci klaster, n_i - C_i-də olan obyektlərin sayı, O - verilənlər bazası D mərkəzi, O_i - verilənlər bazasında C_i mərkəzi, $W(k)$ - bütün klasterlər üçün klasterdaxili dispersiyaların cəmi və

$B(k)$ - C_i ilə verilənlər bazası D arasındakı məsafələrin kvadratlarının çəkili cəmidir. Klasterlərin ən çox ehtimal olunan sayı CH indeksinin maksimum qiymətinə çatdığı k qiymətidir.

Məsafə metrikalarından istifadə etməklə müxtəlif ölçülü verilənlər bazaları üzərində aparılan eksperimental nəticələr göstərdi ki, təklif olunan metod yüksək effektivdir və məlumatların klasterləşdirilməsi keyfiyyətinə görə müasir metodlardan üstündür. Şəkil 5-də λ parametrinin nəzərdən keçirilən NSL-KDD, Phishing və Phone Accelerometer verilənlər bazaları üçün beş klasterləşmə metodunun çəkilərinə təsiri göstərilir. Eksperimental nəticələr DBSCAN (Density-Based Spatial Clustering of Applications with Noise), OPTICS (Ordering Points to Identification the Clustering Structure), CLARANS (Clustering Large Applications with Randomized Search), k-means və SNNC (Shared Nearest Neighbor Clustering) metodları ilə müqayisədə verilənlərin klasterləşdirilməsi üçün təklif olunan metodun effektivliyini sübut etdi. Phishing verilənlər bazası üçün, kvadrat Evklid məsafəsi ilə təklif olunan konsensus yanaşması Purity (0.7166), Mirkin (0.4062), F-measure (0.7283) və PC (0.3053) metrikalarına görə ən yaxşı nəticəni verdi. Əsas bölmələrin nəticələri VI metrikalarını üstələyib və 0.0948 təşkil edib. Kvadrat Evklid məsafəsindən istifadə etməklə təklif olunan metod bütün beş metrikalar üçün ən yaxşı nəticəni göstərdi və NSL-KDD verilənlər bazası üçün CLARANS metodunun nəticəsi ilə uyğunlaşdı.



a) NSL-KDD b) Phishing c) Phone Accelerometer

Şəkil 5. Klasterləşdirmə üsullarının çəkilərinin λ parametrdən asılılığı

Phone Accelerometer verilənlər bazası üçün təklif olunan yanaşma Purity, Mirkin, F-measure və PC-də DBSCAN və OPTICS

kimi klasterləşdirmə metodlarını üstələdi, lakin VI metrikada bir qədər aşağı oldu.
Ən yaxşı nəticə kvadrat Evklid metrikasından istifadə edərək təklif olunan yanaşma ilə göstərilir.

Üçüncü fəsil KFS sistemlərinin informasiya texnologiyalarının kibertəhlükəsizliyinin təmin edilməsi metod və alqoritmlərinin işlənməsinə həsr edilmişdir. Kiberhücumlar KFS sistemlərinin İT domenlərinin fəaliyyətində müşahidə olunan anormal hadisələrin səbəblərindən biridir. Şəbəkə trafikinin anomaliyaları ayrı bir kanalın və ya bütün şəbəkə seqmentlərinin düzgün işləməməsinə səbəb ola bilər ki, bu da şəbəkə avadanlıqlarında xidmətdən imtinaya səbəb olacaqdır. Şəbəkə hücumları daim dəyişir, çünki kiberhücumçular fərdi yanaşmalardan istifadə edirlər. Bu, həm də proqram və aparatdakı dəyişikliklərdən təsirlənir. Fəsil üç paraqrafdan ibarətdir.

Birinci paraqraf ekstremal təlimi (Extreme Learning Machine, ELM) istifadə edərək KFS sistemlərdə kiberhücumları təsnif etmək üçün metod təqdim edir. Ən informativ əlamətləri seçmək üçün təsnifat alqoritminin dəqiqliyini və sürətini artırmaq üçün "atəşböcəklərinin" davranışının genetik alqoritmi istifadə edilmişdir. ELM metodu yüksək hesablama sürətinə malikdir və təlim üçün təkrarlanan parametrlərin tənzimlənməsini tələb etmir.

Eksperimentlər NSL-KDD verilənlər bazasında aparılıb. NSL-KDD verilənlər bazasında bütün kiberhücumlar dörd qrupa bölünür: DoS (Denial of Service Attack), Users to Root Attack (U2R), Remote to Local Attack (R2L) və Probe hücumları. Hər bir nümunənin 41 əlamətləri var. Metod müxtəlif aktivləşdirmə funksiyaları ilə qiymətləndirilir: radial əsas aktivləşdirmə funksiyası (radial basis activation function, RBF), üçbucaqlı əsas aktivləşdirmə funksiyası (triangular basis activation function, TriBas) və Qauss aktivləşdirmə funksiyası (Gaussian) (Cədvəl 2). Qauss aktivləşdirmə funksiyası dispersiya (σ) və riyazi gözləməsi (μ) parametrlərinin müxtəlif qiymətləri üçün tətbiq edilmişdir. DoS, U2R və R2L hücumları üçün ən yaxşı aşkarlama dəqiqliyi $\sigma = 0.1$ və $\mu = 4$ (DoS – 86.89%, U2R – 99.99% və R2L – 99.94%) ilə Qauss aktivləşdirmə funksiyası üçün əldə edilmişdir. Probe hücumlarında $\sigma = 0.2$ və $\mu =$

0 olduqda Qauss aktivləşdirmə funksiyası üçün yüksək dəqiqlik (99.06%) əldə edilmişdir.

Qauss aktivləşdirmə funksiyasından istifadə etməklə təklif olunan metod həm sürət, həm də təsnifat dəqiqliyi baxımından yüksək nəticələr nümayiş etdirdi.

ELM metoduna əsaslanan nəzərdən keçirilən yanaşma kiberhücum təsnifatının məqbul keyfiyyətini və yüksək performansını təmin edir ki, bu da onu real vaxt rejimində KFS sistemlərinin İT domenlərində müdaxilənin aşkarlanması sistemləri üçün cəlbedici həll edir.

Cədvəl 2

Müxtəlif aktivləşdirmə funksiyaları ilə müdaxilənin aşkarlanması dəqiqliyinin müqayisəsi

Aktivləşdirmə funksiyası	DoS	Probe	U2R	R2L
RBF	80.01%	91.79%	99.88%	**99.94%**
TriBas	81.60%	95.62%	99.65%	99.57%
Gaussian (σ =0.2, μ =0)	84.26%	**99.06%**	99.95%	99.70%
Gaussian (σ =0.1, μ =4)	**86.89%**	90.01%	**99.99%**	**99.94%**

Təklif olunan metod dəstək vektor maşını (support vector machines, SVM), təsadüfi meşə (random forest, RF), süni neyron şəbəkəsi (DNN) və dərin neyron şəbəkəsi alqoritmləri ilə müqayisə edilmiş və Qauss aktivləşdirmə funksiyasından istifadə edərkən ən yüksək dəqiqliyi nümayiş etdirmişdir (99.78%) (Cədvəl 3).

Cədvəl 3

NSL-KDD verilənlər bazasında təklif olunan yanaşmanın performansının qiymətləndirilməsi

Metod	Bayes Net	Logit Boost	IBk	SVM	RF	DNN	MLP	ELM (Gauss)
Accuracy (%)	69.9	78.8	99.6	93.8	97.93	91.5	81.43	**99.78**

İkinci paraqraf təsnifatçılar ansamblından istifadə edərək KFS sistemlərdə DoS kiberhücumlarının aşkarlanması metodunu təqdim edir. Serverə və ya məlumat ötürmə şəbəkəsinə DoS kiberhücumu nəticəsində xidmətlər məhdudlaşır, bu da öz növbəsində KFS sistemlərinin sıradan çıxmasına səbəb ola bilər.

Müəyyən siniflərə aid olma ehtimalını göstərən təklif olunan metod hər bir məlumat nöqtəsi üçün təsnifat xallarının vektorunu qaytarır. Təklif olunan yanaşmanın özəlliyi ondan ibarətdir ki, verilənlər bazasından hər bir nöqtə üçün alınan sinif etiketi bu nöqtə üçün təsnifat metodları ilə alınan bütün qiymətlər arasında maksimum qiymətə uyğun gəlir.

Nəzərə alınan təsnifatçılar qərar ağacları, k-ən yaxın qonşular, müxtəlif nüvə funksiyaları olan dəstək vektor maşınları və Naive Bayes (NB) idi. Beş təsnifat ansamblı ən dəqiq nəticəni göstərdi (Cədvəl 4). NB metodunun ən aşağı nəticəni (80.45%) göstərməsinə baxmayaraq, onu təsnifatçılar ansamblına əlavə etdikdə təklif olunan yanaşmanın dəqiqliyi artaraq beş təsnifatçı üçün 92.33% təşkil edib.

Purity, Mirkin, F-measure, VI və PC metrikaları üçün əldə edilmiş dərəcələrə əsasən, bütün klasterləşdirmə metodları üçün əldə edilən dərəcə hesablanmışdır:

$$rank(method) = \sum_{s=1}^{M} \frac{(M-s+1)\cdot r_s}{M}, \qquad (22)$$

burada M – metodların sayı, r_s – metodun s ranqına malik olmasının sayı.

DT+KNN+SVM(Polynom)+NB+SVM(Linear) ansamblı DoS sinfi üçün bütün dörd metrikalar (accuracy, precision, recall və F-measure) üçün ən yaxşı ranqını göstərdi.

Üçüncü paraqraf təsvirə əsaslanan KFS sistemlərdə zərərli proqramların aşkarlanması üçün alqoritmi təqdim edir. Mövcud texnologiyalar müxtəlif vasitələrdən istifadə edərək zərərli proqramların yoluxma riskini azalda bilər. Bununla belə, daha mürəkkəb zərərli proqramlara qarşı mükəmməl müdafiə yoxdur.

Transfer təlimi əsaslanan alqoritm hazırlanmışdır. O, zərərli proqramların vizuallaşdırılmasını və Radon transformasiyasını birləşdirir. Bu araşdırmada binar zərərli proqram nümunələrindən təsvirlər əldə edilmişdir.

Cədvəl 4

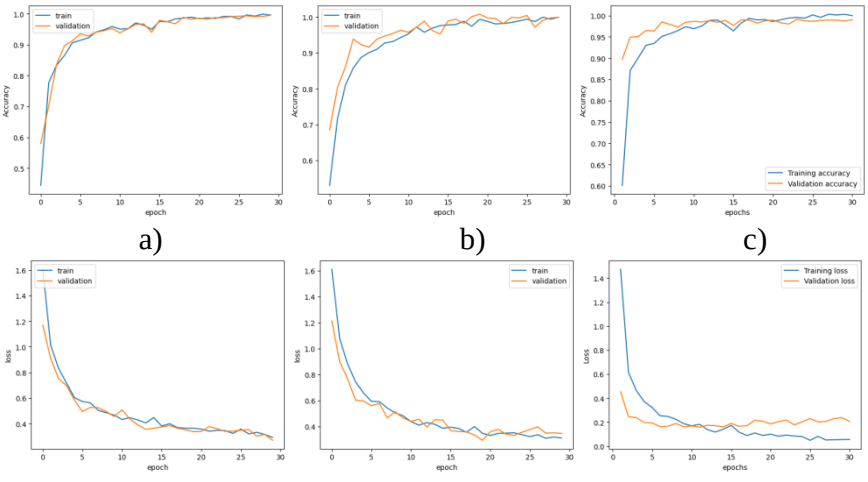
Təklif olunan metodun accuracy metrikası ilə digər təsnifatçılarla müqayisəsi [10, 12]

Sinif / Metod	DoS	"Normal" vəziyyət	Digər kiberhücumlar
DT	86.32% [7]	77.19% [7]	64.25% [8]
KNN	88.21% [3]	79.67% [3]	65.80% [6]
SVM(Linear)	87.21% [5]	77.96% [6]	66.22% [5]
SVM(Polynom)	86.64% [6]	79.50% [4]	68.31% [3]
SVM(RBF)	87.25% [4]	78.84% [5]	65.38% [7]
NB	80.45% [8]	71.25% [8]	66.50% [4]
DT+KNN+ SVM(Polynom)	90.74% [2]	84.77% [2]	74.53% [2]
DT+KNN+ SVM(Polynom)+NB +SVM (Linear)	**92.33% [1]**	**88.58% [1]**	**83.35% [1]**

Radon çevrilməsi təsvir çevrilməsidir. Bu üsul təsvirin fakturasını təmsil edən hesab edilə bilər. O, boz rəngli zərərli proqram təsvirlərinə tətbiq edilir. Digər metodlardan fərqli olaraq, Radon transformasiyası yeni əlamətlərin işlənməsini tələb etmir və zərərli proqram təsvirlərinin vizual təhlilinə əsaslanır.

Eksperimental nəticələr göstərdi ki, iki dərin neyron şəbəkəsinin (AlexNet və MobileNet) əlamətlərinin birləşməsi hətta kiçik təsvir dəyişiklikləri ilə belə KFS sistemlərdə zərərli proqramları effektiv şəkildə təsnif edə bilər. Zərərli proqram Microsoft malware BIG, IoT_Malware və MaLNet-Image verilənlər bazalarından olan təsvirlərin aşkarlanma itkisi əyriləri və təsnifat dəqiqliyi əyriləri Şəkil 6-da göstərilmişdir.

Microsoft malware BIG verilənlər bazası üçün F-measure metrikasına əsasən, zərərli proqram sinifləri Lollipop, Vundo, Kelihos_ver3, Kelihos_ver1 və Obfuscator.ACY >90% nəticə göstərdi. Bununla belə, Ramnit, Tracur və Gatak zərərli proqram ailələri precision görə daha aşağı dəqiqliklə tanınıb və müvafiq olaraq 76%, 82% və 90% təşkil edib.



a) b) c)

d) e) f)

Şəkil 6. Microsoft malware BIG (a, d), IoT_Malware (b, e) və MaLNet-Image (c, f) verilənlər bazası üçün zərərli proqram aşkarlama dəqiqliyi və itki əyriləri

MaLNeT+Images verilənlər bazası üçün precision, recall və F-measure metrikalarına əsasən Addisplay və SPR (security and privacy risk) zərərli proqram sinifləri 100% tanınıb. Eyni zamanda, təklif olunan yanaşma, nəzərdən keçirilən digər zərərli proqram sinifləri üçün də kifayət qədər yüksək dəqiqlik göstərdi. IoT_Malware verilənlər bazasının dörd sinfi üçün precision metrikindən istifadə etməklə aşağıdakı nəticələr əldə edilib: Benign (99.50%), Gafgyt (97.99%), Tsunami (96.09%) və Mirai (97.88%).

Mirai zərərli proqram ailəsinin sinfi recall metrikası ilə ən dəqiq şəkildə tanındı. Bu zərərli proqram KFS cihazlarını təhlükəyə atmağa yönəlib. Eyni zamanda, precision və F-measure metrikaları, demək olar ki, 100% dəqiqliklə Benign sinifini təyin etməyə imkan verir.

Xception, Inception, EfficientNet, CNN, VGG16, LeNet və digər metodlara müqayisə təklif olunan alqoritmin üstünlüyünü sübut etdi (Cədvəl 5).

Tədqiqat Microsoft malware BIG, IoT_Malware və MalNeT-Images zərərli proqram verilənlər bazası üçün müvafiq olaraq

99.89%, 99.95% və 99.20% dəqiqliklə sabit performans nümayiş etdirib.

Cədvəl 5

Dərin təlimi əsaslanan metodlardan istifadə etməklə təklif olunan yanaşmanın effektivliyinin qiymətləndirilməsi

Metod	Verilənlər bazası	Accuracy (%)
VGG16	Microsoft malware dataset	98.94
MobileNet		99.25
Xception		99.17
LeNet, AlexNet, InceptionV3		99.70
CNN		98.64
InceptionV3		99.60
Təklif edilən yanaşma		**99.89**
Adversarial learning	IoT_Malware dataset	97.67
CNN		95.00
Təklif edilən yanaşma		**99.95**
Vision Transformer	MalNet-Image dataset	97.00
EfficientNetB0+SVM+RF		92.90
Təklif edilən yanaşma		**99.20**

Dördüncü fəsil KFS sistemlərinin ƏT təhlükəsizliyinin təmin edilməsi metodları işlənməsinə həsr edilmişdir. KFS sistemlərinin anormal vəziyyətinə nasaz komponentlər, müvəqqəti nasazlıqlar, yanlış konfiqurasiya, kiberhücumlar və ya bunların birləşməsi səbəb ola bilər.

Kibercinayətkar sensor və ya aktuator oxunuşlarını manipulyasiya etmək üçün KFS sistemlərdə müdaxilə edərək sistemin anormal işləməsinə səbəb olur. Sənaye ssenarisində anomaliyaların aşkarlanması vacibdir, çünki aşkarlanmamış nasazlıqlar kritik zərərə səbəb ola bilər.

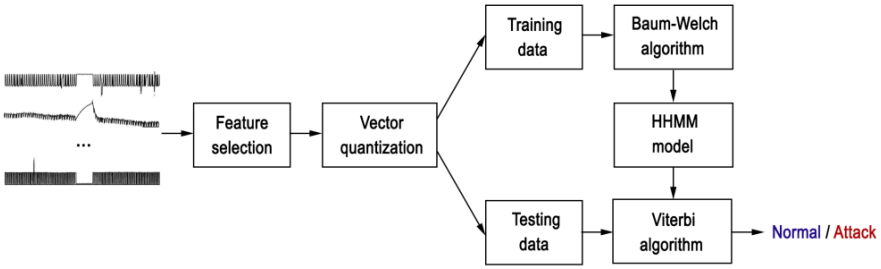
Anomaliyaların erkən aşkarlanması nasazlığa meyilli sənaye avadanlıqlarının etibarlılığını artıra, istismar və texniki xidmət xərclərini azalda bilər. Fəsil dörd paraqrafdan ibarətdir.

Birinci paraqraf iyerarxik gizli Markov modellərinə (Hierarchical Hidden Markov Model, HHMM) əsaslanan KFS sistemlərdə anomaliyaların aşkarlanması metodunu təqdim edir. Bu zaman

müşahidə edilən hadisələr HMM modellərindən istifadə etməklə modelləşdirilir. HHMM modeli mürəkkəb iyerarxik strukturu olan və zamandan asılı olan tapşırıqlar üçün uyğundur. HHMM modelindən əldə edilən normal və anormal vəziyyətlər KFS sistemlərdə kiberhücumları müəyyən etmək üçün giriş məlumatları kimi istifadə edilə bilər (Şəkil 7).

HHMM modelinin istifadə edərək KFS sistemlərdə anomaliyaların aşkarlanmasında ilk addım sensor verilənlərinin toplanmasıdır. Sonra onlardan ən məlumatlandırıcı əlamətlər seçilir. Vektor kvantlaşdırma üsullarından (məsələn, k-means alqoritmi) istifadə edərək model üçün mənalı müşahidələr yaradır. Baum-Welch alqoritmi təlim mərhələsində model parametrlərinin korreksiyasını həyata keçirir. Birinci səviyyəli HMM vəziyyətlərinin ehtimal ardıcıllığı əlamətlər vektorunun yaranması ilə nəticələnir. Bu əlamətlərə vektor kvantlaşdırmasının tətbiqi ikinci səviyyəli HMM-dan müşahidələr ardıcıllığını yaradır və s. Sonra test mərhələsində Viterbi alqoritmi təlim mərhələsinin parametrlərindən istifadə edən vəziyyətlərin ardıcıllığını müəyyən edir.

KFS komponentlərində heç bir "qeyri-adi" davranış aşkarlanmırsa, model növbəti iyerarxik səviyyəyə keçir və sistemə kiberhücum olmadığını yoxlayır.



Şəkil 7. Təklif edilən metodun ümumi sxemi

Müqayisə dərin neyron şəbəkəsi, dəstək vektor maşınları, TABOR (Time Automata and Bayesian netwORk), birölçülü konvolyusiya neyron şəbəkəsi, LSTM-CUSUM və MAD-GAN (Cədvəl 6) kimi

modellərlə aparılmışdır. F-measure metrikasından istifadə etməklə təklif edilən metodun qiymətləndirilməsi daha yüksək performans verir. Bu, HHMM modelindən istifadə etməklə KFS sistemlərdə anomaliyaların aşkarlanmasının uğurunu sübut edir.

Cədvəl 6

Təklif edilən yanaşmanın qiymətləndirilməsi

Metod	Metrikalar		
	Precision	Recall	F-measure
DNN	0.9830	0.6785	0.8028
SVM	0.9250	0.6990	0.7963
TABOR	0.8617	0.7880	0.8232
1D CNN	1.0000	0.8530	0.9200
LSTM-CUSUM	0.9070	0.6770	0.7750
MAD-GAN	0.9610	0.9420	0.9510
Təklif edilən metod	**0.9998**	**0.9164**	**0.9563**

HHMM modelinin böyük tək səviyyəli HMM modelindən üstünlüyü ondan ibarətdir ki, HHMM-nın həddən artıq uyğunlaşmadan əziyyət çəkmə ehtimalı azdır, çünki ayrı-ayrı alt komponentlər daha kiçik həcmdə verilənlər üzərində müstəqil şəkildə öyrədilir. Bunun nəticəsidir ki, HHMM modeli HMM ilə müqayisə edilə bilən performansa nail olmaq üçün əhəmiyyətli dərəcədə daha az təlim verilənləri tələb edir.

İkinci paraqraf, transfer təlimindən istifadə edərək KFS akustik siqnallarında anomaliyaların aşkarlanması metodu təqdim olunur. Dərin təlimi arxitekturasından spektroqramlar və skaloqramlar əldə etmək üçün ilkin emal etmiş akustik siqnallarla işləmək üçün istifadə olunur. Təklif olunan metodun dəqiqliyini artırmaq üçün SPOCU (scaled polynomial constant unit) aktivləşdirmə funksiyası nəzərdə tutulur. Ekstremal gradient gücləndirmə (eXtreme Gradient Boosting, XGBoost) alqoritmi yüksək performansa malik olduğu və təlim mərhələsində az hesablama resursları tələb etdiyi üçün istifadə edilmişdir.

Eksperimentlərin aparılması üçün dörd müxtəlif növ KFS cihazlarının akustik siqnallarını ehtiva edən verilənlər bazasından

istifadə edilmişdir: klapanlar, nasoslar, ventilyatorlar və sürüşdürmələr (Cədvəl 7).

Cədvəl 7

Təklif edilmiş metodun effektivliyinin qiymətləndirilməsi [26]

Model	Metrikalar	Cihaz			
		Fan	Pump	Slider	Valve
Inception+ XGBoost	Recall	87.0	95.0	98.0	100
	Precision	89.1	87.9	100	94.3
	F-measure	92.3	90.6	98.1	96.3
Xception+ XGBoost	Recall	100	88.0	98.0	100
	Precision	84.2	100	100	92.6
	F-measure	96.8	92.8	98.1	95.3
Mobilenet +XGBoost	Recall	96.0	88.0	94.0	100
	Precision	78.7	95.7	100	96.2
	F-measure	92.0	90.9	96.1	97.2
Densenet+ XGBoost	Recall	99.9	96.0	98.0	100
	Precision	87.0	100	100	97.1
	F-measure	98.2	97.1	98.1	97.7

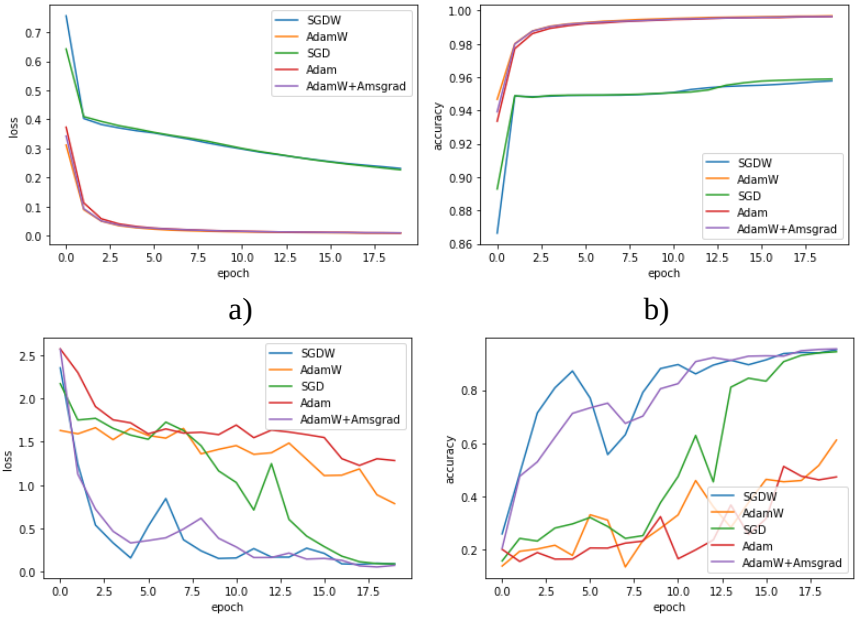
Hər bir cihaz növü üçün müxtəlif real anomaliya ssenariləri nəzərdən keçirilmişdir: çirklənmə, sızma, fırlanma disbalansı, relslərin zədələnməsi və s. Spektroqram və skaloqram təsvirlərindən əlamətləri çıxarmaq üçün aşağıdakı əvvəlcədən öyrədilmiş dərin neyron şəbəkələri nəzərdən keçirilir: Xception, MobileNet, DenseNet və Inception. Eksperimentlər göstərir ki, Densenet+XGBoost F-measure metrikasına uyğun olaraq cihaz siqnallarından anomaliyaların aşkarlanmasında digər hesab edilən modelləri üstələyir (Cədvəl 7).

Təklif edilən model digər modellərlə müqayisədə 95.45% AUC (area under the ROC curve) metrikasına uyğun olaraq cihaz sensor məlumatlarından anomaliyaların aşkarlanmasında əhəmiyyətli irəliləyiş əldə etdi.

Üçüncü paraqraf dərin hibrid modeldən istifadə edərək KFS cihazlarına kiberhücumların aşkarlanması metodunu təqdim edir.

Təklif edilən metod birölçülü konvolyusiya neyron şəbəkəsinin (convolutional neural network, CNN), idarə olunan təkrarlanan neyron şəbəkəsinin (gated recurrent unit, GRU) və uzun qısamüddətli yaddaşa (long short-term memory, LSTM) malik neyron şəbəkəsinin üstünlüklərini birləşdirir. GRU, CNN və LSTM modellərinin nəticələri KFS sistemlərdə kiberhücumların aşkarlanmasının dəqiqliyini artırmaq üçün birləşdirilir. Daha sonra onlar 150 neyrondan ibarət tam birləşmiş iki laylara qidalanırlar. Bunlardan sonra softmax layı gəlir.

Metodun dəqiqliyini artırmaq üçün SPOCU aktivləşdirmə funksiyası nəzərdən keçirilir. AdamW+Amsgrad optimallaşdırıcısı dərin neyron modelinin təlim xətasını azaltmaq və öyrənm sürətini artırmaq üçün istifadə olunur (Şəkil 8).



Şəkil 8. SWaT (a, b) və GHL (c, d) verilənlər bazalarında təklif edilən metod üçün itkilərin və kiberhücumların aşkarlanmasının dəqiqliyi əyriləri

Eksperimentlər iki verilənlər bazası üzərində aparılmışdır: SWaT (secure water treatment) və GHL (gasoil heating loop). Onlar KFS sistemlərinin "normal" vəziyyəti və kiberhücumların səbəb olduğu uğursuzluqlar haqqında məlumatları ehtiva edir.

Metod müxtəlif optimallaşdırıcılardan istifadə etməklə qiymətləndirilmişdir: stoxastik qradiyent enmə (stochastic gradient descent, SGD), azaldılmış çəkilərlə SGD (SGDW), Adam, azaldılmış çəkilərlə Adam (Adam with a weight decay, AdamW) və AdamW+Amsgrad. AdamW+Amsgrad optimallaşdırıcısı ilə təklif olunan metod ən yaxşı nəticəni göstərdi (Şəkil 8).

Təklif edilən metod sadə dərin neyron şəbəkəsi, dəstək vektor maşınları kimi məşhur maşın təlimi metodları ilə müqayisədə KFS sistemlərdə kiberhücumların aşkarlanmasının yüksək dəqiqliyini təmin edir (Cədvəl 8).

Cədvəl 8

Təklif edilən metodun müxtəlif verilənlər bazalarında qiymətləndirilməsi

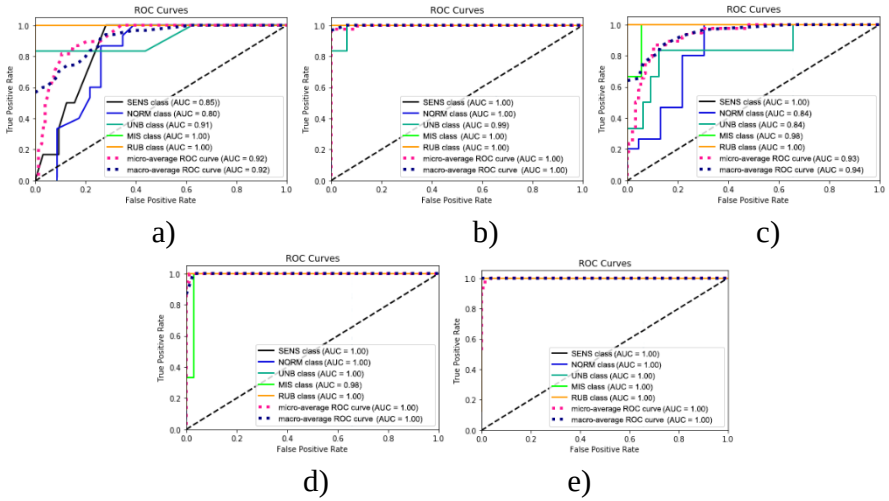
Verilənlər bazası	Metrikalar		
	Precision (%)	Recall (%)	F-measure (%)
Secure Water Treatment dataset	99.76	99.75	99.74
Gasoil Heating Loop dataset	97.06	95.66	96.04

Dördüncü paraqraf təsvirlər əsasında KFS sistemlərinin nasazlıqlarını təsnif etmək üsulu təqdim olunur. KFS sistemlərinin fəaliyyətinin qiymətləndirilməsi və nasazlıqların vaxtında aşkarlanması əməliyyat və texniki xidmət xərclərini azalda bilər. İşlənmiş metod dərin neyron şəbəkəsinin (deep neural network, DNN) və CNN modelinin üstünlüklərini birləşdirir. Tezlik və vaxt əlamətləri və vibrasiya siqnalının təsvirləri dərin hibrid modelin giriş verilənləri kimi qəbul edilir. Qısamüddətli Furye transformasiya spektroqramının təsvirləri və KFS sensor siqnallarının davamlı

veyvlet çevrilməsi skaloqramı təklif olunan metod üçün giriş verilənləri kimi qəbul edilir.

Nümunə olaraq, sualtı neft nasosunda nasazlıqların (electric submersible pump, ESP) aşkarlanması problemi nəzərdən keçirilmişdir. Vibrasiya siqnalı mexaniki cihazların, məsələn, neft avadanlıqlarının vəziyyəti haqqında ən vacib məlumatları daşıyır. KFS komponentlərinin nasazlıqlarını xarakterizə edən əlamətlər xam siqnalların ağıllı təhlili və nasazlıq diaqnostikasının dəqiqliyini artırmaq üçün çıxarılır.

ROC əyri (receiver operator characteristic) analizi təklif olunan dərin hibrid modelin keyfiyyətini qiymətləndirməyə imkan verir (Şəkil 9).



Şəkil 9. Beş sinif üzrə nəzərdən keçirilən metodların təsnifat düzgünlüyünü qiymətləndirmək üçün ROC əyriləri: faulty sensor (SENS), normal operational condition (NORM), unbalance (UNB), misalignment (MIS) и rubbing (RUB) [20]

Eksperimental nəticələr göstərir ki, bu, vibrasiya siqnallarından əldə edilən nəzərə alınan əlamətlərə əsaslanaraq neft nasosunda ESP nasazlıqlarını aşkarlanmaq üçün ən yaxşı modeldir. ROC əyrisi altındakı sahə 100% idi (Şəkil 9).

Eksperimental qiymətləndirmə göstərir ki, təklif edilən dərin hibrid model k-ən yaxın qonşular (k-nearest neighbors, KNN) daxil olmaqla əvvəllər təklif edilmiş dərin təlimi əsaslı metodlardan üstündür (Cədvəl 9).

Cədvəl 9

Təklif edilən yanaşmanın effektivliyinin recall metrikası əsasında digər üsullarla müqayisəsi [20]

Metod	Siniflər				
	NORM (%)	UNB (%)	MIS (%)	RUB (%)	SENS (%)
Ansambl yanaşması	97.82	97.51	76.00	48.29	95.65
KNN	97.50	89.50	60.00	33.50	87.00
KNN+	97.50	89.50	68.00	38.00	89.00
KNN+FS	97.50	90.50	71.00	35.50	89.50
KNN+EFS	98.00	93.00	81.00	34.50	91.00
Təklif edilən metod	**100**	**100**	**99.93**	**100**	**100**

Bu tədqiqatın nəticələri göstərir ki, təklif edilən dərin hibrid model avtomatik və eyni vaxtda zaman, tezlik və zaman-tezlik domenlərində nasazlıqlara həssas olan sensor siqnallarının xüsusiyyətlərini çıxara bilir. Buna görə də dərin neyron şəbəkələrdən istifadə etməklə təklif edilən hibrid model KFS avadanlığının nasazlığının diaqnostikasında tətbiq oluna bilər.

Beşinci fəsil KFS sistemlərinin kiber dayanıqlığının qiymətləndirilməsi metodlarının işlənməsinə həsr edilmişdir. Ən vacib vəzifə KFS sistemlərinin destruktiv məlumat təsirləri altında düzgün işləmə qabiliyyətini qorumaqdır. Bunun səbəbi belə sistemlərə kiberhücumların mənfi maliyyə nəticələrinə və ekoloji fəlakətlərə, eləcə də insan tələfatına səbəb ola bilər. Kibercinayətkarlar tez-tez ən zəif həlqəni – KFS sistemlərdə ən həssas funksional komponenti axtarır və hədəfləyirlər.

Ən həssas cihazlar sistemin kiber dayanıqlığına dair effektiv tədqiqatlar üçün yaxşı başlanğıc nöqtəsi ola bilər. Mövcud metodlar

KFS mühitində ümumi çoxmərhələli kiberhücumları hərtərəfli təhlil edə bilməz. Fəsil iki paraqrafdan ibarətdir.

Birinci paraqrafda Bayes kiberhücum qraf əsasında KFS sistemlərinin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metod təqdim edilmişdir. İntellektual cihazların və texnologiyaların müxtəlif sənaye sahələrində inteqrasiyası bütün texnoloji infrastrukturu əhəmiyyətli dərəcədə dəyişdi. KFS sensorlardan istifadə edərək ətraf mühiti tanıyır, məqsədinə uyğun qərarlar qəbul edir və aktuatorlardan istifadə edərək düzəldici tədbirlər həyata keçirir. İT və ƏT şəbəkələri arasında əlaqə KFS sistemlərinin modelləşdirilməsi zamanı vacibdir. İT və ƏT şəbəkələrinin yaxınlaşması artır ki, bu da KFS sistemlərinin daha səmərəli idarə edilməsinə və fəaliyyət göstərməsinə imkan verir. KFS komponentinin nasazlığı komponentlərin sayından və onların müxtəlifliyindən asılı olaraq sistemə təsir göstərir. Bu, sistem komponentlərinin zəifliklərinin kritikliyini ölçməyin zəruriliyini sübut edir. KFS sistemlərdə kritik təhlükəsizlik qüsurlarının vaxtında aşkarlanması riskləri və potensial təhlükələri aşkar etməyə imkan verir. Bu problemi həll etmək üçün təhlükə modelləri yaradılır. Onlar sistemin etibarlılığını təmin etmək üçün nəzərə alınmalı olan potensial zəifliklərı daha yaxşı başa düşməyə imkan verir.

KFS komponentlərinin funksional zəifliklərinin kritikliyini qiymətləndirmək üçün optimal həllin seçilməsi mürəkkəb prosesdir. Bu onunla bağlıdır ki, kiber dayanıqlıq prosesi çərçivəsində vahid yanaşmaya uyğun olaraq bütün zəifliklər müəyyən edilməli, təsnifləşdirilməli və kəmiyyətcə müəyyən edilməlidir. Son bir neçə il ərzində statistika KFS sistemlərdə kiberhücumların sayında artım olduğunu göstərir. Əksər hallarda kibercinayətkarların məqsədi nəzarət alt sistemi üzərində idarə etməkdir.

Bununla belə, bu problemi KFS komponentlərinin zəifliklərinin kritikliyini qiymətləndirməyə imkan verən Bayes kiberhücum qrafından (Bayesian attack graph, BAG) istifadə etməklə həll etmək olar. O, vacib amil olan zəifliklər arasındakı əlaqələr haqqında məlumat verir. BAG əməliyyat sistemlərindən və şəbəkə

protokollarından, KFS girişinə nəzarət qaydalarından, proqram təminatının identifikasiyasından və zəiflik məlumatından asılıdır.

Çoxmeyarlı qərar qəbuletmə metodları KFS komponentlərinin zəifliklərinin kritikliyini sıralamaq probleminin həllinə uyğun yanaşma kimi istifadə edilə bilər. Onlar qərar qəbul edənlərə müəyyən edilmiş meyarlar əsasında optimal alternativləri seçməkdə kömək edirlər.

KFS komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün Promethee II çoxmeyarlı qərar qəbuletmə metodundan istifadə etmək təklif olunur. Çoxmeyarlı analiz metodları arasında kifayət qədər sadə hesab olunur və tez-tez ekspertlər tərəfindən istifadə olunur. Metod kifayət qədər sabit nəticələr verir və hər bir kriteriyaya cavab verən alternativlərin ikili müqayisəsinə əsaslanır. Promethee II nəzərdən keçirilən sistemin ən kritik zəifliklərini təşkil etməyə və müəyyən etməyə imkan verir. Boşluqların ümumi qiymətləndirilməsi sistemi (Common Vulnerability Scoring System, CVSS) və Milli Zəiflik Məlumat Bazasından (National Vulnerability Database, NVD) istifadə etməklə ölçülür.

KFS komponentlərindəki zəifliklərdən istifadə edən potensial kiberhücum ssenarilərini göstərmək üçün kritik infrastruktur sektorlarından biri kimi təbii qazın nəqli nümunəsini nəzərdən keçirə bilər (Şəkil 10). Təbii qaz boru kəmərləri ilə kompressor stansiyaları ilə nəql olunur. Onlar qazı boru kəmərindən keçirən bir neçə qaz kompressorundan ibarətdir. Filtrləmə ayrıldıqdan sonra təbii qaz kompressor qurğusuna verilir. Kompressor mühərrikinin yağlama və soyutma sistemləri qaz axınının sürətini qorumaq və saxlamaq üçün xidmət edir.

Nəzərdən keçirilən KFS sistemlərinin ƏT sensorlara və aktuatorlara qoşulmuş proqramlaşdırıla bilən məntiq nəzarətçiləri (programmable logic controller, PLC) və uzaq terminal bloklarıdır (remote terminal units, RTU). Sensorlar siqnalları idarəedicilərə ötürür, onlar nəzarət etmə siqnallarını aktuatorlara göndərirlər. Proses operatorları idarəetmə sistemi ilə insan-maşın interfeysi (Human-Machine Interface, HMI) vasitəsilə qarşılıqlı əlaqə qurur.

Verilənlər arxivi proses parametrlərinin qiymətlərini saxlayır. Verilənlər serveri nəzarətçidən məlumat alır və onu digər kontrollerlərə və ya HMI-yə ötürür. İdarəetmə şəbəkəsi SCADA nəzarət və ölçmə vahidləri arasında təlimat və verilənləri ötürür. Mühəndislik iş stansiyaları korporativ şəbəkəyə və ya İnternetə qoşula bilər. Burada proqram təminatının işlənməsi alətləri quraşdırılır, onların köməyi ilə texniki mütəxəssis mərkəzləşdirilmiş şəkildə sistem konfiqurasiyasına dəyişiklik və əlavələr edə bilər. Təbii qazın nəqlində kompressor stansiyaları adətən ayrıca təhlükəsizlik sistemi ilə birləşdirilmiş paylanmış idarəetmə sistemindən istifadə etməklə idarə olunur. Stansiyalar mərkəzi SCADA (Supervisory Control and Data Acquisition system) WAN (Wide Area Network) sisteminə qoşulmuş RTU bloklar vasitəsilə uzaqdan idarə olunur.

Güman edilir ki, kiberhücumçunun məqsədi verilənlər arxivini və ya iş stansiyasını (Engineering Workstation, EWS) pozmaq ola bilər. Bunlar bir-biri ilə əlaqəli təbiətinə görə adətən əsas hədəflərdir. Təbii qazın nəqli sisteminə kiberhücumların üç ssenarisi araşdırılır (Şəkil 10):

• İdarəetmə vasitələrinin manipulyasiyası

Sistem konfiqurasiyasından asılı olaraq, WAN SCADA ilə qarşılıqlı əlaqə qura bilən kibercinayətkar sistem parametrlərini, faylları və ya kritik qiymətləri manipulyasiya etmək üçün CVE-2020-13500 və ya CVE-2022-29966-dan istifadə edə bilər. Onlar autentifikasiyadan yan keçmək və sonra kompressor stansiyaları ilə əlaqəli monitorinq qiymətlərini manipulyasiya etmək üçün CVE-2022-33139 boşlugundan istifadə edə bilərlər. Bu, operatorları yanlış həyəcan siqnalları ilə sıxışdırır və ya təbii qazın nəqlini pozmaq üçün axın təyinat nöqtələrini dəyişir.

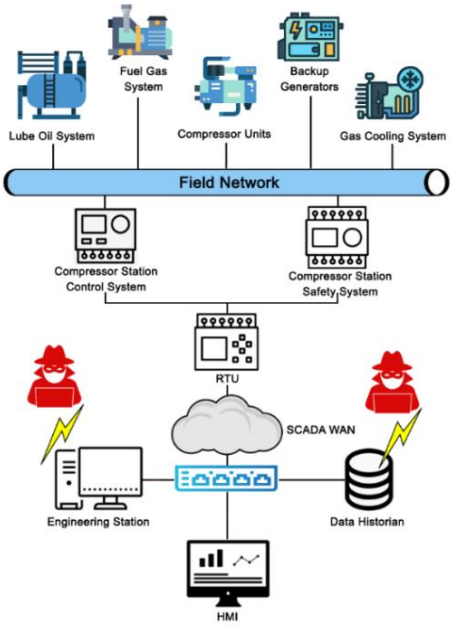
• Nəzarət uğursuzluğu

RTU ilə qarşılıqlı əlaqə qura bilən təcavüzkar autentifikasiyadan yan keçmək üçün CVE-2022-29961 və ya CVE-2022-29955 boşluqlarından istifadə edə bilər. Onlar prosesi dayandıran əmrlər yeridirlər. CVE-2022-30262 zəifliyi operatorların PLC1 və PLC2 kompressor stansiyalarını idarə etməsinə və monitorinqinə mane ola

bilər. Şəbəkə Dəyişdiricisi (network switcher, NS) ilə qarşılıqlı əlaqə qura bilən təcavüzkar təsdiqlənməmiş bağlantıdan (CVE-2021-30276 və ya CVE-2021-31886) istifadə edə və RTU-ya xüsusi əmrlər göndərə bilər. Bu, SCADA WAN və RTU arasındakı əlaqəni dayandıra və ya poza bilər, operatorların kompressor stansiyalarını izləməsinə və idarə etməsinə mane olur.

• Nəzarətin itirilməsi

Bunun üçün kibercinayətkar CVE-2022-30262, CVE-2022-26657, CVE-30315, CVE-2022-30260 və ya CVE-2022-31801 boşluqlarından istifadə edərək kompressor stansiyasının özünün idarəetmə sistemini sındırır. Bu, RTU bloklarda kodun icrasına və müxtəlif şəbəkə interfeysləri vasitəsilə məhdudiyyətsiz ünsiyyətə imkan verir.



Şəkil 10. KFS konfiqurasiyasının nümunəsi

CVE-2022-30313 və CVE-2022-30315 boşluqlarından istifadə təhlükəsizlik şəbəkəsinə nüfuz etməyə imkan verir. Bu yolla, kibercinayətkar yanğın və qaz təhlükəsizliyi fövqəladə hal sistemlərini söndürmək üçün parametrləri dəyişir və ya proqramlaşdırıla bilən məntiq nəzarətçi PLC2 proqramlaşdırıla bilən məntiq nəzarətçilərində kodun icrasına nail olur.

KFS ƏT domeninin cihazlarına təhlükə yarandıqdan sonra kibercinayətkarlar fiziki proseslərə təsir edən kiberhücumlar üçün müxtəlif CVSS-dan istifadə edə bilərlər.

Boşluqların haqqında məlumat NVD təsvirlərindən götürülüb. Kibercinayətkar zərərli kodu icra etmək üçün İnternetə KFS İT şəbəkəsindən istifadə edir.

Eksperimentləri həyata keçirmək üçün KFS komponentlərinin müxtəlif boşluqları haqqında məlumat, o cümlədən base score, impact score γ, exploitability subscore ε, attack vector, user interaction, privilege required və exploit complexity score nəzərə alınmışdır.

Təklif edilən metod TOPSIS (Technique for Order Preference by Similarity to Ideal Solution), VIKOR (VIseKriterijumska Optimizacija I Kompromisno Resenje) və ELECTRE (Elimination and Choice Translating Reality) kimi tanınmış çoxmeyarlı qərar qəbuletmə metodları ilə müqayisə edilmişdir (Cədvəl 10).

Cədvəl 10

Təklif edilən metodun məlum yanaşmalarla müqayisəsi

KFS komponenti	TOPSIS	VIKOR	ELECTRE	Təklif edilən metod
PLC_1	4	4	3	4
PLC_2	3	3	4	3
RTU	3	4	3	3
SW	1	1	1	1
DH	2	2	2	2
NS	1	1	1	1
HMI	1	1	1	1
EWS	1	1	1	1

Promethee II və TOPSIS metodlarından istifadə etməklə risk raqlaşdırmasının nəticələri oxşardır. Bundan əlavə, üçüncü və dördüncü mövqelərdə VIKOR və ELECTRE üsulları üçün iki fərqli həll variantı yerləşdirildi.

Yekun olaraq, Promethee II çoxmeyarlı qərar qəbuletmə metodu əsasında KFS komponentlərinin zəifliklərinin kritikliyini qiymətləndirmək üçün kəmiyyət metodu təklif edilmişdir. Bu, sistemin ən zəif komponentlərini ranqlaşdırma və müəyyən etməyə imkan verir. BAG onun komponentlərinin məlum boşluqları nəzərə alınmaqla KFS strukturu əsasında yaradılmışdır.

Nəticədə Promethee II-dən istifadə etməklə KFS sistemlərinin funksional komponentlərinin ən kritik zəifliklərini müəyyən etmək mümkün olub.

İkinci paraqraf Sugeno qeyri-səlis inteqralından istifadə edərək KFS risklərinin qiymətləndirilməsi metodunu təqdim edir. KFS sistemlərinin kiberhücumlardan qorunması kibertəhlükəsizlik risklərinin qiymətləndirilməsi metodlarını tələb edən ciddi problemdir. Hazırda KFS risklərinin təhlili və qiymətləndirilməsi metodlar üsullarını keyfiyyət və kəmiyyət metodlarına bölmək olar. Birincilər risklərin ehtimalını və potensial təsirini müəyyən etmək, həmçinin risklərin xarakterini aşkarlanmaq üçün ekspert qiymətləndirməsinə əsaslanır. Eyni zamanda, kəmiyyət riskinin təhlili risklərin ehtimalını və potensial təsirini hesablamaq üçün riyazi və statistik metodlardan istifadə edir.

Bununla belə, tədqiqatçılar risklərin təhlili və qiymətləndirilməsinin kəmiyyət metodlarına üstünlük verirlər, çünki onlar təhlükəsizlik resurslarının daha dəqiq optimallaşdırılmasına imkan verir.

Təklif olunan risklərin qiymətləndirilməsi metodologiyasının strukturuna sistemin modelləşdirilməsi, sistem komponentlərinin kritikliyinin müəyyən edilməsi və ranqlaşdırılması və risklərin qiymətləndirilməsi daxildir. Kiber-fiziki cihazlarını hədəf alan modelləşdirilmiş kiberhücum qrafı kiber riskin qiymətləndirilməsi üçün müxtəlif ölçmələr əldə etməyə imkan verir.

Kiber və fiziki mühitlərdən müxtəlif ölçmələr sistemin vəziyyətinin diaqnostikası üçün istifadə olunan vahid kəmiyyət qiymətləndirməsində birləşdirilir.

Sugeno qeyri-səlis inteqral əsasında sistem riskini hesablamaq üçün KFS sistemlərinin kiber və fiziki təbəqələrindəki komponentlərin zəiflik qiymətlərindən istifadə olunur. Əldə edilmiş qiymətlər əsasında KFS sistemlərinin ən kritik qovşaqları seçilir və mümkün kiberhücum yolları proqnozlaşdırılır.

Kiber hücum qrafı əsasında KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün onun qovşaqlarının kritikliyini müəyyən etmək lazımdır. Riskin qiymətləndirilməsi indeksləri sistemin kiberhücumlara nə dərəcədə həssas olduğunu ölçməyə və KFS komponentlərinin bir-birinə nisbətən yerini müəyyən etməyə imkan verir. Baxılan indekslər aşağıdakı iki əsas sahəni əhatə edir: (1) ƏT və (2) İT. Nəzərə alınan mühitlər (1) fiziki mühit və (2) kiber mühitdir.

İT və ƏT göstəriciləri arzuolunmaz hadisə baş verdikdə KFS sistemlərinin vəziyyətini proqnozlaşdırır. Məsələn, külək enerjisi sisteminin vəziyyətini nasazlıqlara görə təhlil etmək üçün operator əvvəlcə sistemin hər bir qovşağında açılma sürəti, nominal sürət, söndürmə sürəti və nominal güc kimi parametrləri bilməlidir. KFS sistemlərinin ayrı-ayrı komponentlərinin uğursuzluğu kibercinayətkar hücumlar nəticəsində müxtəlif parametrlərin nəzarətsiz kənarlaşmasına səbəb ola bilər ki, bu da son nəticədə sistemin məhvinə səbəb ola bilər.

Hücum qraf müxtəlif zəiflikləri əlaqələndirməyə imkan verir. O, sistemdəki hücum yollarını təmsil etmək üçün boşluqlar haqqında məlumat əsasında kiber-fiziki sistemlərinin qovşaqlarına potensial təhlükələri müəyyən edir. Əslində, CVSS, KFS sistemlərinin xüsusi qovşağında mövcud olan hər bir cihaz üçün zəiflikləri nəzərə alaraq kiberhücumun həyata keçirilməsinin mürəkkəbliyini qiymətləndirir. KFS sistemləri müxtəlif topoloji quruluşa malikdir. Hücum qrafının qovşaqlarının kritikliyini qiymətləndirmək üçün bəzi indeksləri nəzərdən keçirək. Bu indekslər bütün şəbəkə haqqında ətraflı məlumat verir.

Fərz edək ki, $G = (\mathcal{N}, \mathcal{E})$ - qrafdır, burada $\mathcal{N} = \{1, \dots, \mathrm{n}\}$ qovşaqlar (təpələr) çoxluğudur, $\mathcal{E}$ isə kənarlar çoxluğudur, $\mathcal{E} = \{(\mathrm{i}, \mathrm{j}) | \mathrm{i}, \mathrm{j} \in \mathcal{N}\}$. n şəbəkədəki qovşaqların ümumi sayıdır.

a) *Yaxınlıq mərkəzliyi (closeness centrality*). Bir qovşağın yaxınlıq mərkəzliyi bir qovşağın (i) bütün digər qovşaqlara nə qədər yaxın olduğunu ölçür. Bu, şəbəkədəki bir qovşaqdan digər qovşaqlara ən qısa yol uzunluğunun hesablanması ilə müəyyən edilir. Yüksək yaxınlıq mərkəzi olan qovşaqlar şəbəkənin digər qovşaqlarına daha çox təsir göstərir.

Tərif (yaxınlıq mərkəzliyi). i qovşaq üçün C_i^c yaxınlıq mərkəzliyi aşağıdakı kimi hesablanır:

$$C_i^c = \frac{n-1}{\sum_{\substack{j=1 \\ i \neq j}}^{n} d_{ij}}, \; i = 1, \dots, n, \tag{23}$$

burada $d_{ij} - i$ təpəsindən j təpəsinə ən qısa məsafədir. Qrafda i-ni j ilə birləşdirən bir neçə yol ola bilər, onların arasında d_{ij} ən qısa yoldur.

b) *Özi vektor mərkəzliyi* (*eigenvector centrality*) qrafının ən "nüfuzlu" təpəsi ilə onun qonşu təpələri arasında əlaqəni göstərir.

Tərif (öz vektor mərkəzliyi). i qovşaq üçün öz vektor mərkəzliyi E_i^c aşağıdakı kimi müəyyən edilir:

$$E_i^c = \frac{1}{\delta_{max}} \sum_{j=1}^{n} a_{ij} E_j^c, \; i = 1, \dots, n, \tag{24}$$

burada δ_{max} qonşuluq matrisinin ən böyük özəl qiymətini bildirir. Qonşuluq matrisi $n \times n$ ölçülü kvadrat matrisdir, $\mathbb{A} = \left\| a_{ij} \right\|_{i,j=1}^{n}$, onun elementləri aşağıdakı kimi müəyyən edilir: i qovşaq j qovşağına ilə əlaqəsi olduqda $a_{ij} = 1$, əks halda $a_{ij} = 0$.

c) *Aralıq mərkəzliyi (betweenness centrality)* qrafda müəyyən bir qovşaqdan keçən ən qısa yolların sayını ölçür. Bu qraf-nəzəri metrika bir qovşağın digər iki qovşaq arasında ən qısa yollarda "körpü" rolunu oynamasını ölçür. Şəbəkəni qraf-nəzəri modelə çevirərkən qovşağın aralıq mərkəzliyi (B_i^c) hücumun həmin qovşaqdan keçmə ehtimalını göstərir.

Tərif (aralıq mərkəzliyi). i qovşağının aralıq mərkəzliyi B_i^c aşağıdakı kimi müəyyən edilir:

$$B_i^c = \sum_{\substack{k,j=1 \\ k\neq j\neq i}}^{n} \frac{\sigma_{kj,i}}{\sigma_{kj}},\ i = 1, \dots, n, \qquad (25)$$

burada σ_{kj} – qovşaq k qovşağından j təyinat qovşağına qədər ən qısa yolların ümumi sayı, $\sigma_{kj,i}$ isə i-dən keçən k-dan j-ə qədər olan yolların sayıdır.

Ən qısa yollar qrafdakı hər bir təpə cütü arasındakı ən qısa yollara aiddir. Əgər bir təpə ən qısa yolların bir hissəsidirsə, o zaman o, yüksək kənar arasında mərkəzliyə malikdir.

d) *Katz mərkəzliyi* (*Katz centrality*) şəbəkə strukturu və şəbəkədəki qovşağın mövqeyini nəzərə alaraq qovşaq üçün əhəmiyyət kəsb edən qraf nəzəriyyəsi parametridir. Həmin yol vasitəsilə bağlanan qovşaqların sayını müəyyən edir və uzaq qovşaqların töhfəsi "cəzalandırılır".

Tərif (*Katz mərkəzliyi*). i qovşağının Katz mərkəzliyi K_i^c aşağıdakı kimi müəyyən edilir:

$$K_i^c = \sum_{q=1}^{\infty} \sum_{j=1}^{n} \beta^q (\mathbb{A}^q)_{ji},\ i = 1, \dots, n, \qquad (26)$$

burada $\beta \in (0,1)$ – zəifləmə əmsalı, yəni uzaq qovşaqların iştirak payıdır, $(\mathbb{A}^q)_{ji}$ isə i və j qovşaqları arasında q dərəcəli əlaqələrin ümumi sayıdır.

Bu indekslər müxtəlif topoloji quruluşa malik bütün KFS sistemlər haqqında ətraflı məlumat verir.

KFS risk qiymətləndirmə meyarlarının qiymətlərinin birləşməsi qeyri-səlis ölçülərə nisbətən müəyyən edilən qeyri-səlis inteqrallardan istifadə etməklə həyata keçirilir. Fərz edilir ki, qeyri-səlis ölçünün qiymətləri və bütün giriş parametrləri vahid intervalda dəyişir.

Tərif (qeyri-səlis ölçü). Tutaq ki, $N = \{1, \dots, n\}$ sonlu çoxluq və $\mu: 2^{\mathcal{N}} \to [0,1]$ funksiyası elə funksiya olsun ki, $\mu(\emptyset) = 0$ və $\mu(\mathcal{N}) = 1$ olsun. Əgər hər hansı A və B üçün $\subseteq B \subseteq \mathcal{N}$ və $\mu(A) \leq \mu(B)$ şərti ödənilirsə, o zaman qeyri-səlis μ çoxluğu qeyri-səlis ölçü adlanır.

Tərif (Sugeno λ-ölçü). Tutaq ki, $N = \{1, \dots, n\}$ sonlu çoxluq və $\lambda \in (-1, +\infty)$. Aşağıdakı şərtlər yerinə yetirildikdə $\mu: 2^{\mathcal{N}} \to [0,1]$ funksiyası Sugeno λ -ölçüsüdür:

$$\mu(\emptyset) = 0, \quad (27)$$

$$\mu(\mathcal{N}) = 1, \quad (28)$$

$$\mu(A) \leq \mu(B), \forall A, B \text{ belə ki, } A \subseteq B \subseteq \mathcal{N}, \quad (29)$$

$$\mu(A \cup B) = \mu(A) + \mu(B) + \lambda\, \mu(A)\, \mu(B), \forall A, B \subseteq \mathcal{N} \text{ c } A \cap B = \emptyset, \quad (30)$$

burada $\emptyset$ — boş çoxluqdur.

(27) və (28) tənlikləri müvafiq olaraq boş çoxluğun ölçülərini və bütün çoxluqların birləşməsini təmsil edir. Tənlik (29) monotonluğu təmsil edir. Tənlik (30) mümkün alt çoxluqları və alt çoxluqların birləşməsini təmsil edir.

Yenidən (30) tətbiq edilərək, hər $A \subseteq \mathcal{N}$ üçün $\mu(A)$ qiyməti aşağıdakı kimi hesablana bilər:

$$\mu(A) = \left[\frac{\prod_{i \in A}(1 + \lambda\mu(\{i\}))}{\lambda}\right]. \quad (31)$$

$\mu(\mathcal{N}) = 1$ (28) məhdudiyyətindən və (31) tətbiqindən istifadə edərək (32) ifadəsindən λ-nın qiymətini hesablamaq olar:

$$\lambda + 1 = \prod_{i=1}^{n}(1 + \lambda\mu_i), \quad (32)$$

burada $\mu_i = \mu(\{i\})$.

Tərif (diskret Sugeno inteqralı). Tutaq ki, $\mathcal{N}$-da μ qeyri-səlis ölçüsudur. $x = (x_1, x_2, \dots, x_n)$: $[0,1]^{\mathrm{n}} \to [0,1]$ funksiyasının μ-ə münasibətdə diskret Sugeno inteqralı aşağıdakı kimi müəyyən edilir:

$$SI_\mu(x) = \max_{1 \leq i \leq n}(min(x_{\pi(i)}, \mu(\{\pi(1), \pi(2), \dots, \pi(n)\}))) =$$

$$= \max_{1 \leq i \leq n}\{min\{x_{\pi(i)}, \mu(\{\pi(1)\})\}, \dots, min\{x_{\pi(n)}, \mu(\{\pi(1), \dots, \pi(n)\})\}\}, \quad (33)$$

burada π – $\mathcal{N}$ üzərində elə bir permutasiyadır $x_{\pi(1)} \leq \cdots \leq x_{\pi(n)}$.

Sugeno inteqralının əsas ideyası qeyri-səlis ölçülərdən istifadə etməklə hər bir modelin əhəmiyyətini qiymətləndirməyə imkan verən çəkili minimum və maksimuma əsaslanır. Sugeno qeyri-səlis inteqralı hədəf və proqnozlaşdırılan qiymətlər arasında ən yüksək oxşarlıq səviyyəsini müəyyən edir.

KFS risk qiymətləndirmə meyarlarının qiymətlərinin birləşməsi qeyri-səlis ölçülərə nisbətən müəyyən edilən qeyri-səlis inteqrallardan istifadə etməklə həyata keçirilir. Fərz edilir ki, qeyri-səlis ölçünün qiymətləri və bütün giriş parametrləri vahid intervalda dəyişir.

Tədqiqat kiberhücum yollarının risklərini qiymətləndirmək üçün Sugeno qeyri-səlis inteqralına əsaslanan metrikdən istifadə edir. Hücum qrafdakı hər bir qovşağın riski aşağıdakı kimi hesablanır:

$$Risk_i = Probability_i \times ImpactSI_i, i = 1, \dots, n, \quad (34)$$

burada $Probability_i$ – kiberhücum yollarının sayını göstərən və aşağıdakı kimi hesablanan i qovşaqlıqda daxilolma ehtimalıdır:

$$Probability_i = 1 - \prod_{j=1}^{n}(1 - P_j),\ i = 1, \dots, n, \quad (35)$$

burada P_j – j qovşağına kiberhücum ehtimalıdır.

Burada P_i kimi hesablanır

$$P_i = AV_i \times AC_i \times UI_i \times PR_i,\ i = 1, \dots, n, \quad (36)$$

burada AV_i – attack vector, AC_i – attack complexity, UI_i – user interaction, PR_i – privilege required.

Sugeno qeyri-səlis inteqral (SI) riskə məruz qalma B_i^c, C_i^c, E_i^c və K_i^c indekslərindən, eləcə də CVSS v3.1-dən əldə edilmiş bütövlük (I_i), əlçatanlıq (A_i) və məxfilik (C_i) xallarından istifadə etməklə hesablanır:

$$ImpactSI_i = SI(B_i^c, C_i^c, E_i^c, K_i^c, I_i, A_i, C_i),\ i = 1, \dots, n. \quad (37)$$

Yüksək $ImpactSI$ qiymətlərinə malik qovşaqlar KFS kiber-təhlükəsizliyi baxımından daha həssas hesab edilir. Bir neçə indeksə əsaslanan metrika sistemin hər bir qovşağını daha yaxşı xarakterizə edir.

Tək bir indeksdən fərqli olaraq, daha çox məlumatlandırıcıdır. Tələb olunan əmsallar hesablandıqdan sonra onlar çox kriteriyalı qərar təhlilindən istifadə etməklə birləşdirilir. Sugeno qeyri-səlis inteqralı KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün hücum yollarının risklərini qiymətləndirmək üçün istifadə olunur.

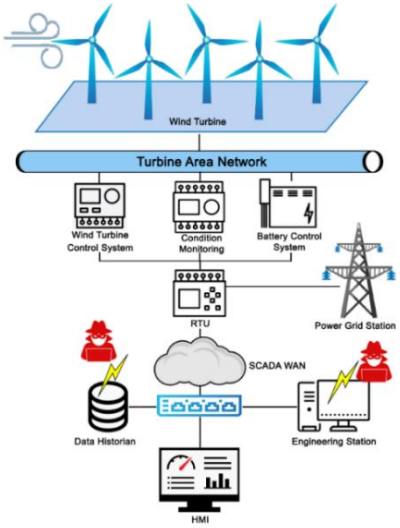
Dəyişən R0 təqdim edilir – bu eşikdən yuxarı riskə malik KFS qovşağın "qeyri-dayanıqlı" hesab edildiyi həddi qiyməti.

Praktikada bu qiymət təcrübəli mütəxəssislər tərəfindən müəyyən edilməlidir. Düyün "qeyri-dayanıqlıdır"sa, riski aradan qaldırmaq üçün dərhal təcili tədbirlər görülür. Risk R0-dan aşağı olarsa, node "dayanıqlı" sayılır və risk yoxdur. Bu halda, növbəti risk qiymətləndirməsi müəyyən fasilədən sonra həyata keçirilə bilər. Son

Risk qərarı sistemi kiber-fiziki təhlükəsizlik baxımından daha kiber dayanıqlı edir.

Nümunə olaraq külək enerjisi sistemi nəzərdən keçirilmişdir (Şəkil 11). Külək enerjisi kritik infrastruktur sektorlarından biridir. Külək turbinləri müxtəlif obyektlərdə geniş istifadə olunur: müəssisələrdə, təsərrüfatlarda, fərdi evlərdə və s.

Külək axınları turbininin qanadlarını döndərərək onu hərəkətə gətirir. Külək nə qədər güclü olarsa, o qədər çox enerji yaranır. Bu fırlanma turbini işə salır, o da dönməyə başlayır. Külək turbinləri külək enerjisini elektrik enerjisinə çevirən qurğulardır. Enerji, elektrik generatorunu idarə edən sürət qutusuna qoşulan rotor şaftı boyunca ötürülür. Turbin soyutma sistemindən, vəziyyətin monitorinqi sistemindən və hava qanadından ibarətdir. Onlar bıçaqların və rotorun mövqeyini təyin edən nəzarətçi üçün giriş məlumatları kimi xidmət edir. Akkumulyatorununn idarəetmə sistemi bir neçə batareya bankını izləyir, idarə edir və şəbəkənin sabitləşməsini təmin edir. Monitorinq zamanı alınan proses parametrlərinin qiymətləri verilənlər arxivində saxlanılır. HMI proses operatorları ilə idarəetmə sistemi arasında qarşılıqlı əlaqəni təmin edir (Cədvəl 11).



Şəkil 11. KFS sistemlərdə kiberhücum ssenarilərinin nümunələri

Mühəndislik iş stansiyaları mütəxəssisə korporativ şəbəkə və ya İnternet vasitəsilə sistem konfiqurasiyasına dəyişiklik və əlavələr etməyə imkan verən proqram inkişaf etdirmə vasitələrini ehtiva edir. RTU bağlantısı külək parkını mərkəzi SCADA sistemi ilə əlaqələndirir.

Cədvəl 11

Boşluqlar haqqında məlumatı

Təpə	Boşluq CVE-ID	*BS*	*IS*	*ζ*	*AV*	*C*	*I*	*A*	*UI*	*PR*	*AC*
1	CVE- 2021-41773	7.5	3.6	3.9	0.85	0.56	0	0	0.85	0.85	0.77
2	CVE-2022-22720	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
3	CVE-2022-30522	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
4	CVE-2014-7844	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.85	0.85	0.77
5	CVE-2019-9557	6.1	2.7	2.8	0.85	0.22	0.22	0	0.62	0.85	0.77
6	CVE-2020-2512	5.9	3.6	2.2	0.85	0	0	0.56	0.85	0.85	0.44
7	CVE-2020-24673	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
8	CVE-2020-6992	6.7	5.9	0.8	0.55	0.56	0.56	0.56	0.85	0.27	0.77
9	CVE-2021-27395	8.1	5.2	2.8	0.85	0	0.56	0.56	0.85	0.62	0.77
10	CVE-2020-3960	8.4	5.8	2.0	0.55	0.56	0	0.56	0.85	0.62	0.77
11	CVE-2021-22797	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.62	0.85	0.77
12	CVE-2019-14925	6.5	3.6	2.8	0.85	0.56	0	0	0.85	0.62	0.77
13	CVE-2019-9013	8.8	5.9	2.8	0.62	0.56	0.56	0.56	0.85	0.85	0.77
14	CVE-2022-1159	7.2	5.9	1.2	0.85	0.56	0.56	0.56	0.85	0.27	0.77
15	CVE-2020-7566	7.3	5.2	2.1	0.62	0.56	0.56	0	0.62	0.85	0.77
16	CVE-2018-5452	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
17	CVE-2023-0286	7.4	5.2	2.2	0.85	0.56	0	0.56	0.85	0.85	0.44

Fərz edək ki, kibercinayətkar KFS komponentlərinin boşluqlarından istifadə edib və aşağıdakı kiberhücum ssenarilərini həyata keçirib:

- *Manipulyasiya və nəzarətdən imtina.* SCADA serveri ilə qarşılıqlı əlaqə qura bilən kibercinayətkar sistem konfiqurasiyalarını, faylları və ya külək təsərrüfatı əməliyyatları ilə bağlı kritik qiymətləri manipulyasiya etmək üçün CVE-2019-14925 boşluqlarından istifadə edə bilər.

Boşluq istifadəçi adları, parollar və digər həssas məlumatlar da daxil olmaqla həssas məlumatlara icazəsiz girişə səbəb ola bilər.

Kibercinayətkar həmçinin məlumatların icazəsiz manipulyasiyasına və RTU əmrlərinin verilməsinə imkan verən bağlantıların autentifikasiya edilməməsi faktından sui-istifadə edə bilər (CVE-2021-27395). Bu, məntiqi tapşırıqların icrasını dayandıra, SCADA və RTU arasında əlaqəni poza bilər. Bu, operatorların kompressor stansiyalarını idarə etməsinə mane olardı.

- *Nəzarətin itirilməsi*. Etibarnamələri pozmaq və külək təsərrüfatı şəbəkəsinə giriş əldə etmək üçün kibercinayətkar RTU blokda kodu icra etmək üçün CVE-2019-9013, CVE-2022-1159 və CVE-2021-22797 boşluqlarından istifadə edir. Bu, ayrı-ayrı turbinlər üzərində nəzarəti ələ keçirməyə imkan verəcək. Kiberhücumçular CVE-2018-5452 boşluqdan istifadə edərək idarəetmə sisteminin daxili şəbəkəsinə daxil olaraq sistem konfiqurasiyası, əməliyyat parametrləri və nəzarətçi mikroproqramını manipulyasiya edə bilər (Cədvəl 11).

Bu, RTU blokda quraşdırılmış həddindən artıq sürətdən qorunma funksiyasını söndürə və yükü azalda bilər, nəticədə turbin bağlanır. Kibercinayətkar CVE-2020-7566-dan istifadə edərək verilənləri poza və təhlükə barədə erkən xəbərdarlıq təmin edən sağlamlıq monitorinq sistemlərini söndürə bilər.

Bundan əlavə, onlar proqramlaşdırıla bilən məntiq nəzarətçiləri PLC hədəfə ala, etimadnamələri pozmaq və proqramlaşdırıla bilən məntiq nəzarətçilərdə PLC icra kodu əldə etmək üçün CVE-2020-6992 boşluqdan istifadə edə bilərlər.

Bununla, kibercinayətkar batareya idarəetmə funksiyalarına təsir göstərərək sistemin dayanmasına səbəb ola bilər və KFS sistemlərinin potensial olaraq stabilləşdirə bilər.

Eksperimentlərin aparılması üçün sistemin hər bir i qovşağı üçün yaxınlıq mərkəzliyi C_i^c, öz vektor mərkəzliyi E_i^c, Katz mərkəzliyi K_i^c, aralıq mərkəzliyi B_i^c indekslərinin qiymətləri, həmçinin CVSS əsasında alınan bütövlük (I_i), mövcudluq (A_i), məxfilik (C_i) hesablanmışdır.

Bu, sistemin kritik qovşaqlarını müəyyən etməyə imkan verdi. İndekslərə "ekspert" çəkiləri təyin edildi. Çəki nə qədər yüksəkdirsə, indeksin "məlumatlılıq" o qədər yüksəkdir.

Cədvəl 11-də nəzərdən keçirilən KFS sistemlərinin bütün qovşaqları üçün indeks qiymətləri göstərilir. Bu qiymətlər təsir və ehtimal qiymətlərinə əsaslanaraq sistem cihazlarının kritikliyini qiymətləndirməyə imkan verir.

Təklif edilən yanaşma kriteriyalara uyğun olaraq boşluğun şiddətini qiymətləndirmək üçün seçilmişdir:

$$\mathrm{R} = \begin{cases} \text{critical}, & \mathrm{v} \in [5, 10] \\ \text{high}, & \mathrm{v} \in [3, 5) \\ \text{medium}, & \mathrm{v} \in [2, 3) \\ \text{low}, & \mathrm{v} \in [0, 2) \end{cases}. \quad (38)$$

Qrafının mümkün qovşaqlarının vəziyyətlərini dəyişdirmək məqsədi daşıyan müxtəlif hücum yolları nəzərdən keçirilmişdir.

Model kiber-fiziki şəbəkənin topologiyasını və zəifliklərini birləşdirir və təklif olunan metodun kiber dayanıqlığın qorunmasında effektivliyini təmin edir.

Mövcud yanaşmalardan fərqli olaraq, bu tədqiqat həm onun fiziki laylarına, həm də kiber laylarına təsir edən amilləri nəzərə alaraq, KFS sistemlərinin kiber dayanıqlığının kəmiyyətcə ölçülməsi ilə bağlı xüsusi problemi həll etmək məqsədi daşıyırdı.

Nəticədə dissertasiya işinin ən əhəmiyyətli nəticələri əks edilmiş, təklif edilmiş metod və alqoritmlərdən və alınmış nəticələrdən çıxan əsas müddəalar ifadə edilmişdir.

DİSSERTASİYA İŞİNİN ƏSAS NƏTİCƏLƏRİ

Dissertasiya işi çərçivəsində qarşıya qoyulmuş məsələlərin həllində əldə edilən əsas elmi-nəzəri və praktiki nəticələr aşağıdakılardır:

1. Mövcud metodların təhlili göstərdi ki, aşağıdakı problemlər KFS sistemlərinin kiber dayanıqlığını təmin etmək üçün aktualdır: böyük verilənlərin intellektual emalı üçün metod və alqoritmlərin işlənməsi; KFS sistemlərinin İT kibertəhlükəsizliyinin və ƏT şəbəkələrdən qorunmasının təmin edilməsi üçün metod və alqoritmlərin işlənməsi; KFS sistemlərinin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metodun və KFS risklərinin qiymətləndirilməsi metodunun işlənməsi. Tədqiqatın elmi probleminin qoyuluşu təqdim olunmuşdur. KFS sistemlərinin kiber dayanıqlığının təmin edilməsi üçün bir sıra problemlərin həlliyinə üç səviyyəli konseptual model işlənmişdir.
2. KFS sistemlərinin bloklanması riskini azaltmaq üçün k-means metodundan istifadə etməklə böyük verilənlərdə sıradançıxma aşkarlanması üçün klasterlərin kompaktlığı və ayrılması nəzərə alınmaqla klasterləşdirməyə əsaslanan alqoritmlər işlənmişdir.
3. Çəkili klasterləşmə əsasında KFS sistemlərinin böyük verilənlərinin təhlili üçün alqoritm işlənmişdir ki, verilənlər toplusundan hər bir nöqtənin çəkilərinin cəmlənməsi ilə alınan çəkilər klasterlərə təyin edilib və k-means alqoritmi ilə müqayisədə KFS sistemlərdə anomaliyaları daha dəqiq aşkarlayır.
4. KFS sistemlərinin uğursuzluq riskini azaltmaq üçün böyük verilənlərin paralel işlənməsi metodu hazırlanmışdır və müqayisədə klasterləşmə vaxtını əhəmiyyətli dərəcədə azaldıb.
5. Konsensus ansamblına əsaslanan KFS böyük verilənlərinin klaster analizi üçün kvadrat Evklid metrikasından istifadə etməklə metodu təklif edilmişdir.
6. Ekstremal maşın təlimindən və "atəşböcəyi" davranışının genetik alqoritmi istifadə edərək KFS sistemlərdə kiberhücumların təsnifatı üçün metod işlənmişdir.
7. Beş təsnifatçılardan ibarət ansamblından istifadə etməklə

KFS sistemlərdə DoS hücumlarının aşkarlanması üsulu işlənmişdir. Metod verilənlər bazasından hər bir nöqtə üçün alınan sinif etiketi bu nöqtə üçün təsnifat metodları ilə əldə edilən bütün qiymətləndirmələr arasında maksimum qiymətə uyğun gəlir [10, 12].

8. Dərin neyron şəbəkələrdən istifadə edərək təsvirlər əsasında KFS sistemlərdə zərərli proqramların aşkarlanması üçün alqoritm təklif edilmişdir.

9. Su təmizləmə sistemi üçün iyerarxik gizli Markov modelləri əsasında KFS sistemlərinin ƏT sahəsində anomaliyaların aşkarlanması metodu işlənmişdir.

10. Transfer təlimindən və ekstremal gradient gücləndirmə metodu istifadə edərək KFS akustik siqnallarında anomaliyaların aşkarlanması metodu işlənmişdir [26].

11. Su təmizləmə sistemi üçün dərin hibrid modeldən istifadə edərək KFS cihazlarına kiberhücumların aşkarlanması metodu təklif edilmişdir.

12. Neftə batan nasos üçün dərin neyron şəbəkələrindən istifadə edərək təsvirə əsaslanan KFS nasazlıqlarının təsnifatı üçün metodu işlənmişdir.

13. Təbii qazın boru kəməri ilə nəqli üçün Bayes hücum qrafı əsasında KFS sistemlərinin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metodu işlənmişdir.

14. Külək enerjisi istehsalı üçün qeyri-səlis Suqeno inteqralından istifadə edən KFS risklərin qiymətləndirilməsi metodu işlənmişdir.

Eksperimental tədqiqatlar zamanı alınmış nəticələr təklif edilmiş metodların üstünlüklərini göstərir və seçilmiş yanaşmaların perspektivli olduğunu sübut edir.

Dissertasiya işinin əsas nəticələri aşağıdakı elmi işlərdə dərc edilmişdir:

1. Imamverdiyev, Y.N., Sukhostat, L.V. Anomaly detection in network traffic using extreme learning machine // IEEE International Conference on Application of Information and Communication Technologies (AICT'2016). Baku, Azerbaijan, – 2016, – p. 418-421. (**WoS, Scopus**)
2. Имамвердиев, Я.Н., Сухостат, Л.В. Вопросы безопасности киберфизических систем // "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" üzrə III respublika elmi-praktiki konfransı. Сумгаит, Азербайджан, – 2016, – с. 257-259.
3. Имамвердиев, Я.Н., Сухостат, Л.В. Вопросы применения методов машинного обучения для решения проблем информационной безопасности // "Big data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı. Баку, Азербайджан, – 2016, – с. 127-131.
4. Алгулиев, Р.М. Киберфизические системы: основные понятия и вопросы обеспечения безопасности / Р.М.Алгулиев, Я.Н.Имамвердиев, Л.В.Сухостат // Информационные технологии, – 2017, 7, – с. 517–528. (**РИНЦ**)
5. Alguliyev, R.M. Anomaly Detection in Big Data based on Clustering / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // Statistics, Optimization and Information Computing, – 2017, 5 (4), – p. 325-340. (**Scopus**)
6. Имамвердиев, Я.Н. Обнаружение аномалий в сетевом трафике на основе информативных признаков / Я.Н.Имамвердиев, Л.В.Сухостат // Radio Electronics, Computer Science, Control, – 2017, 3, – с. 113-120. (**WoS**)
7. Alguliyev, R. An anomaly detection based on optimization / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // International Journal of Intelligent Systems and Applications, – 2017, 9 (12), – p. 87-96. (**Scopus)**
8. Алыгулиев, Р.М., Имамвердиев, Я.Н., Сухостат, Л.В. Оптимизационный подход к обнаружению аномалий в Big data // XIII Международная научно-техническая конференция «Распознавание-2017». Курск, Россия, – 2017, – с. 38-40. (**РИНЦ**)
9. Алгулиев, Р.М., Имамвердиев, Я.Н., Сухостат, Л.В. Обеспечение информационной безопасности киберфизических систем // "Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika konfransı. Баку, Азербайджан, – 2017, – с. 40-45.
10. Алгулиев Р.М., Алыгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Обнаружение DoS атак с применением ансамбля классификаторов // "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" III respublika elmi-praktiki konfransı. Баку, Азербайджан, – 2017, – с. 12-18.
11. Alguliyev, R. Cyber-physical systems and their security issues / R.Alguliyev, Y.Imamverdiyev, L.Sukhostat // Computers in Industry, – 2018, 100, – p. 212-223. (**Scopus, WoS, IF=4.769**)

12. Alguliyev, R.M. An improved ensemble approach for DoS attacks detection / R.M.Alguliyev, R.M.Aliguliyev, Y.N.Imamverdiyev [et al.] // Radio Electronics, Computer Science, Control, – 2018, 2 (45), – p. 73-82. (**WoS**)
13. Alguliyev, R. Weighted clustering for anomaly detection in big data / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // Statistics, Optimization & Information Computing, – 2018, 6 (2), – p. 178–188. (**Scopus**)
14. Alguliyev, R.M., Aliguliyev, R.M., Sukhostat, L.V. Purity-based consensus clustering for anomaly detection in Big data // XIV Internatıonal scientific conference "Recognition - 2018". Kursk, Russia, – 2018, – p. 17-20. (**РИНЦ**)
15. Сухостат, Л.В. Обнаружение атак на киберфизические системы на основе глубокого обучения // "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı. Баку, Азербайджан, – 2018, – с. 42-46.
16. Alguliyev, R.M., Aliguliyev, R.M., Sukhostat, L.V. Consensus clustering by weight optimization of input partitions // IEEE 13th International Conference "Application of Information and Communication Technologies (AICT'2019). Baku, Azerbaijan, – 2019, – p. 1-4. (**WoS, Scopus**)
17. Алгулиев, Р.М., Имамвердиев, Я.Н., Шыхалиев, Р.Г., Сухостат, Л.В. Об одном подходе по выявлению кибератак на киберфизические системы с применением глубокой гибридной модели // The First International Scientific and Practical Forum «GLOBAL CYBER SECURITY FORUM 2019». Харьков, Украина, – 2019, – с. 27-28.
18. Alguliyev, R.M., Imamverdiyev, Y.N., Sukhostat, L.V. Detection of cyber-attacks on cyber-physical systems using deep neural network. XV International scientific conference "Recognition - 2019". Kursk, Russia, – 2019, – p. 18-20.
19. Сухостат, Л.В. Вопросы защиты персональных данных в киберфизических системах // "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı. Баку, Азербайджан, – 2019, – с. 92-96.
20. Alguliyev, R.M. Intelligent diagnosis of petroleum equipment faults using a deep hybrid model / R.M.Alguliyev, Y.N.Imamverdiyev, L.V.Sukhostat // SN Applied Sciences, – 2020, 2 (5), – p. 1-16. (**WoS, Scopus)**
21. Alguliyev, R.M. Efficient algorithm for big data clustering on single machine / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // CAAI Transactions on Intelligence Technology, – 2020, 5 (1), – p. 9-14. **(WoS, Scopus)**
22. Alguliyev, R.M. Weighted Consensus Clustering and its Application to Big Data / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Expert Systems with Applications, – 2020, 150, – p. 1-15. (**Scopus, WoS, IF=6.954)**
23. Alguliyev, R.M., Imamverdiyev, Y.N., Sukhostat, L.V. Diagnostics of DoS attacks on cyber-physical systems based on hierarchical hidden Markov models // XIII International Conference for young researchers "TECHNICAL SCIENCES. INDUSTRIAL MANAGEMENT". Borovets, Bulgaria, – 2020, – p. 39-41.

24. Alguliyev, R.M. Parallel batch k-means for big data clustering / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Computers and Industrial Engineering, – 2021, 152, – p. 1-11. **(Scopus, WoS, IF=7.180)**
25. Alguliyev, R.M. Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems / R.M.Alguliyev, Y.N.Imamverdiyev, L.V.Sukhostat // Neural Computing and Applications, – 2021, 33 (16), – p. 10211-10226. (**Scopus, WoS, IF=5.102**)
26. Sukhostat, L.V. An intelligent model based on deep transfer learning for detecting anomalies in cyber-physical systems / L.V.Sukhostat // Radio Electronics, Computer Science, Control, – 2021, 3, – p. 124-132. (**WoS**)
27. Сухостат, Л.В. Об одном подходе по обнаружения аномалий в киберфизических системах на основе акустических сигналов // 1st International Conference on "Information security: problems and prospects". Баку, Азербайджан, – 2021, – с. 115-118.
28. Сухостат, Л.В. Обзор некоторых решений безопасности современных АСУ ТП / Л.В.Сухостат // Телекоммуникации, – 2022, 2, – с. 14-23. (**РИНЦ**)
29. Sukhostat, L.V. Anomaly detection in industrial control system based on the hierarchical hidden Markov model / Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security (IOS Press), – 2022, 62, – p. 48-55.
30. Алгулиев, Р.М., Алыгулиев, Р.М., Сухостат, Л.В. Оценка критичности киберфизических систем на основе графа атак // XVII International scientific conference "Recognition - 2023". Курск, Россия, – 2023, – с. 52-54. (**РИНЦ**)
31. Alguliyev, R. Radon transform based malware classification in cyber-physical system using deep learning / R.Alguliyev, R.Aliguliyev, L.Sukhostat // Results in Control and Optimization, – 2024, 14, – p. 1-14. (**Scopus, WoS, IF=3.2**)
32. Alguliyev, R.M. Method for Quantitative Risk Assessment of Cyber-Physical Systems based on Vulnerability Analysis / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Kybernetika, – 2024, 60 (6), – p. 779-796. (**Scopus, WoS, IF=2.2**)
33. Alguliyev, R. An approach for assessing the functional vulnerabilities criticality of CPS components / R.Alguliyev, R.Aliguliyev, L.Sukhostat // Cyber Security and Applications, – 2025, 3, – p. 1-7. (**Scopus**)

Həmmüəlliflərlə dərc olunmuş işlərdə iddiaçının şəxsi rolu:

[2-4,9,11] – KFS-nin kiber dayanıqlığinin və informasiya təhlükəsizliyinin təmin edilməsi metod və alqoritmlərinin təhlili aparılmışdır;

[21,24] – KFS-nin nasazlıq riskini azaltmaq üçün böyük verilənlərin paralel işlənməsi metodları təklif edilmişdir;

[13] – çəkili klasterləşdirmə əsasında KFS-nin böyük verilənlərinin təhlili üçün alqoritmi təklif edilmişdir;

[5,7,8] – KFS-nin bloklanması riskini azaltmaq üçün k-means metoduna əsaslanan böyük verilənlərdə kənar göstəriciləri aşkarlanmaq üçün alqoritmləri təklif edilmişdir;

[14,16,22] – konsensus ansamblına əsaslanan böyük KFS verilənlərinin klaster analizi metodu təklif edilmişdir;

[1,6] – ekstremal maşın təlimindən istifadə edərək KFS-də kiberhücumların təsnifatı üçün metodu təklif edilmişdir;

[10,12] – təsnifatçılar ansamblından istifadə edərək KFS-də DoS hücumlarının aşkarlanması metodu təklif edilmişdir;

[31] – təsvirlər əsasında KFS-da zərərli proqramların aşkarlanması üçün alqoritmi təklif edilmişdir;

[23] – iyerarxik gizli Markov modellərinə əsaslanan KFS-də ƏT anomaliyaların aşkarlanması metodu təklif edilmişdir;

[17,18,25] – dərin hibrid modeldən istifadə edərək KFS cihazlarına hücumların aşkarlanması metodu təklif edilmişdir;

[20] – təsvirlər əsasında KFS nasazlıqlarını təsnif etmək üçün metodu təklif edilmişdir;

[30,33] – Bayes hücum qrafı əsasında KFS-nin funksional komponentlərinin zəifliklərinin kritikliyini müəyyən etmək üçün metodu təklif edilmişdir;

[32] – qeyri-səlis Sugeno inteqralından istifadə edərək KFS risklərinin qiymətləndirilməsi üçün metodu təklif edilmişdir.

Dissertasiyanın müdafiəsi 31 oktyabr 2025-ci il tarixində saat 10^{00}-da Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun nəzdindəki ED 1.35 Dissertasiya Şurasının iclasında keçiriləcək.

Ünvan: Az1141, Bakı şəhəri, B.Vahabzadə küçəsi, 9A.

Dissertasiya ilə Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Azərbaycan Respublikası Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun rəsmi internet saytında (*ict.az*) yerləşdirilmişdir.

Avtoreferat 29 sentyabr 2025-ci il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb: 27.09.2025

Kağızın formatı: 60x84 1/16

Həcm: 76140 (işarə)

Tiraj: 30