AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ MODELLƏRİ VƏ METODLARI

İxtisas: 3338.01 – Sistemli analiz, idarəetmə və informasiyanın işlənməsi

Elm sahəsi: Texnika elmləri

İddiaçı: **Yadigar Nəsib oğlu İmamverdiyev**

Elmlər doktoru elmi dərəcəsi

almaq üçün təqdim edilmiş dissertasiyanın

AVTOREFERATI

Bakı - 2021

Dissertasiya işi Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunda yerinə yetirilmişdir.

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

Rəsmi oppenentlər: texnika elmləri doktoru, professor
Nadir Bafadin oğlu Ağayev

texnika elmləri doktoru, dosent
Lalə Mehdi qızı Zeynalova

texnika elmləri doktoru, professor
Ramin Rza oğlu Rzayev

texnika elmləri doktoru, professor
Cavanşir Firudin oğlu Məmmədov

Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunun nəzdində fəaliyyət göstərən
ED 1.35 Dissertasiya şurası

Dissertasiya şurasının sədri:

AMEA-nın həqiqi üzvü,
texnika elmləri doktoru, prof.
Rasim Məhəmməd oğlu Əliquliyev

Dissertasiya şurasının elmi katibi:

texnika üzrə fəlsəfə doktoru, dosent
Fərhad Firudin oğlu Yusifov

Elmi seminarın sədri:

texnika elmləri doktoru
Mütəllim Mirzəəhməd oğlu Mütəllimov

İŞİN ÜMUMİ XARAKTERİSTİKASI

İşin aktuallığı. Hazırda informasiya və kommunikasiya texnologiyaları (İKT) cəmiyyətin bütün sahələrinə geniş nüfuz etməkdədir. Bunun nəticəsində bəşəriyyət yeni inkişaf mərhələsinə – informasiya cəmiyyətinin formalaşması dövrünə qədəm qoyur. Cəmiyyətin idarə olunması proseslərini optimallaşdırmaq məqsədi ilə dövlət və yerli özünüidarəetmə orqanlarında İKT-nin geniş tətbiqi informasiya cəmiyyətinin formalaşmasında mühüm mərhələ olan e-dövlətin qurulmasına şərait yaradır. E-dövlətdə vətəndaşlar dövlət siyasətinin formalaşdırılması və reallaşdırmasına daha geniş cəlb edilir, dövlət, özəl sektor və vətəndaş cəmiyyəti arasında qarşılıqlı təsirin və əməkdaşlığın effektiv sistemi qurulur, dövlət idarəçiliyinin səmərəliliyi və göstərilən xidmətlərin keyfiyyəti yüksəlir. Qeyd edək ki, e-dövlət təkcə e-hökumətdə deyil, dövlət hakimiyyətinin bütün qollarında və bütövlükdə, cəmiyyət həyatının bütün sahələrində informasiya və kommunikasiya texnologiyalarını İKT-nin geniş istifadəsini nəzərdə tutur. Həmçinin e-dövlətin əsas vəzifələrindən biri elektron məkanda da dövlət suverenliyini həyata keçirməkdir.

Lakin e-dövlət quruculuğu sahəsində öz həllini gözləyən bir sıra ciddi problemlər də vardır, ən əsas və ən çətin məsələlərdən biri yeni şəraitdə fəaliyyət göstərən dövlətin informasiya təhlükəsizliyinin etibarlı təmin edilməsidir. İnformasiya təhlükəsizliyi e-dövlətin effektivliyinə və vətəndaşların dövlətə inamına birbaşa və həlledici təsir edir.

İKT-nin geniş tətbiqi bəşəriyyətin inkişafını sürətləndirməklə yanaşı milli, regional və qlobal təhlükəsizliyə yeni təhdidlər də yaradır.

Dövlətlərarası ziddiyyətlər və münaqişələr kiberfəzaya keçir və ölkələr bu fəzada informasiya müharibəsi əməliyyatlarının aparılması ilə peşəkar şəkildə məşğul olan kiberqoşunlar formalaşdırır[1].

İnformasiya fəzası transmilli, qlobal xarakter daşıyır və milli səviyyədə nəzarətdən çıxır. Kütləvi informasiya vasitələrinin (KİV) beynəlxalq inhisara alınması və ictimai şüurla manipulyasiya edilməsi

[1] İmamverdiyev, Y. N. Kiberqoşunlar: funksiyaları, silahları və kadr potensialı // – Bakı: İnformasiya cəmiyyəti problemləri, – 2015. №2, – s. 15-25.

də güclənir. Fərdi məlumatların cinayətkar məqsədlər üçün toplanması geniş vüsət alır, mütəşəkkil kibercinayətkarlıq inkişaf edir.

Əşyaların İnterneti, sənaye İnterneti, xidmətlərin İnterneti və süni intellekt sayəsində Industry 4.0 inqilabı baş verir və yeni imkanlar və təhdidlər gətirən kiber-fiziki-sosial sistemlər formalaşır.

Beynəlxalq təhlükəsizlik təhdidlərinin transformasiyası ilə əlaqədar yeni müharibə konsepsiyaları – "asimmetrik müharibə", "şəbəkə müharibəsi" və "dövlətsiz müharibə" konsepsiyaları meydana çıxır. Asimmetrik aktorlara qarşı tamamilə yeni mübarizə strategiyaları tələb edilir.

Milli informasiya infrastrukturunun kritik elementlərinə olan kiberhücumlar daha mürəkkəb, məqsədyönlü və genişmiqyaslı olur və tez-tez baş verir. Eyni zamanda, dövlət orqanlarına və siyasi aktorlara qarşı siyasi motivli hücumlar da artır. Belə hücumların qarşısının uğurla alınması ayrı-ayrı təşkilatların və insanların gücü xaricindədir, özəl sektor və vətəndaş cəmiyyəti də daxil olmaqla bütün maraqlı tərəflərin arasında sıx əməkdaşlıq tələb edilir.

Beləliklə, hərtərəfli qloballaşma və onun gətirdiyi təhdidlər mühitində, ictimai proseslərə artan kibertəhlükəsizlik riskləri və qeyri-müəyyənliklər şəraitində informasiya təhlükəsizliyi e-dövlətin özünü qorumasının əsas funksiyalarından biri olur. Buna görə e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi sisteminin idarə edilməsi aktual məsələdir.

Qlobal informasiya cəmiyyəti şəraitində e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi problemi beynəlxalq, kompleks və multidissiplinar xarakter kəsb edir və onun həlli müvafiq elmi-metodoloji bazanın inkişaf səviyyəsindən birbaşa asılı olur.

Ölkədə informasiya cəmiyyətinin və e-dövlətin qurulması, informasiya təhlükəsizliyinin etibarlı təmin edilməsi Azərbaycan Respublikasında dövlət siyasətinin prioritet istiqamətlərindən biridir. Ölkəmizdə informasiya təhlükəsizliyi sahəsində dövlət siyasətinin həyata keçirilməsi istiqamətində normativ və hüquqi bazanın təkmilləşdirilməsi, informasiya təhlükəsizliyi sisteminin təşkilati strukturunun formalaşdırılması, informasiya təhlükəsizliyi siyasətinin işlənməsi, informasiya təhlükəsizliyi sahəsində kadr hazırlığı, elmi

tədqiqat işləri üzrə bir sıra tədbirlər sistemli şəkildə müvafiq dövlət qurumları tərəfindən həyata keçirilməkdədir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə elmi və praktiki tədqiqatlar nisbətən yaxın dövrlərdə meydana çıxmışdır. Eyni zamanda, e-dövlətin informasiya təhlükəsizliyi mühiti çox dinamik dəyişir, təhlükəsizliyə təhdidlər daim evolyusiya edir və kiberhücum və müdafiə mexanizmləri yenilənir. Meydana çıxan yeni informasiya təhlükəsizliyi çağırışlarına operativ cavab verilməsi informasiya təhlükəsizliyinin idarə edilməsinin təkmilləşdirilməsini, yeni idarəetmə modellərinin və metodlarının işlənməsini tələb edir.

Yuxarıda qeyd edilənlərdən çıxış edərək bu dissertasiya işi e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin elmi-metodoloji əsaslarının işlənməsi məsələlərinə həsr edilmişdir.

İşin məqsədi və məsələləri. Dissertasiya işinin məqsədi e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin elmi-nəzəri və metodoloji əsaslarının inkişafı və təkmilləşdirilməsi üçün modellərin və metodların işlənməsidir.

Dissertasiya işində qarşıya qoyulmuş məqsədə çatmaq üçün aşağıdakı **məsələlər** tədqiq edilmişdir:

- e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modelinin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinə strateji təhdidlərin və kritik risklərin qiymətləndirilməsi metodlarının işlənməsi;
- e-dövlətin biometrik identifikasiya sisteminin təkmilləşdirilməsi üçün metodların işlənməsi;
- informasiya təhlükəsizliyi insidentlərinin aşkarlanması və effektiv idarə edilməsi üzrə metodların işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin təmin edilməsinə cəlb edilmiş dövlət, qeyri-dövlət və beynəlxalq aktorlar arasında kooordinasiya modellərinin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin müxtəlif səviyyələrində qərarların qəbul edilməsi modellərinin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün metod və modellərin işlənməsi.

Tədqiqat metodları. Qoyulmuş məsələlərin həlli üçün idarəetmə nəzəriyyəsi, qərar qəbuletmə nəzəriyyəsi, qeyri-səlis idarəetmə

nəzəriyyəsi, oyunlar nəzəriyyəsi, ehtimal nəzəriyyəsi və riyazi statistika, kombinator optimallaşdırma, qraflar nəzəriyyəsi, sosial şəbəkə analizi, maşın təlimi metodları istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar:

- e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli;
- e-dövlətdə informasiya sahəsində milli maraqlara təhdidlərin konsensus ranqlaşdırılması metodu;
- e-dövlət infrastukturunda kritik risklərin qiymətləndirilməsi metodu;
- milli İnternet infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri;
- biometrik sistemlərin tanıma göstəricilərinin və təhlükəsizliyinin təkmilləşdirilməsi və biometrik kriptosistemlərin sintezi metodları;
- DDoS hücumların dərin təlim yanaşması əsasında aşkarlanması metodu;
- informasiya təhlükəsizliyi insidentlərinin emalı üzrə optimal planlaşdırma metodu;
- e-dövlətin informasiya təhlükəsizliyi sahəsində koordinasiya modelləri;
- e-dövlətin informasiya təhlükəsizliyinin strateji, taktiki və operativ idarə edilməsi modelləri;
- e-dövlətin informasiya təhlükəsizliyinin qiymətləndirilməsi metodları və modelləri.

Elmi yeniliklər. Dissertasiya işində aparılmış tədqiqatların və alınmış nəticələrin elmi yenilikləri aşağıdakılardan ibarətdir:

- siyasi və intellektual elitanı təmsil edən ekspertlərin qiymətləndirmələri əsasında informasiya sahəsində milli maraqlara təhdidlərin konsensus ranqlaşdırılması modelinin işlənməsi;
- e-dövlətin qarşılıqlı asılı informasiya infrastrukturlarında risklərin və İnternetin milli infrastrukturunun dayanıqlığının qiymətləndirilməsi metodlarının və modellərinin işlənməsi;
- e-dövlətin biometrik autentifikasiya sisteminin təkmilləşdirilməsi üçün metodların və biometrik kriptosistemlərin sintezi üçün yanaşmaların işlənməsi;

- InT insidentlərinin aşkarlanması, çoxmeyarlı prioritetləşdirilməsi və emalının optimal planlaşdırılması üçün metodların və alqoritmlərin işlənməsi;
- e-dövlətin InT-nin ikisəviyyəli iyerarxik idarəetmə sistemində investisiyaların koordinasiyası modelinin işlənməsi;
- InT sahəsində beynəlxalq koalisiyaların formalaşdırılması modelinin işlənməsi;
- e-dövlətin InT-nin strateji, taktiki və operativ səviyyələrdə idarə edilməsi üçün riyazi və konseptual modellərin işlənməsi;
- e-dövlətin InT-nin birbaşa (e-xidmətlər) və əks-əlaqələr (vətəndaş etimadı) üzrə qiymətləndirilməsi modellərinin işlənməsi.

İşin praktiki əhəmiyyəti. İşin praktiki əhəmiyyəti alınmış elmi-nəzəri nəticələrin aşağıdakı sahələrdə istifadə oluna bilmələri ilə şərtlənir:

- milli informasiya təhlükəsizliyi siyasəti, strategiyası və proqramları üzrə təkliflərin işlənməsi;
- informasiya təhlükəsizliyi üzrə strateji qərarların qəbulunu intellektual dəstəkləmə sistemlərində;
- kiberhücumların aşkarlanması sistemlərində;
- informasiya təhlükəsizliyinin real zamanda idarə edilməsini həyata keçirən situasiya mərkəzlərində;
- milli biometrik eyniləşdirmə sistemində;
- informasiya təhlükəsizliyi üzrə idarələrarası koordinasiya mərkəzlərində.

İşin nəticələrinin reallaşdırılması və tətbiqi. Əsas nəticələr Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı, Azərbaycan Milli Elmlər Akademiyası (AMEA) fundamental tədqiqatlar çərçivəsində "Elektron dövlətin yaradılması, idarə olunması və informasiya təhlükəsizliyinin elmi-nəzəri əsaslarının işlənməsi" mövzusu üzrə, ABŞ Mülki Tədqiqatlar və İnkişaf Fondunun "Biometrik sistemlərin təhlükəsizliyinin test edilməsi" qrant layihəsi üzrə, Koreya Milli Elm Fondunun dəstəklədiyi "Biometrik kriptosistemin yaradılması" qrant layihəsi üzrə, Azərbaycan Respublikası Prezidenti yanında Elmin İnkişafı Fondunun

maliyyələşdirdiyi “Səsə görə şəxsin biometrik tanınması üçün robast yanaşmaların işlənməsi”, “Böyük verilənlər ("Big Data") mühitində informasiya təhlükəsizliyinin təmin olunması metodları və alqoritmlərinin işlənilməsi və onların bəzi tətbiqləri” mövzuları üzrə elmi-tədqiqat işlərinin yerinə yetirilməsi gedişində əldə edilmişdir.

Dissertasiya işinin əsas nəzəri və praktiki nəticələri AMEA-nın AzScienceNet elmi kompüter şəbəkəsinin təhlükəsizlik sistemlərinin layihələndirilməsi və istismarı zamanı istifadə edilmişdir.

Tədqiqat işinin aprobasiyası. İşin əsas elmi-nəzəri və praktiki nəticələri aşağıdakı konfranslarda məruzə edilmiş və müzakirə olunmuşdur:

- 1-, 2-, 3-cü Beynəlxalq konfrans “Kibernetika və informatika problemləri”, Bakı, 2006, 2008, 2010;
- The 6th International Conference on Information Security and Cryptology (ISCTurkey), 2013;
- İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, Bakı, 2015;
- IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, 2009, 2013, 2016;
- II Міжнародна науково-практична конференція "Інформаційна безпека та комп’ютерні технології", Київ, 2017;
- İnformasiya təhlükəsizliyi üzrə III respublika elmi-praktiki seminarı, Bakı, 2017.

Elmi nəşrlər. Dissertasiyanın nəticələri üzrə 33 elmi iş, o cümlədən nüfuzlu elmi-praktiki jurnallarda 22 məqalə, beynəlxalq və respublika səviyyəli konfranslarda 11 məruzə çap olunmuşdur.

İşin strukturu və həcmi. Dissertasiya girişdən, yeddi fəsildən, nəticədən, 313 adda ədəbiyyat siyahısından və əlavələrdən ibarətdir. İşin əsas məzmunu 40 şəkil və 45 cədvəl daxil olmaqla 246 səhifədə şərh edilmişdir.

İŞİN MƏZMUNU

Girişdə dissertasiya işinin mövzusunun aktuallığı əsaslandırılmış, tədqiqatın məqsədi və həll olunacaq məsələlər müəyyən edilmiş, əldə edilmiş nəticələrin elmi yeniliyi və praktiki əhəmiyyəti göstərilmişdir.

Birinci fəsil e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin elmi-nəzəri problemlərinin analizinə və tədqiqinə həsr edilmişdir. Ümumiyyətlə, informasiya təhlükəsizliyinin idarə edilməsi dedikdə, informasiya təhlükəsizliyinin təmin edilməsi proseslərinin idarə edilməsi nəzərdə tutulur. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi çətin formallaşdırılan məsələlər sinfinə aiddir: idarəetmə obyekti hər biri məqsədyönlü fəaliyyət göstərən avtonom komponentlərdən ibarət mürəkkəb sosio-texniki sistemdir və burada bir-birinə əhəmiyyətli dərəcədə qarşılıqı təsir göstərən bir çox proses (siyasi, hüquqi, sosial, texnoloji və s.) baş verir, onlar arasında olduqca mürəkkəb səbəb-nəticə əlaqələri mövcuddur. Proseslərin xarakteri zamana görə dinamik dəyişir və bu dinamika haqqında kifayət qədər kəmiyyət informasiyası yoxdur, qeyri-müəyyənliyin müxtəlif növləri iştirak edir və s.

Çətin formallaşdırılan belə mürəkkəb məsələlərin həllində ilkin mərhələ kimi konseptual modelin qurulması çox faydalıdır. Bu məqsədlə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin məqsədlərini, əsas idarəetmə funksiyalarını və idarəetmə sisteminin arxitekturasını müəyyən edən konseptual model təklif edilmişdir [6, 9]. Dissertasiya işində əsas idarəetmə funksiyaları kimi təhdidlərin və risklərin identifikasiyası və qiymətləndirilməsi, e-xidmət istifadəçilərinin autentifikasiyası, informasiya təhlükəsizliyinin monitorinqi və insidentlərin emalı, informasiya təhlükəsizliyi üzrə fəaliyyətin koordinasiyası, idarəetmə qərarlarının qəbul edilməsi və informasiya təhlükəsizliyi səviyyəsinin qiymətləndirilməsi seçilmişdir.

Daha sonra, bu konseptual modelə uyğun olaraq, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin əsas funksiyaları üzrə aktual elmi-tədqiqat problemləri müəyyən edilmiş və onların müasir vəziyyəti analiz edilmişdir [8].

Nəhayət, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə dissertasiya işində baxılacaq elmi-tədqiqatların prioritet istiqamətləri müəyyən edilmişdir.

İkinci fəsildə e-dövlətin informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodları və modelləri işlənmişdir.

E-dövlətin informasiya təhlükəsizliyinə yönəlmiş strateji risklər informasiya sahəsində milli maraqları hədəfə alır. İnformasiya

sahəsində milli maraqlara çoxsaylı təhdidlər mövcuddur və kiber-müdafiəyə ayrılan resursların məhdudluğu şəraitində bu təhdidlərə qarşı effektiv əks-tədbirlər görmək üçün bu təhdidlərin çoxkriteriyalı konsensus ranqlaşdırılması zəruridir [21, 28].

Fərz edək ki, n sayda A_i $(i = 1,2, \dots, n)$ milli kibertəhlükəsizlik təhdidlərinin siyahısı tərtib edilib (rəsmi sənədlərin, elmi tədqiqatların, ekspertlərin rəyləri və KİV-də olan məlumatların əsasında). Tutaq ki, p sayda DM_k $(k = 1,2, \dots, p)$ ekspert seçilmişdir və ekspertlərin hər biri təhdidlər siyahısında olan təhdidləri m sayda C_j $(j = 1,2, \dots, m)$ kriteriyalarına nəzərən qiymətləndirilməlidir. Ekspertlər başvermə ehtimalı böyük olan və böyük təsir göstərə bilən təhdidlərə daha yüksək reytinqlər verirlər. Təhdidlərin reytinqi 6-ballıq şkala ilə qiymətləndirilir: 0 – Təhdid yoxdur; 1 – Aşağı; 2 – Məqbul; 3 – Orta; 4 – Əhəmiyyətli; 5 – Yüksək.

Qiymətləndirmə hər bir ekspert tərəfindən həyata keçirilir və $\mathbf{X}^k = \left(X_{ij}^k\right)_{n\times m}$ $k = 1,2, \dots, p$ qərar matrisləri alınır. Hər bir qərar matrisi böyük qiymətlərin təsirini azaltmaq üçün əvvəlcə normallaşdırılır. Normallaşdırma hər bir j kriteriyası üzrə aşağıdakı qaydada aparılır (sadəlik üçün düsturlarda x_{ij}^k elementlərinin yuxarısındakı k indeksi yazılmır):

$$x_{ij} = \frac{X_{ij}}{\sum_{i=1}^{n} X_{ij}} \qquad (1)$$

Bu ekspert qiymətləndirmələri əsasında hər bir ekspert üçün kriteriya çəkilərinin müəyyən edilməsi $(w^C = (w_1^C, w_2^C, \dots, w_m^C))$, alternativlərin qiymətləndirilməsi $(A_1' > A_2' > \cdots > A_n')$, ekspertlərin çəkilərinin təyin edilməsi $(w = (w_1, w_2, \dots, w_p))$ və ranqlar barədə yekun konsensus qərarın $(r^* = (r_1, r_2, \dots, r_n))$ müəyyən edilməsi tələb edilir. Çəkili konsensus ranqlaşdırma məsələsini ümumi şəkildə aşağıdakı kimi ifadə etmək olar.

Tutaq ki, $\boldsymbol{r}_i = (r_{i1}, r_{i2}, \dots, r_{in})$ – i-ci ekspertin təhdidlərə verdiyi ranqlar vektorudur (i =1, …, p), burada r_{ij} – i-ci ekspertin j-cu təhdidə verdiyi ranqdır (j =1, …, n). Məsələ hər bir ekspertə w_i fərdi çəkisini təyin etməklə təhdidlərin $\boldsymbol{r}^*$ çəkili konsensus ranqını tapmaqdır. Məqsəd $\boldsymbol{r}^*$ ilə bütün $\boldsymbol{r}_i$-lər arasındakı çəkili məsafələri

minimallaşdırmaqdır. Əgər $\boldsymbol{w} = (w_1, w_2, \dots, w_p)$ ekspertlərə təyin edilmiş çəkilərin vektorudursa, onda çəkili konsensus ranqlaşdırması məsələsi aşağıdakı optimallaşdırma məsələsi kimi ifadə oluna bilər:

$$argmin_{\boldsymbol{w},\boldsymbol{r}^*}(1-\lambda)\sum_{i=1}^{p} w_i\|\boldsymbol{r}^* - \boldsymbol{r}_i\|^2 + \lambda\|\boldsymbol{w}\|^2, \quad (2)$$

$$\text{Şərtlər: } \sum_{i=1}^{p} w_i = 1, w_i \geq 0, \forall i, \quad (3)$$

burada $0 \leq \lambda \leq 1$ requlyarlaşdırma parametridir, çəkili məsafənin minimallaşdırılması ilə çəkilərin hamarlığı arasındakı balansı tənzimləyir. Sadəlik üçün $\boldsymbol{r}^*$ konsensus ranqlaşdırması ilə $\boldsymbol{r}_i$ fərdi ekspert ranqlaşdırması arasındakı uzlaşmamanı ölçmək üçün Evklid məsafəsi istifadə edilir. Buna görə $w_i\|\boldsymbol{r}^* - \boldsymbol{r}_i\|^2$ i-ci ekspertin $\boldsymbol{r}_i$ ranq vektoru ilə $\boldsymbol{r}^*$ konsensus ranqı arasındakı çəkili məsafəni ölçür və (2)-dəki birinci həddi hər bir ekspert üçün bu məsafəni minimallaşdırmaq üçün istifadə edilir, ikinci toplanan isə çəkilərin hamarlığını təmin edən requlyarlaşdırma həddidir.

Bu məsələ xətti məhdudiyyətlər ilə kvadratik funksiyanın optimallaşdırılması məsələsidir və onun həlli üçün mövcud alqoritmlər istifadə edilir.

E-dövlətin informasiya infrastrukturunu güclü qarşılıqlı asılılıqları olan kritik informasiya infrastrukturları (Kİİ) təşkil edir. E-dövlət inkişaf etdikcə bu qarşılıqlı asılılıqlar daha da güclənir ki, bu, e-xidmətlərin keyfiyyətini yüksəltməyə imkan verir. Lakin bu qarşılıqlı asılılıqlar həm də e-dövlətin informasiya təhlükəsizliyi üçün böyük təhdidlərdən birinə çevrilir. Bu infrastrukturlardan hər hansı birinin fəaliyyətinin pozulması bütün e-dövlət ekosisteminə fəlakətli təsir göstərə bilər. Mövcud metodlarda informasiya təhlükəsizliyi riskləri ayrı-ayrı infrastrukturlar üzrə hesablanır və bir qayda olaraq, infrastrukturların qarşılıqlı asılılıqları nəzərə alınmır.

Yuxarıdakı arqumentləri nəzərə alaraq, qarşılıqlı asılı informasiya infrastrukturlarında risklərin qiymətləndirilməsi üçün e-dövlətin Kİİ-nın qarşılıqlı asılılıqlarının ikisəviyyəli iyerarxik modeli, qarşılıqlı asılı informasiya infrastrukturlarında informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodu və ekstremal risklərin modelləşdirilməsi üçün yanaşma işlənmişdir [31].

E-dövlətin Kİİ-nın qarşılıqlı asılılıqlarının ikisəviyyəli iyerarxik modelində iyerarxiyanın aşağı səviyyəsində Kİİ operatorları (KİİO) yerləşirlər, yuxarı səviyyədə isə E-Dövlətin Milli Operatoru (EDMO) fəaliyyət göstərir. KİİO ilə EDMO müvafiq sektor Koordinatoru vasitəsilə qarşılıqlı əlaqədə olur, Koordinator onlar arasında interfeys kimi çıxış edir.

Fərz olunur ki, hər bir KİİO Kİİ-də risklərin ümumi qiymətləndirməsini aparır və beləliklə, özünün birinci tərtib asılılıqlarını müəyyən edir. Bu qarşılıqlı asılılıqlar məlum olduğu üçün gözlənilir ki, hər bir KİİO özünün giriş risklərini, yəni başqa bir infrastrukturdakı təhlükəsizlik hadisəsi səbəbindən özünün potensial risklərini qiymətləndirəcəkdir.

EDMO bütün e-dövlət infrastrukturlarının qorunmasında maraqlıdır. O, hər bir KİİO-nun asılılıq ağacları haqqında müvafiq sektorun koordinatorundan məlumat alır. EDMO bu məlumatları müxtəlif KİİO-ları arasında asılılıqların tam təsvirini yaratmaq və milli səviyyədə daha makroskopik bir baxış yaratmaq üçün birləşdirir. EDMO səviyyəsində KİİO-larının giriş riskləri onlar arasındakı asılılıqları müəyyən etmək və təsdiqləmək üçün, həmçinin insidentin və ya təhdidin asılı Kİİ-larına təsirini qiymətləndirmək üçün analiz edilir.

Tutaq ki, müəyyən infrastruktur üçün j-cu növ risk hadisəsinin qiymətləndirilməsi tələb edilir. Fərz edək ki, müəyyən müddət ərzində j-cu risk hadisəsinin tezliyi və riskin reallaşması nəticəsində infrastrukturlara vurulan zərərlər haqqında məlumatlar EDMO-na məlumdur. Bu məlumatlar riskin qiymətləndirilməsi üçün itkinin ehtimal paylanması (Loss Distribution Approach, LDA) yanaşmasından istifadə etməyə imkan verir. LDA-nın tətbiqi zərər tezliyini və zərər həcmini modelləşdirməkdən və sonra ümumi zərərin paylanmasını hesablamaq üçün onların birləşdirilməsindən ibarətdir. Tutaq ki, EDMO verilmiş "Kİİ/risk hadisəsi" kombinasiyası üçün asılı infrastrukturlar siyahısını müəyyən etmişdir. Onları $1, 2, \dots m$ kimi işarə edək. Aşağıdakı işarələri qəbul edək:

- $X_{ij} - (i;\ j)$ cütü üçün itkilərin həcminin təsadüfi kəmiyyəti; $f_{ij}(x)$ – onun paylanma sıxlığı funksiyası; $F_{ij}(x) = P(X_{ij} \leq x)$ – ehtimal paylanması funksiyasıdır.

- N_{ij} – $(i;\ j)$ cütü üçün itkilərin tezliyinin təsadüfi kəmiyyəti;
  $p_{ij}(k) = \mathrm{P}(N_{ij} = k)$ – onun paylanma sıxlığı funksiyası;
  $P_{ij}(n) = \mathrm{P}(N_{ij} \le n)$ – ehtimal paylanması funksiyasıdır.

Onda $(i;\ j)$ cütü üçün ümumi itki L_{ij} belə müəyyən olunur:

$$L_{ij} = \sum_{k=1}^{N_{ij}} X_{ij}(k) = X_{ij}(1) + X_{ij}(2) + \cdots + X_{ij}(N_{ij}), \quad (4)$$

burada $X_{ij}(k)$ – $(i;\ j)$ cütü üçün baş vermiş k-cı itkinin həcmidir.

Modeli sadələşdirmək üçün aşağıdakı fərziyyələr qəbul edilir:

1. N_{ij} tezliyi və itkilərin həcmi X_{ij} asılı olmayan təsadüfi kəmiyyətlərdir;
2. İtkilərin həcmi X_{ij} asılı olmayan və eyni paylanmış təsadüfi kəmiyyətdir.

Birinci fərziyyə itkilərin tezliyi ilə həcmləri arasında korrelyasiya imkanını tamamilə istisna edir. İkinci fərziyyə bildirir ki, eyni bir $(i;\ j)$ üçün iki müxtəlif itki asılı deyil və eyni paylanır.

Nəhayət, j-cu risk hadisəsi üçün itkilərin ümumi həcmi T_j bütün asılı infrastrukturlar üzrə cəm kimi hesablanır:

$$T_j = \sum_{i=1}^{m} L_{ij}. \quad (5)$$

İtkilərin tezliyini Puasson paylanması kimi modelləşdirmək standart hesab edilir. İnformasiya təhlükəsizliyi sahəsində də çox zaman fərz edirlər ki, kiberhücumlar Puasson prosesinin xassələrini ödəyir, yəni müdaxilələrin sayı Puasson paylanması ilə yaxşı modelləşdirilir və müdaxilələr arasındakı müddət eksponensial paylanır.

Ekstremal hadisələri nəzərə almaq üçün itkilərin həcmi "ağır quyruqlu" paylanmalar ilə təsvir olunur [13]. İtkilərin həcmini təsvir etmək üçün istifadə olunan tipik ehtimal modelləri loqnormal, qamma və Veybull paylanmaları və ümumiləşdirilmiş Pareto paylanmasıdır. Son zamanlar tədqiqatçıların diqqəti daha dərin analitik analiz imkanı verən loqnormal paylamasına yönəlmişdir.

Bu tədqiqatda ümumiləşdirilmiş Pareto paylanmasının parametrlərini qiymətləndirmək üçün eksperimentlərdə AzScienceCERT kompüter insidentlərinin emalı komandası tərəfindən toplanmış verilənlər bazası istifadə edilmişdir [13].

Kritik infrastrukturların əsas kommunikasiya və idarəetmə magistralı İnternetdir və bu baxımdan ölkənin İnternet infrastrukturunun dayanıqlığını e-dövlətin təhlükəsizliyinin olduqca vacib komponenti hesab etmək olar. Bu cəhəti nəzərə alaraq, İnternetin milli infrastrukturunun genişmiqyaslı kiberhücumlara və təsadüfi qəzalara qarşı dayanıqlığının qiymətləndirilməsi üçün modellər təklif edilir [30].

İnternetin milli infrastrukturunun dayanıqlığını qiymətləndirmək üçün uyğun kriteriyalar seçilməlidir. ANSI T1A1.2 komitəsi şəbəkənin dayanıqlığını arzuolunmaz hadisə baş verdiyi andan yolverilən məhsuldarlıq səviyyəsinə malik stasionar vəziyyət bərpa olunana qədər keçid məhsuldarlığı kimi müəyyən edir. İnternet infrastrukturu sahəsində məhsuldarlıq metrikası kimi bir saatda xidmət edilən istifadəçilərin sayını, İnternet kəsintisi baş verdiyi andan keçən müddəti və s. götürmək olar. Təklif olunan dayanıqlıq modelləri bu göstəricilər əsasında işlənmişdir.

Fərz edək ki, İnternetin milli infrastrukturunda tranzit beynəlxalq trafikə xidmət edən provayderlərin (milli ISP-lər) sayı n-dir. a_i – i-ci ISP-nin istifadəçilərinin nisbi sayıdır. $x_i(t) \in \{0,1\}$ t – anında i-ci ISP-nin vəziyyətidir (1 – normal, 0 – dayanmış). Bu işarələrlə t anında İnternet infrastrukturunun dayanıqlığını belə ifadə etmək olar:

$$A(t) = \sum_{i=1}^{n} a_i x_i(t) \qquad (6)$$

Milli ISP-lər arasında kommunikasiya (tranzit, pirinq) olduğu və dayanmış ISP-nin yükünün xüsusi Əlaqələndirmə Mərkəzi tərəfindən digər ISP-lərə yönləndirildiyi fərz olunur. Bu halda İnternet infrastrukturunun dayanıqlığı:

$$A(t) = \sum_{i=1}^{n} a_i x_i(t) + \sum_{i=1}^{n} \sum_{j \in J_i} \big(1 - x_i(t)\big) b_{ij} d_{ij}, \qquad (7)$$

burada J_i – i-ci ISP-nin yükünün yönləndirildiyi ISP-lər çoxluğu, $(b_{i,1}, b_{i,2}, \dots, b_{i,k})$ – yükün paylanması vektorudur, $k = |J_i|$ və $\sum_{j \in J_i} b_{ij} \le a_i$. Əgər i- və j-cu ISP-lər arasında pirinq varsa, $d_{ij} = 1$, əks halda $d_{ij} = 0$.

Dayanıqlığın qiymətləndirilməsi üçün AI³ modeli. Aşağıdakı işarələri daxil edək: C – ISP-lərin sayı; N – İnternet istifadəçilərinin

sayı; K_j – müşahidə periodu ərzində j-cu ISP-də baş vermiş imtinaların sayı; N_{jk} – j-cu ISP-də k-cı imtinanın təsir etdiyi istifadəçilərin sayı; φ_{jk} – j-cu ISP-də k-cı imtinanın yaratdığı kəsintinin müddəti (saatlarla); K_j – müşahidə periodu ərzində j-cu ISP-də baş vermiş imtinaların orta sayı.

İnternet kəsintilərinin orta müddətini (Average Internet Interruption duration Index, AI^3) belə ifadə etmək olar:

$$AI^3 = \sum_{j=1}^{C} \sum_{k=1}^{K_j} \varphi_{jk} \frac{N_{jk}}{N} \tag{8}$$

Üçüncü fəsildə e-dövlətin biometrik identifikasiya sisteminin təkmilləşdirilməsi məqsədilə bir sıra metodlar işlənmişdir.

Biometrik identifikasiya sistemi e-dövlətdə autentifikasiya və avtorizasiya sisteminin əsasını təşkil edir və e-xidmətlərin təhlükəsizliyinin təmin edilməsində olduqca vacib rol oynayır. Lakin ölkə miqyasında biometrik eyniləşdirmə sisteminin qurulması zamanı qarşıya bir sıra elmi-praktiki problemlər çıxır. Bu qəbildən əsas problemlər mövcud biometrik sistemlərin tanıma keyfiyyətinin və təhlükəsizliyinin praktikada istifadə baxımından arzulanan səviyyədə olmaması, eyni biometrik xarakteristika ilə işləyən müxtəlif sistemlər arasında interoperabelliyin aşağı səviyyəsi və biometrik sistemlərin digər informasiya təhlükəsizliyi sistemləri, o cümlədən kriptoqrafik sistemlərlə inteqrasiyasında meydana çıxan çətinliklərdir. Bu problemlərin həlli istiqamətində biometrik sistemlərdə biometrik nümunənin keyfiyyəti haqqında informasiyanın biometrik sistemin qərarı ilə aqreqasiyası metodu [4], dəyişiklik edilmiş barmaq izlərinin fraktal xarakteristikalar əsasında aşkarlanması metodu [7] və biometrik kriptosistemlərin sintezi üçün müxtəlif metodlardan ibarət yanaşma təklif olunur [10].

Məlumdur ki, biometrik sistemlərdə birinci və ikinci növ statistik səhvlər baş verir və bu səhvlər iki göstərici ilə xarakterizə olunur: 1) FRR (False Rejection Rate) – səhv imtina nisbəti – sistemə buraxılmayan qanuni istifadəçilərin nisbi sayı (faizlə); 2) FAR (False Acceptance Rate) – səhv qəbul nisbəti – sistemə buraxılmış icazəsi olmayan istifadəçilərin nisbi sayı (faizlə). Biometrik sistemin qərarına

(qəbul/imtina) inamın qiymətini ədəbiyyatda çox zaman qərarın etibarlılığı adlandırırlar. Biometrik sistemin qərarının etibarlığının qiymətləndirilməsi problemi nisbətən son dövrlərdə diqqəti cəlb edir. Qərarın etibarlılığının qiymətləndirilməsi unimodal biometrik verifikasiya sistemini ikisinifli klassifikasiya sisteminə çevirir (əvvəlcə etibarlı/etibarsız, sonra qəbul/imtina klassifikasiyası aparılır).

Aydındır ki, biometrik sistemdə qəbul edilən qərarın etibarlılığı biometrik nümunənin keyfiyyətindən asılıdır. Biometrik sistemin ümumi sxemində keyfiyyətə nəzarət biometrik sistemin vacib elementidir və biometrik nümunələrin müqayisəsi mərhələsindən əvvəl yerinə yetirilir. Təklif edilən yanaşmada qeydiyyat zamanı alınmış və verifikasiya üçün təqdim olunmuş barmaq izi təsvirlərinin keyfiyyət qiymətləri Dempster-Şafer nəzəriyyəsi əsasında aqreqasiya edilərək biometrik sistemin etibarlılığı müəyyən edilir.

Dempster-Şafer nəzəriyyəsi Bayesin subyektiv ehtimallar nəzəriyyəsini ümumiləşdirir, lakin Bayes ehtimalından fərqli olaraq, hər bir hipotezə ehtimalın qiymətini yox, qeyri-müəyyənliyin (həqiqətəoxşarlığın) ehtimal intervalını qarşı qoyur.

Dempster-Şafer nəzəriyyəsində predmet oblastı tam və bir-birini qarşılıqlı istisna edən hipotezlərin Θ çoxluğu ilə təsvir edilir. Θ çoxluğununun boş çoxluq daxil olmaqla bütün altçoxluqları çoxluğunu 2^{Θ} ilə işarə edək.

Sübutların etibarlılığının başlanğıc qiymətlərini təyin etmək üçün $m()$ kütlə funksiyası müəyyən edilir. Kütlə funksiyası 2^{Θ} çoxluğunda təyin olunub, $[0,\ 1]$ intervalından qiymətlər alır və aşağıdakı şərtləri ödəyir:

$$m(\emptyset) = 1; \sum_{A \in 2^{\Theta}} m(A) = 1. \quad (9)$$

$m(A)$ kəmiyyəti sübutun etibarlılıq dərəcəsini, A sübutu ilə təsdiqlənən hipotezlərin həqiqiliyinə inamı təsvir edir. A çoxluğunun $m(A) > 0$ şərtini ödəyən hər bir altçoxluğuna m-in fokal elementi deyilir. Baza ehtimallarından çıxış edərək inam funksiyasını (ing. belief function) və həqiqətəoxşarlıq funksiyasını (ing. plausibility) müəyyən edirlər.

$bel(): 2^{\Theta} \to [0,1]$ inam funksiyası $bel(\emptyset) = 0$ və $bel(\Theta) = 1$ şərtlərini ödəyir. İstənilən A fokal elementi üçün inam funksiyasını A-

nın bütün altçoxluqları üzrə $m()$ qiymətlərini toplamaqla hesablamaq olar:

$$bel(A) = \sum_{B|B\subseteq A} m(B) \tag{10}$$

$pl(A)$ həqiqətəoxşarlıq funksiyası inam funksiyası ilə $pl(A) = 1 - bel(\bar{A})$ şəklində əlaqəlidir:

Biometrik şablonda təsvirin keyfiyyət qiymətlərinin aqreqasiyası üçün 2 sinfə klassifikasiya məsələsinə baxılır. Siniflər çoxluğunu $\Lambda = \{\lambda^{reliable}, \lambda^{non-reliable}\}$ kimi işarə edək. Fərz edək ki, mövcud informasiya $T = \{(x^1, \lambda^1), \dots, (x^N, \lambda^N)\}$ təlim seçməsindən ibarətdir, burada $x^i, i = 1, \dots, N$ – obrazlardır, λ^i, $i \in$ {reliable, non-reliable}– uyğun sinif nişanlarıdır. Fərz edək ki, obrazlar arasındakı oxşarlıq müəyyən $d(\cdot,\cdot)$ məsafə funksiyası ilə ölçülür.

Tutaq ki, x – T-də olan informasiya əsasında klassifikasiya edilməli olan obrazdır. Hər bir (x^i, λ^i) cütü x-in sinfi mənsubiyyəti barədə müxtəlif sübut təşkil edir. Əgər təlim seçməsindən hər bir obraza baxılsa, onda Dempster qaydasından istifadə etməklə kütlənin birləşdirilməsini həyata keçirmək olar, nəticədə x obrazının sinfi barədə yekun inam alınır. x-dən uzaqda yerləşən təlim obrazları az informasiya verir, buna görə x-in ən yaxın k qonşusuna baxmaq kifayətdir, bu halda m:

$$m = m(\cdot\,|x^{i_1}) \oplus \dots \oplus m(\cdot\,|x^{i_k}), \tag{11}$$

kimi müəyyən ediləcək, burada $I_k = \{i_1, \dots, i_k\} - T$ təlim seçməsində x-in k ən yaxın qonşularının indeksləridir.

Əgər d məsafə funksiyası kimi Evklid məsafəsi istifadə edilərsə, onda $\phi_q(d) = exp(-\gamma_q d^2)$ qəbul etmək və istənilən $q \in$ {*reliable, non-reliable*} üçün m düsturunu

$$m(\{\lambda_q\}) = \frac{1}{K}\left(1 - \prod_{i\in I_{k,q}} \left(1 - \alpha \cdot exp(-\gamma d_i^2)\right)\right) \prod_{r\neq q} \prod_{i\in I_{k,q}} (1 - \alpha \cdot exp(-\gamma d_i^2)_r) \tag{12}$$

şəklində göstərmək olar, burada $I_{k,q} - I_k$-nın x obrazının λ_q sinfinə aid olan qonşularına uyğun altçoxluğu, K – normallaşdırıcı vuruqdur. x obrazı ən böyük $m(\{\lambda_q\})$ qiymətinə uyğun λ_q sinfinə aid edilir, burada $0 < m(\{\lambda_q\}) < 1$.

Barmaq izlərinin avtomatik tanınması sistemləri dünya biometrik sistemlər bazarının təxminən yarısını tutur. Bu sistemlər barmaq izlərinin unikal olması və yaşlı insanlarda bütün həyatı boyu dəyişmədiyi fərziyyəsinə əsaslanırlar. Süni dəyişilmiş barmaq izləri bu fərziyyələri pozur və biometrik sistemlərin təhlükəsizliyinə və etibarlılığını sual altında qoyur.

Barmaq izinə süni dəyişiklik edilməsi nəticəsində yeni struktur elementləri: çapıqlar, papilyar naxışların pozulduğu sahələr, barmaq izinin istiqamətlər meydanının kəskin dəyişməsi zonaları və s. yaranır. Tədqiqat hipotezi bu müşahidəyə əsaslanır və fraktal analizin mürəkkəb sistemlərin qlobal və lokal fəza strukturunu təsvir etmək xassəsindən istifadə edir.

Dəyişilmiş barmaq izlərinin fraktal xarakteristikalar əsasında aşkarlanması metodu aşağıdakı addımlar ardıcıllığı ilə göstərilə bilər:

1. Barmaq izinin təsviri ilkin emal edilir və normallaşdırılır.
2. Fraktal xarakteristikalar hesablanır və əlamətlər vektoru formalaşdırılır.
3. Əlamətlər vektoru SVM ilə klassifikasiya edilir.

Eksperimentlərdə modifikasiya olunmuş Katz metodu ilə hesablanmış fraktal ölçü; lokal miqyaslama eksponenti və multifraktal spektr kimi fraktal xarakteristikalar əsasında əlamət vektorları istifadə edilmişdir.

Barmaq izləri üçün təklif edilmiş biometrik kriptosistemin ümumi sxeminə barmaq izlərinin ilkin emalı; barmaq izində nüvə (istinad) nöqtəsinin tapılması; barmaq izi təsvirinin hissələrə bölünməsi; FingerCode (Qabor filtrləri) və LBP (Local Binary Pattern) daxil olmaqla barmaq izinin tekstur əlamətlərinin çıxarılması; biometrik diskretləşdirmə; etibarlı bitlərin birləşdirilməsi və FCS (Fuzzy Commitment Scheme) daxildir. FCS kriptoqrafik açarı biometrik şablonda gizlətmək üçün səhvləri korreksiya edən kodlardan və kriptoqrafik heş-funksiyadan istifadə edir.

Barmaq izi tekstur deskriptorlarının binar təsviri üçün etibarlılığa əsaslanan diskretləşdirmə sxemi seçilmişdir. Tekstur deskriptorların aşağı dəqiqliyi, diskretləşdirmə sxemlərində diskriminativ informasiyanın itirilməsi və s. səbəblərdən bir diskretləşdirilmiş barmaq izi deskriptorunun istifadəsi arzulanan məhsuldarlığa malik biometrik kriptosistem qurmağa imkan vermir. Bu problemi aradan qaldırmaq üçün diskretləşdirilmiş barmaq izi tekstur deskriptorlarının aqreqasiyası üsulu təklif edilir. Səhvləri korreksiya edən kodların seçilməsi məsələsi də çox vacibdir. Diskretləşdirilmiş barmaq izi tekstur deskriptorlarından ən etibarlı bitlərin aqreqasiyası və effektiv LDPC (Low-Density Parity-Check) kodlarının istifadəsi praktikada tələb edilən açar uzunluğuna və biometrik tanıma göstəricilərinə malik biometrik kriptosistem qurmağa imkan verir.

Təklif edilmiş yanaşmanın iş göstəricilərini test etmək üçün 100 müxtəlif barmağın hər birinin 8 təsviri olan FVC 2000 DB2a barmaq izləri bazası istifadə edilmişdir. Hər bir barmağın ilk beş təsviri təhlükəsiz biometrik şablonun yaradılması üçün və sonrakı üç barmaq izi verifikasiya üçün istifadə edilir.

Cədvəl 1-də təklif edilmiş biometrik kriptosistem ədəbiyyatda rast gələn digər biometrik kriptosistemlərlə müqayisə edilir. Təklif edilmiş kriptosistem IrisCode kriptosistemi istisna olmaqla, digər sistemlərdən açarın uzunluğu, FRR və FAR baxımından üstündür.

Cədvəl 1. Təklif edilmiş sistemin digər sistemlərlə müqayisəsi

Metod	Biometrik əlamət	Açarın uzunluğu (bitl)	GAR (%)	FAR (%)
Hao et al.	Qüzehli qişa	140	99.53	0.0
Zhou et al.	Sifət	107	99.6	12.0
Maiorana	Əl imzası	29	93.05	6.95
Nandakumar et al.	Barmaq izi	40	99.98	17.5
Arakala et al.	Barmaq izi	34	85.0	15.0
Li et al.	Barmaq izi	50	95.15	0.0
Tuyls et al.	Barmaq izi	76	94.6	5.2
Təklif edilmiş	Barmaq izi	76	95.3	0.0
		100	92.67	0.0
		120	92.0	0.0
		140	89.33	0.0

Dördüncü fəsildə e-dövlət mühitində informasiya təhlükəsizliyi insidentlərinin idarə edilməsi metodları tədqiq edilmişdir.

E-dövlətdə informasiya təhlükəsizliyi insidentlərinin erkən mərhələdə aşkarlanması və onların qısa müddətdə minimal xərclərlə aradan qaldırılması informasiya təhlükəsizliyinin idarə edilməsinin çox vacib aspektidir. Xidmətdən paylanmış imtina hücumları (Distributed Denial of Service, DDoS) tez-tez təsadüf edilən informasiya təhlükəsizliyi insidentlərindən biridir və geniş tədqiq olunmasına baxmayaraq, onun erkən aşkarlanması hələ də problem olaraq qalır. Dissertasiya işində DDoS hücumların real zamanda daha dəqiq aşkarlanması üçün dərin neyron şəbəkələrindən Məhdud Bolsman maşınına (ing. Restricted Boltzman Machine, RBM) əsaslanan yanaşma işlənmişdir [24].

RBM neyronların stoxastik şəbəkəsidir, iki laydan: görünən laydan və görünməyən laydan ibarətdir. Görünən lay verilənləri təsvir edir, gizli lay isə görünən laydan əlamətləri öyrənir və verilənlərin ehtimal paylanmasını yaradır. Bir layın neyronları yalnız digər layın neyronları ilə əlaqələndiyi üçün şəbəkə məhdud adlandırılır. Laylar arasındakı əlaqələr simmetrikdir, informasiyanı hər iki istiqamətdə ötürmək mümkündür.

Eksperimentlərdə üç dərin təlim metodu: Bernulli-Bernulli RBM, Qauss-Bernulli RBM, Deep Belief Network və üç ənənəvi maşın təlimi metodu: SVM (radial basis), SVM (ε-SVR) və Decision Tree klassifikatorları reallaşdırılıb.

DoS hücumların aşkarlanması üçün 7 laydan, çəkiləri təsadüfi seçilmiş 100 gizli neyrondan və 38 görünən neyrondan ibarət RBM istifadə edilmişdir, aktivləşdirmə funksiyası sigmoid-dir. Eksperimentlər 5 sinifdən: probe, U2R (User to Root), R2L (Remote to Local), DoS və normal ibarət olan NSL-KDD bazasında (38 əlamət üzrə) aparılmışdır.

Əlamətlər sütun üzrə [0, 1] intervalında normallaşdırılmışdır. Şəbəkəni öyrətmək üçün 5 epoxa istifadə edilmişdir. NSL-KDD-Train verilənlərinin 20 faizi (25194 nümunə) treninq, NSL-KDD-Test verilənlərinin 20 faizi (4508 nümunə) isə test üçün istifadə edilmişdir.

Eksperimentlərin nəticələrini qiymətləndirmək üçün Accuracy, F-measure, g-mean, Precision, Recall, TN (True Negative), TP (True

Positive) indeksləri istifadə edilmişdir. Cədvəl 2-də RBM-in nəticələrinin klassik klassifikasiya alqoritmləri ilə müxtəlif metrikalar üzrə müqayisəli analizi verilmişdir.

Cədvəl 2. Metodların effektivliyinin qiymətləndirilməsi

	F-measure	g-mean	Precision	Recall	TN	TP
SVM (radial basis)	0.7400	0.7173	0.6096	0.9416	0.5464	0.9416
SVM (ε-SVR)	0.7550	0.7251	0.6139	0.9804	0.5363	0.9804
Decision tree	0.7190	0.6620	0.5710	0.9705	0.4516	0.9705
RBM	0.7530	0.7348	0.6233	0.9509	0.5678	0.9509

Cədvəl 2-dən göründüyü kimi, RBM alqoritminin nəticələri digər alqoritmlərlə müqayisədə daha üstündür.

Böyük informasiya sistemlərində hər gün onlarla, bəzən yüzlərlə informasiya təhlükəsizliyi insidenti qeydə alınır. İnformasiya təhlükəsizliyi insidentlərinin emalını CERT (Computer Emergency Response Team) adlanan xüsusi komandalar həyata keçirir. İnsan resurslarının məhdudluğu və insidentlərin emalı müddətlərinə qoyulan ciddi tələblər insidentlərə bir sıra meyarlar əsasında emal ardıcıllığını müəyyən edən prioritetlərin təyin edilməsini tələb edir.

Dissertasiya işində insidentlərin emalı prioritetlərini təyin etmək üçün genişlənmiş qeyri-səlis AHP istifadə edilir [12].

Tutaq ki, $X = \{x_1, x_2, ..., x_m\}$ insidentlər çoxluğu və $G = \{g_1, g_2, ..., g_n\}$ kriteriyalar çoxluğudur. Məlum genişlənmə analizinə uyğun olaraq, hər bir kriteriya götürülür və hər bir g_i kriteriyası üçün genişlənmə analizi yerinə yetirilir. Deməli, m hər bir insident üçün aşağıdakı kimi işarə olunan genişlənmə analizi qiymətləri alına bilər:

$$M_{g_i}^1, M_{g_i}^2, \dots, M_{g_i}^m, i = 1, \dots, n, \quad (13)$$

burada $M_{g_i}^j (j = 1, \dots, m)$ hamısı qeyri-səlis üçbucaq ədədlərdir. Genişlənmə analizinin addımları aşağıdakı kimi verilə bilər:

Addım 1. i-ci insidentə nəzərən qeyri-səlis sintetik ölçü belə təyin olunur:

$$S_i = \sum_{j=1}^m M_{g_i}^j \otimes \left[\sum_{i=1}^n \sum_{j=1}^m M_{g_i}^j\right]^{-1}. \quad (14)$$

Addım 2. $M_1 = (l_1, m_1, u_1)$ və $M_2 = (l_2, m_2, u_2)$ iki üçbucaqlı qeyri-səlis ədədləri üçün $M_1 \geq M_2$ mümkünlük dərəcəsi belə təyin edilir:

$$V(M_2 \geq M_1) = \begin{cases} 1, \text{əgər } m_2 \geq m_1 \\ 0, \text{əgər } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, \text{əks halda} \end{cases} \quad (15)$$

Addım 3. M_1 və M_2-ni müqayisə etmək üçün $V(M_1 \geq M_2)$ və $V(M_2 \geq M_1)$ qiymətlərinin hər ikisini müəyyən etmək lazımdır. Qabarıq qeyri-səlis ədədin verilmiş k qabarıq qeyri-səlis $M_i(i = 1, \dots, k)$ ədədlərindən böyük olmasının mümkünlük dərəcəsi belədir:

$$V(M \geq M_1, M_2, \dots, M_k) = \\ = V[(M \geq M_1)\ and\ (M \geq M_2) \dots and\ (M \geq M_k)] = \\ = \min V(M \geq M_i), i = 1,2, \dots, k. \quad (16)$$

Fərz edək ki,

$$d(A_i) = \min V(S_i \geq S_k), k = 1,2, \dots, n; k \neq i. \quad (17)$$

Onda çəki vektoru

$$W' = (d'(A_1), d'(A_2), \dots, d'(A_n))^T, \quad (18)$$

ilə verilir, burada A_i $(i = 1, \dots, n)$ – n elementdir.

Addım 4. Normallaşdırılmış çəki vektorları hesablanır:

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T, \quad (19)$$

burada W qeyri-səlis olmayan (həqiqi) ədədlərin vektorudur. İnsidentlərin prioritetləri normallaşdırılmış çəki vektorlarına əsasən müəyyən edilir.

İnformasiya təhlükəsizliyi insidentlərinin real zamanda emalı üzrə işlərin CERT-qrupları arasında optimal paylanması da aktual məsələdir və aşağıda insidentlərin emalı proseslərinin çoxmeyarlı optimallaşdırılması üçün də yanaşma təklif edilir [29]. Fərz olunur ki, CERT xidmətləri göstərən provayderə bir neçə informasiya təhlükəsizliyi insidentini emal etmək sifarişi daxil olub. İnsidentlər müxtəlif təhlükəsizlik domenlərindən daxil ola bilər. CERT-provayderinin əlaqələndirmə mərkəzi bu işləri özünün insidentlərin emalı üzrə ixtisaslaşmış cavablandırma qrupları (CERT-qrupları) arasında bəzi məhdudiyyətləri nəzərə almaqla müəyyən kriteriyalara görə optimal paylamalıdır. CERT-qrupu bir nəfərdən də ibarət ola bilər.

Tutaq ki, J_1, J_2, …, J_n insidentlər çoxluğu R_1, R_2, …, R_m CERT-qrupları tərəfindən emal edilməlidir. J_i insidentinin emalı n_i prosedurdan ibarətdir (i =1, …, n). Fərz olunur ki, insidentlər bir-

birindən asılı deyil və müxtəlif insidentlərin prosedurları arasında ardıcıllıq münasibətləri yoxdur. Eyni bir insidentin prosedurları isə ardıcıllıq münasibətinə görə zəncir əmələ gətirirlər: $O_{1j} \to O_{2j} \to \cdots \to O_{n_i,j}, i = 1, \dots, n$. Hər bir J_i insidenti ilə direktiv cavablandırma müddəti d_i və w_i çəkisi (kritiklik dərəcəsi və ya gecikməyə görə cərimə əmsalı) əlaqələndirilir.

Fərz olunur ki, planlaşdırma üfüqü period adlanan (məsələn, saatlar) bərabər uzunluqlu zaman intervallarına bölünüb və emal müddətləri bir periodun diskret misilləridir. Prosedura başladıqdan sonra onu dayandırmaq olmaz, yəni kəsintiyə yol verilmir (ing. preemption). $t = 0$ anında bütün CERT-qrupları əlyetərdir və istənilən insidentin emalına başlamaq olar. Hər bir prosedur yalnız bir CERT-qrupu tərəfindən emal edilə bilər.

Aşağıdakı işarələri daxil edək:

n – insidentlərin sayı;

m – cavablandırma qruplarının (CERT-qrupların) sayı;

n_i – i insidentində cavablandırma prosedurlarının ümumi sayı;

N – cavablandırma prosedurlarının ümumi sayı, $N = \sum_{i=1}^{n} n_i$;

O_{ij} – i insidentinin j-cu cavablandırma proseduru;

p_{ijk} – O_{ij} prosedurunun k-cı CERT-qrup tərəfindən emal müddəti;

t_{ijk} – k-cı CERT-qrupun O_{ij} prosedurunun emalına başlama vaxtı;

t_{ij}^{F} – O_{ij} prosedurunun başa çatma vaxtı;

i, h – insidentlərin indeksi, i, h = 1, 2, ..., n;

k – cavablandırma qruplarının indeksi, k = 1, 2, ..., m;

j, g – cavadlandırma prosedurlarının indeksi, j, g = 1, 2, ..., n_i;

d_i – i-ci insidentin direktiv cavablandırma müddəti;

T_i – i-ci insidentin cavablandırılmasının gecikmə müddəti;

w_i– i-ci insidentin çəkisi;

W_k – k-cı CERT-qrupun insidentlərin emalına sərf etdiyi ümumi müddət;

$$x_{ijk} = \begin{cases} 1, \text{əgər } k\text{cı CERTqrup } O_{ij} \text{ proseduruna təyin olunubsa,} \\ 0, \text{əks halda} \end{cases}$$

Yuxarıdakı işarələrlə k-cı CERT-qrupun insidentlərin emalına sərf etdiyi ümumi W_k müddətini belə ifadə etmək olar:

$$W_k = \sum_{i=1}^{n} \sum_{j=1}^{n_j} p_{ijk} x_{ijk}, \qquad (20)$$

i-ci insidentin cavablandırılmasının gecikmə müddəti T_i aşağıdakı kimi müəyyən olunur:

$$T_i = max\left(t_{i,n_i}^F - d_i, 0\right), \quad (21)$$

Adətən, insidentlərin emalını planlaşdıran zaman bir deyil, bir neçə kriteriyanı nəzərə almaq lazım gəlir. Əlbəttə, ilk növbədə insidentlərin emalına sərf olunan ümumi zaman müddətini minimallaşdırmaq lazımdır. Lakin iş yükünü CERT-qruplar arasında elə bölmək lazımdır ki, hər hansı CERT-qrup həddindən çox yüklənməsin. Eyni zamanda, kritik insidentlərin emalını da direktiv müddətlər ərzində həyata keçirmək tələb olunur. Bunu nəzərə alaraq, insidentlərin emalı zamanı aşağıdakı kriteriyaların minimallaşdırılması məsələsi qarşıya qoyulmuşdur:

(1) İnsidentlərin emalına sərf edilən ümumi zaman müddəti;
(2) İnsidentlərin kritikliyi nəzərə alınmaqla emalın maksimum gecikmə müddəti;
(3) CERT-qrupların insidentlərin emalına sərf etdiyi ümumi müddətin maksimumu.

Yuxarıdakı işarələrdən istifadə etməklə bu kriteriyaları belə ifadə etmək olar:

$$min\, F_1 = \max_{1\le i\le n}\left\{\max_{1\le j\le n_i}\left\{t_{ij}^F\right\}\right\}, \quad (22)$$

$$\min F_2 = \max_{1\le i\le n}\{w_i T_i\}, \quad (23)$$

$$min\, F_3 = \max_{1\le k\le m}\{W_k\}. \quad (24)$$

Modeldə aşağıdakı məhdudiyyətlər vardır:

$$t_{ij}^F - t_{i,j-1}^F \ge p_{ijk}x_{ijk}, j = 2, \dots, n_i, \forall i, k \quad (25)$$

$$\left[(t_{hg}^F - t_{ij}^F - t_{hgk})x_{hgk}x_{ijk} \ge 0\right] \vee \left[(t_{ij}^F - t_{hg}^F - t_{ijk})x_{hgk}x_{ijk} \ge 0\right], \forall (i,j),(h,g),k \quad (26)$$

$$\sum_{k=1}^{m} x_{ijk} = 1, \forall i, j. \quad (27)$$

(26) şərti prosedurların ardıcıllığına olan məhdudiyyətləri təmin edir. (27) şərti hər bir CERT-qrupun ixtiyari zaman anında yalnız bir

proseduru emal edə bildiyini ifadə edir. (28) şərti hər bir prosedurun emalı üçün bir cavablandırma qrupunun seçilə bildiyini göstərir.

Yuxarıdakı çoxkriteriyalı optimallaşdırma məsələsini həll etmək üçün mövcud yanaşmalardan ən sadəsi götürülmüşdür - ümumi məqsəd funksiyası hər birinə eyni çəki verməklə yuxarıda ifadə edilmiş məqsəd funksiyalarının çəkili cəmi kimi müəyyən edilir:

$$F = \frac{1}{3}F_1 + \frac{1}{3}F_2 + \frac{1}{3}F_3. \quad (28)$$

Beşinci fəsildə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sahəsində koordinasiya modellərinə baxılmış və koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi üçün indikatorlar sistemi təklif edilmiş [32], ikisəviyyəli iyerarxik sistemdə informasiya təhlükəsizliyi investisiyalarının koordinasiyası modeli [25] və informasiya təhlükəsizliyi servislərinin təşkili üzrə beynəlxalq koalisiya modeli [33] işlənmişdir.

Koordinasiya sisteminin qiymətləndirilməsi üçün informasiya yanaşması əsas götürülür. İnformasiya koordinasiya üçün əsas resursdur, bütün koordinasiya sisteminin effektivliyi onun keyfiyyətindən, həqiqiliyindən, vaxtında olmasından asılıdır.

Tutaq ki, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin koordinasiyası sistemində n agent iştirak edir və agentlərin qarşılıqlı əlaqələri qrafla göstərilir. Qrafın təpələri olaraq koordinasiya sistemində iştirak edən agentlər (sosial şəbəkə analizi termini ilə aktorlar), tilləri isə onlar arasındakı qarşılıqlı əlaqələrdir. Fərz edək ki, koordinasiya şəbəkəsinin əlaqələr qrafı agentlərın $A = \|a_{ij}\|$ insidentlik matrisi ilə təsvir olunur, onun elementləri məlum qaydada müəyyən olunur:

$$a_{ij} = \begin{cases} 1 - i \text{ və } j \text{ agentləri til ilə birləşir,} \\ 0 - \text{əks halda.} \end{cases} \quad (29)$$

Topoloji struktur qarşılıqlı əlaqə və ya tabeçilik dərəcəsini əks etdirir, koordinasiya funksiyaları və informasiya axınları haqqında heç bir məlumat daşımır. Lakin topoloji strukturu əsas götürməklə və onun analizini aparmaqla koordinasiya sisteminin reinjinerinqini həyata keçirmək və onun iş effektivliyini yüksəltmək mümkündür.

Burada koordinasiya sisteminin operativliyini xarakterizə etmək üçün sistemin inersiallıq dərəcəsindən istifadə edilir. Ümumiyyətlə,

sistemin inersiallıq dərəcəsi ($\Delta\tau$) sistemdə çıxış siqnalı (t_{out}) ilə giriş siqnalı (t_{in}) arasındakı gecikmə kimi müəyyən olunur ($\Delta\tau = t_{out} - t_{in}$).

Tutaq ki, koordinasiya sistemini təsvir edən müəyyən qraf verilib və onun hər bir (i, j) tili üçün iki ədəd təyin edilib: (In_{ij}, Fb_{ij}). In_{ij} informasiyanın i-dən j-a ötürülməsi müddəti, Fb_{ij} isə bu informasiyaya j-dan i-yə reaksiya müddətidir. Hər hansı μ yolunun $K(\mu)$ inersiyası informasiyanın bu yol ilə toplam ötürmə müddəti $In(\mu) = \sum_{(i,j)\in\mu} In_{ij}$ilə reaksiyanın toplam ötürmə müddəti $Fb(\mu) = \sum_{(i,j)\in\mu} Fb_{ij}$ arasındakı fərq kimi müəyyən edilir:

$$K(\mu) = In(\mu) - Fb(\mu). \tag{30}$$

Verilmiş koordinasiya strukturu üçün "inersiya diametri" anlayışını da daxil etmək olar. Qrafın diametri $d(G)$ onun iki təpəsini birləşdirən ən qısa yolun maksimal uzunluğu kimi müəyyən edilir:

$$d(G) = \max_{a,b\in V(G)} d(a, b), \tag{31}$$

burada a və b qrafın ixtiyari iki təpəsidir, $V(G)$ – bütün təpələrin çoxluğudur, $d(a, b)$ – a və b təpələri arasındakı məsafədir. Bu məsələni həll etmək üçün Floyd-Uorşell (və ya Bellman-Ford) alqoritmi ilə qrafda bütün təpələr cütləri arasında ən qısa yolları tapmaq və onlardan maksimumu seçmək olar.

Reaksiya müddətinə direktiv tələblər irəli sürülə bilər. Əgər reaksiya direktiv müddətdə göstərilməsə, cərimə mexanizmi nəzərdə tutmaq olar. Cərimə mexanizmi nəzərə alınmaqla koordinasiyanın operativliyinin qiymətləndirilməsinə baxaq. Tutaq ki, qrafın hər bir (i, j) tili üçün iki çəki verilib: $\left(Out_{ij}, T_{ij}\right)$. Burada Out_{ij} – yuxarıda olduğu kimi cari reaksiya müddəti, T_{ij} – direktiv reaksiya müddətidir. Verilmiş başlanğıc aktordan son aktora hər bir yolu müəyyən informasiya prosesini təyin edir. Baxılan halda yolun uzunluğu onun tilləri üzrə reaksiya müddətlərinin cəmidir. Əgər baxılan prosesin müddəti əvvəlcədən verilmiş T_{ij} müddətindən fərqlidirsə, onda kənarlaşmaya mütənasib olan cəriməsi müəyyən edilir:

$$\chi_{ij} = \begin{cases} \alpha\left(T_{ij} - Out_{ij}\right), Out_{ij} \le T_{ij} \\ \beta\left(T_{ij} - Out_{ij}\right), T_{ij} \le Out_{ij} \end{cases} \tag{32}$$

burada α və β əmsalları həm müsbət, həm də mənfi ola bilər.

Gecikməyə görə cərimələr nəzərə alınmaqla koordinasiya sisteminin operativliyinin qiymətləndirilməsi məsələsini cəriməni minimallaşdıran yolun tapılması kimi qoymaq və həmin məsələni həll etmək üçün Bellman-Ford alqoritmindən istifadə etmək olar.

İkisəviyyəli informasiya təhlükəsizliyi sisteminin yuxarı səviyyəsində Koordinator (C_0), aşağı səviyyədə isə ayrı-ayrı informasiya təhlükəsizliyi domenləri (C_1,..., C_n) durur. Koordinator bütün domenlərin informasiya təhlükəsizliyinin təmin edilməsinə ümumi B büdcəsi ayırır. Hər bir i domeni Koordinatora özünün informasiya təhlükəsizliyi səviyyəsi (s_i) haqqında məlumat verir və Koordinatordan informasiya təhlükəsizliyinin təmin edilməsinə və təkmilləşdirilməsinə $x_i \geq 0$ büdcəsi (investisiya) xahiş edir. Hər bir domenin informasiya təhlükəsizliyi səviyyəsi $0 \leq s_i < 1, i = 1, \dots, n$ şərtini ödəyir. s_i-nin qiyməti nə qədər böyükdürsə, informasiya təhlükəsizliyinin səviyyəsi bir o qədər yüksəkdir. Mütləq informasiya təhlükəsizliyinin təmin edilməsi gözlənilmir, buna görə $s_i = 1$ halı istisna edilir. $s_i = 0$ i-ci altsistemdə təhlükəsizliyin təmin edilmədiyini göstərir. Bütün sistemin informasiya təhlükəsizliyi səviyyəsi $\bar{s} = \frac{1}{n}\sum_{i=1}^{n} s_i$ kimi müəyyən edilir.

Koordinator bütün domenlərdən məlumatları aldıqdan sonra, domenlərin informasiya təhlükəsizliyi səviyyələrini, ümumi büdcəyə məhdudiyyəti və domenlərin qarşılıqlı asılılıqlarını nəzərə alaraq domenlərə $\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n$ investisiyalarının ayrılması barədə qərar qəbul edir. Hər bir domen eqoist hərəkət edir və mümkün olduqca yüksək investisiya səviyyəsi əldə etməkdə maraqlıdır. Koordinatorun məqsədi verilmiş büdcə çərçivəsində bütün sistemdə informasiya təhlükəsizliyi insidentlərindən itkiləri minimallaşdırmaq, başqa sözlə sosial rifahı maksimallaşdırmaqdır. Aşağıda bu məsələ qarşılıqlı asılı təhlükəsizlik oyunu kimi ifadə olunur.

n oyunçudan (informasiya təhlükəsizliyi domenlərindən) ibarət sistemə baxaq. Tutaq ki, oyunçuların qarşılıqlı asılılığı $G = (N, L)$ istiqamətlənmiş qrafı ilə təsvir edilir, burada $N = \{1, \dots, n\}$ və $L \in R_+^{n \times n}$ uyğun olaraq oyunçular çoxluğunu və onlar arasındakı istiqamətlənmiş əlaqələr çoxluğunu işarə edir. Oyunçu j yalnız $l_{ji} > 0$

olduqda oyunçu *i*-nin təhlükəsizlik vəziyyətinə təsir edə bilər. Oyunçu *i*-nin qonşuları çoxluğunu $N^i = \{j: l_{ji} > 0\}$ ilə işarə edək. Hər bir zaman anında oyunçu i birbaşa xarici mühitdən p_i ehtimalı ilə və l_{ji} ehtimalı ilə istənilən $j \in N^i$ qonşusu tərəfindən kiberhücuma məruz qala bilər. G şəbəkəsinin topologiyası və xaricdən kiberhücum ehtimalı p_i zamana görə dəyişmir.

Hər bir *i*-ci oyunçunun məqsədi – özünün aşağıda verilən u_i faydalılıq funksiyasını maksimallaşdırmaqdır:

$$U_i(\mathbf{x}) = -L_i x_i + C_i x_i - t_i \,, \tag{33}$$

burada $\boldsymbol{x} = \{x_1, x_1, \dots, x_n\}^T$ bütün investisiyalar vektorunu işarə edir, L_i – informasiya təhlükəsizliyi insidenti baş verdikdə oyunçu *i*-nin potensial itkiləri, C_i – oyunçu *i*-nin investisiyalarının (xüsusi) dəyəridir, bir investisiya vahidinə C_i>0 xərci çəkilir. t_i həddi oyunçunun məruz qala biləcəyi cəriməni/mükafatı xarakterizə edir və ümumi halda $\boldsymbol{x}$ investisiyalar vektorundan asılı ola bilər. Sadəlik üçün, sonrakı şərhlərdə $t_i = 0$ qəbul olunub. Fərz olunur ki, hər bir oyunçu rasional hərəkət edir və öz investisiya səviyyəsini faydalılıq funksiyasını maksimallaşdırmaq üçün seçir.

Yuxarıda sadalanmış n oyunçu arasında qarşılıqlı asılı təhlükəsizlik oyunu $(\{1, \dots, n\}, \{x_{i \geq 0}\}, \{u_i(\cdot)\})$ strateji oyunu kimi müəyyən edilir. Bu oyunda informasiya təhlükəsizliyi investisiyalarının optimal vektoru sosial rifahı maksimallaşdıran və Koordinator tərəfindən həll edilən aşağıdakı məsələnin həlli kimi tapılır:

$$\max_x \sum_{i=1}^{n} U_i(x) \tag{34}$$

$$x_i \geq 0, i = 1, \dots, n,$$

$$\sum_{i=1}^{n} C_i x_i \leq B, \tag{35}$$

Oyunçular barədə yuxarıda edilmiş fərziyyəyə görə, (34)-(35) məsələsi üçün yeganə x* sosial-optimal investisiya profili mövcuddur. Qeyd edək ki, L_i, C_i əmsalları və f_i risk fuksiyaları oyunçuların konfidensial informasiyasıdır, Koordinator bu informasiya barədə məlumatlı deyil və buna görə (34)-(35) məsələsini həll edə bilməz.

Eyni zamanda, x* həllini axtarmaq üçün oyunçuların da yetərli informasiyası yoxdur.

Buna görə Koordinator tərəfindən yerinə yetirilən elə koordinasiya mexanizmi tapmaq lazımdır ki, (34)-(35) məsələsi həlli oluna bilsin. Bunun üçün fərz edilir ki, oyunçular öz konfidensial məlumatlarını digər oyunçulara açıqlamamaq şərtilə Koordinatora təqdim edirlər. Bu fərziyyə ona əsaslanır ki, dövlət orqanlarının informasiya təhlükəsizliyi üzrə statistik hesabatlarını səlahiyyətli dövlət orqanına təqdim etmələri üçün qanunvericilik tələbləri ola bilər. Bu halda, Koordinator məsələni tam informasiya ilə həll edəcək və bu oyun üçün Neş tarazlığını tapa bilər.

İnformasiya təhlükəsizliyinin təmin edilməsi sıx beynəlxalq əməkdaşlıq tələb edir, ayrılıqda götürülmüş istənilən ölkə bu sahədə öz məqsədlərinə tam çata bilmir və bu məsələni həll etmək üçün digər ölkələrlə kooperasiya etməyə məcburdur. Fərz olunur ki, müəyyən ölkələrin informasiya təhlükəsizliyi sahəsində maraqlarının münaqişəsi antaqonist deyil, onların arasında bu sahədə qarşılıqlı öhdəliklər olan sazişlərin bağlanması mümkündür və ölkələr koalisiyadan əldə etdikləri faydanı bölə bilərlər.

Tutaq ki, koalisiyada n ölkə iştirak edir. i-ci ölkənin uduş funksiyasını (U_i) onun əldə etdiyi fayda (B_i) ilə xərcləri (C_i) arasındakı fərq kimi ifadə etmək olar.

Fərz edək ki, $t_i \in (0;1)$ – i-ci ölkənin ümumi xərclərdə pay bölgüsüdür. Ümumi halda, xərc funksiyasını t_i-nin funksiyası $C_i=C(t_i)$ kimi müəyyən etmək olar. Koalisiyanın toplam xərcləri G olarsa, i-ci ölkənin koalisiyada xərcləri $g_i = t_i G$ olacaq. Aydındır ki, $G = \sum_{i \in N} g_i$.

Həmçinin fərz edək ki, i-ci ölkənin koalisiyanın təqdim etdiyi informasiya təhlükəsizliyi xidmətindən istifadə edən istifadəçilərinin sayı n_i-dir, $S(n_i)$ isə i-ci ölkənin bu xidmətdən istifadə üçün çəkdiyi xərclərdir.

Tutaq ki, koalisiyanın bütün qazancı B funksiyası ilə təsvir olunur. Ümumi qazancın koalisiya ölkələri arasında pay bölgüsünü xarakterizə etmək üçün $\alpha_i \in (0;1)$ parametrini daxil edək, burada $\sum_{i \in N} \alpha_i = 1$. i-ci ölkə bu qazancın α_i hissəsini alır, yəni $B_i(G, \alpha_i) = \alpha_i B(G)$.

Yuxarıda qeyd edilənləri nəzərə almaqla koalisiyadakı i-ci ölkənin uduş funksiyasını aşağıdakı kimi təyin etmək olar:

$$U_i(G, g_i, \alpha_i, n_i) = \alpha_i B(G) - C(g_i) - S(n_i). \quad (36)$$

Qərar qəbuletmə parametrləri t_i və α_i-dir. Koalisiyada iştirak edən hər bir ölkənin strategiyası öz xərclərini minimallaşdırmaq və uduşunu maksimallaşdırmaqdır.

Koalisiya oyunlarında koalisiyanın dayanıqlığı vacib məsələdir. Bu tədqiqatda aşağıdakı dayanıqlıq konsepsiyaları istifadə edilir:

- daxili dayanıqlıq (koalisiya üzvünün koalisiyanı tərk etmək üçün stimulu yoxdur);
- xarici dayanıqlıq (koalisiya üzvü olmayanın koalisiyaya qoşulmaq üçün stimulu yoxdur).

Tutaq ki, P baxılan koalisiyadır; $P\backslash\{i\}$ ilə iştirakçı ölkə i koalisiyanı tərk etdikdə qalan koalisiya, $P\cup\{j\}$ ilə isə iştirakçı olmayan j koalisiyaya birləşdikdə yaranan koalisiya işarə edilir. Dayanıqlı P koalisiyası aşağıdakı kimi təyin edilir:

Daxili dayanıqlıq: $U_i(P) \geq U_i(P\backslash\{i\})\ \forall i \in P,$ (37)

Xarici dayanıqlıq: $U_j(P) \geq U_j(P \cup \{j\})\ \forall j \notin P.$ (38)

U_i uduş funksiyalarının iki dəfə kəsilməz diferensiallanan, kvazi-qabarıq və ciddi monoton artan olması fərz edilir. Bu fərziyyələr $g^*(P)$ və $\alpha^*(P)$ tarazlıq vektorlarını P koalisiyası və P-də olmayan bütün oyunçular arasında Neş tarazlığı kimi tapmağa imkan verir. Hər bir koalisiya üzvü "fayda-xərc nisbəti" qaydası ilə öz uduşunu əldə edə bilər.

Altıncı fəsildə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə qərarların qəbul edilməsi modelləri işlənmişdir.

E-dövlətin informasiya təhlükəsizliyinin strateji idarə edilməsi üçün qeyri-səlis koqnitiv xəritələr (Fuzzy Cognitive Map, FCM) əsasında model təklif edilmiş və e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sisteminin inkişafının müxtəlif strateji senariləri analiz edilmişdir [18]. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin koqnitiv modelləşdirilməsi üçün aşağıdakılar zəruridir:

1) informasiya təhlükəsizliyi vəziyyətinə təsir edən faktorların müəyyən edilməsi;
2) Faktorların qarşılıqlı təsir matrisinin qurulması;

3) informasiya təhlükəsizliyinin idarə edilməsinin koqnitiv modelinin qurulması;
4) Qurulmuş model üzərində e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin mümkün startegiyalarının yoxlanması.

Ümumiyyətlə, FCM biliklərin təsviri üsullarından biridir və FCM-in qurulması üçün predmet sahəsi ekspertlərinin bilik və təcrübəsi istifadə edilməlidir. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinə təsir edən faktorları müəyyən etmək üçün bir sıra ölkələrin milli kibertəhlükəsizlik strategiyaları analiz edilmişdir. Bu strategiyalar aparıcı informasiya təhlükəsizliyi mütəxəssisləri cəlb edilməklə işlənmişdir və ekspert biliklərinin toplandığı yetərincə yaxşı mənbələr hesab oluna bilər. Kibertəhlükəsizlik strategiyalarının analizi gedişində e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinə təsir edən bir sıra faktorlar müəyyən edilmişdir, onların siyahısı cədvəl 3-də verilir.

Qarşılıqlı təsir çəkilərinin təyin edilməsi üçün də ekspert qiymətləndirilməsi metodundan istifadə edilir. Hər bir ekspert qarşılıqlı təsir çəkisini $[-1,\ 1]$ intervalından ədəd kimi qiymətləndirir. Sonra qarşılıqlı təsirlərin bu matrisləri çəkilərin cəminin ortalama qiyməti və ya keçid funksiyası (məsələn, siqmoid funksiya) tətbiq edilməklə aqreqasiya olunur. Ekspertlərin inam çəkiləri nəzərə alınmaqla qarşılıqlı təsir çəkilərinin aqreqasiya olunmuş qiymətləri aşağıdakı düsturla hesablana bilər (yalnız eyni işarəli çəkilər nəzərə alınır):

$$W_{ij} = \frac{\sum_{k=1}^{m} b_k w_{ij}^k}{m}, \qquad (39)$$

burada w_{ij}^k – k-cı ekspertin C_i və C_j arasındakı qarşılıqlı təsir çəkisinə verdiyi qiymət; b_k – k-cı ekspertə inamın çəkisi; m – ekspertlərin sayıdır. Əgər ekspertin qiymətləri əksər ekspertlərin qiymətlərindən fərqlənirsə, onda həmin ekspert cərimələnir – ona çox kiçik və ya 0 inam çəkisi verilir.

FCM-də də digər qeyri-səlis sistemlərin əsas nöqsanları vardır: onlar müstəqil öyrənə bilmirlər. Müvafiq verilənlər olduqda neyron şəbəkələrinin öyrənmə mexanizmlərindən istifadə etməklə faktorların təsir çəkilərini yaxşılaşdırmaq olar. Adətən, belə yanaşmalar Hebb

öyrənmə metoduna əsaslanır, lakin evristik metodlardan istifadə edən yanaşmalar da var.

FCM dinamikasının modelləşdirilməsi. FCM çıxarış proseslərinə faktorların n qiymətindən ibarət olan A_{1xn} vəziyyətlər vektoru və çəki matrisi $W_{n\times n}$ daxildir. Hər bir faktorun qiymətinə onunla əlaqəli faktorların cari və əvvəlki qiymətləri təsir göstərir. Hər bir faktor üçün aktivləşdirmə qiyməti aşağıdakı qayda ilə iterativ hesablanır:

$$A_i^{(t+1)} = f\left(\sum_{j=1}^{n} w_{ij}A_j^{(t)}\right), i \neq j, \quad (40)$$

burada t – cari zaman; A_i – C_i faktorunun aktivləşdirmə səviyyəsi;; A_j – C_j faktorunun aktivləşdirmə səviyyəsi; w_{ij} – C_i və C_j arasında qarşılıqlı təsir çəkisi; f – keçid funksiyasıdır.

FCM üçün keçid funksiyaları kimi binar, üçvalentli və siqmoid funksiyaları istifadə edilir. Bu işdə siqmoid funksiyası tətbiq edilir:

$$f(x) = \frac{1}{1+e^{-\lambda x}}, \lambda > 0. \quad (41)$$

Fərz olunur ki, faktorların vəziyyətləri qeyri-səlis dəyişənlər kimi müəyyən edilə bilər: Yüksək (High), Orta (Medium) və Aşağı (Low).

İnformasiya təhlükəsizliyinin idarə edilməsinin müxtəlif strategiyalarının modeldə test edilməsi. Qeyd edək ki, hər bir C_j konsepti [0, 1] intervalından qiymətlər ala bilər, onu həm də «aktivləşdirmə səviyyəsi» adlandırırlar.

FCM-in modelləşdirilməsi prosesi hər bir FCM qovşağının aktivləşdirmə səviyyəsinə cari vəziyyət üçün mütəxəssislərin/maraqlı tərəflərin rəyi əsasında [0, 1] intervalından qiymətlər mənimsədilməklə başlayır. 0 qiyməti baxılan faktorun müəyyən iterasiyada sistemdə iştirak etmədiyini, 1 qiyməti isə faktorun maksimal dərəcədə iştirak etdiyini bildirir. Digər qiymətlər aktivləşdirmənin aralıq səviyyələrinə uyğun gəlir.

İnformasiya təhlükəsizliyinin idarə edilməsinin aşağıdakı senarilərinin modelləşdirilməsinə baxılır.

A senarisi: *Situasiyanın öz-özünə inkişafı*

A(0) = (1., 1., 1., 1., 1., 1., 0.).

B senarisi: *Yalnız texniki tədbirlərin tətbiqi* A(0)=(0, 0, 1, 0, 0, 0, 0).

Hesablama eksperimentlərində $\lambda = 1$ parametri ilə siqmoid funksiyası istifadə edilmişdir. Adətən, (41) düsturu ilə hesablamalar ən çoxu 5 zaman addımında yığılır. Bütün modellər stabil vəziyyətdə dayanır, lakin nəzəri olaraq onlar limit tsiklinə və ya xaotik attraktora da keçə bilərlər. B senarisi üzrə faktorların hesablanmış aralıq qiymətləri cədvəl 3-də verilib.

Cədvəl 3-ə əsasən nəticəyə gəlmək olar ki, yalnız texniki tədbirlərin istifadə edilməsi informasiya təhlükəsizliyinin səviyyəsinin əhəmiyyətli yaxşılaşmasına gətirmir (Senarilərin stabil vəziyyətləri arasında maksimal fərq 0.0424-dür).

Cədvəl 3. B senarisi üzrə hesablamaların son nəticələri

Faktorlar	Başlanğıc qiymətlər – B senarisi	Son qiymətlər – B senarisi	A və B senarilərinin stabil vəziyyətləri arasındakı fərq
Qanunvericilik tədbirləri	0.00	0.5275	0.0008
Təşkilati tədbirlər	0.00	0.5147	0.0008
Texniki tədbirlər	1.00	1.00	0.4184
Potensialın inkişafı	0.00	0.5875	0.0309
Maraqlı tərəflərin əməkdaşlığı	0.00	0.5378	0.0104
İnformasiya təhlükəsizliyi təhdidlərinin inkişafı	0.00	0.5000	0
İnformasiya təhlükəsiz-liyinin səviyyəsi	0.00	0.6048	0.0424

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi taktikalarının optimal seçilməsi üçün hiperoyun modeli işlənmişdir [11]. Oyunlar nəzəriyyəsi informasiya təhlükəsizliyi qərarlarını modelləşdirmək üçün ən güclü riyazi vasitələrdən biridir. Lakin ənənəvi oyunlar nəzəriyyəsində istənilən oyunçunun hər bir digər oyunçunun strategiyaları, üstüntutmaları haqqında tam məlumatlı olması fərz olunur. Bu çox ciddi fərziyyədir, bir çox real situasiyada oyunçular arasında çox zaman əhəmiyyətli informasiya asimmetriyası olur. Oyunçular həmişə hər bir oyunçunun əsl niyyətləri, strategiyaları və ya üstüntutmaları haqqında bütün informasiyanı bilmirlər. Nəticədə onlar situasiyanı öz baxış nöqtələrindən qavrayırlar və öz

qavrayışlarında səhv edə bilərlər. Bu işdə natamam informasiyalı oyunların hiperoyunlar adlanan xüsusi bir ailəsinə baxılır. Hiperoyun nəzəriyyəsi klassik oyunlar nəzəriyyəsini oyunçuların yanlış qavrayışlarında fərqləri nəzərə almaq imkanı ilə genişləndirir. Hiperoyunların informasiya təhlükəsizliyi üzrə qərarların tədqiq edilməsinə tətbiqi sahəsində tədqiqat işləri olduqca azdır. Burada hiperoyun yanaşması informasiya təhlükəsizliyi kontekstində taktiki analiz vasitəsi kimi təqdim olunur. Təklif olunan ikisəviyyəli hiperoyun hücum edənin (A) və müdafiə olunanın (D) informasiya təhlükəsizliyi situasiyası haqqında qavrayışlarını aşağıdakı kimi oyunlar seriyası kimi modelləşdirir.

Tutaq ki, $T_A = \{a_1, a_2, \dots, a_n\}$ A-nın taktikaları (hücum senariləri) çoxluğu və $T_D = \{d_1, d_2, \dots, d_m\}$ *D*-nin taktikaları (müdafiə mexanizmləri) çoxluğudur; həm də taktikaların sayı eyni olmaya bilər. Oyunun nəticəsi A və D-nin seçdikləri taktikalar cütündən ibarətdir. Beləliklə, mümkün nəticələr çoxluğu $O = T_A \times T_D = \{(a_1, d_1), (a_1, d_2), \dots (a_n, d_m)\}$. Hər bir oyunçu nəticələrin nizamlanmış üstüntutma vektorunu tərtib edir: $P_A = \langle o_{A1}, o_{A2}, \dots, o_{An \cdot m} \rangle$ və $P_D = \langle o_{D1}, o_{D2}, \dots, o_{Dn \cdot m} \rangle$. Üstüntutma vektorunda elementlər daha üstün tutulandan az üstüntutulana doğru nizamlanır: $\forall o_i, o_{i+1} \in P$, o_i elementi o_{i+1}-dən üstün tutulur.

İki oyunçunun oyununu $G_{A,D} = ([A, D], [T_A, T_D], [P_A, P_D])$ kimi təsvir etmək olar. Bu işarələrlə A və D-nin hiperoyunu $H(A, B) = \{p(A, G_{A,D}), p(D, G_{A,D})\}$ kimi müəyyən olunur, burada p funksiyası oyunçunun təsəvvür etdiyi (qavradığı) oyunu işarə edir. Məsələn, $p(D, G_{A,D})$ D-nin malik olduğu informasiya əsasında təsəvvür etdiyi oyunu işarə edir.

A-nın 2 hücum senarisi və D-nin 3 müdafiə mexanizminə malik olduğu hiperoyun üçün HYPANT[2] açıq kodlu proqram təminatı vasitəsilə ədədi eksperimentlər aparılmışdır.

E-dövlətin informasiya təhlükəsizliyinin situasiyalar üzrə idarə edilməsi üçün konseptual modeli işlənmiş və modelin presedentlər nəzəriyyəsi əsasında reallaşdırılması üçün yanaşma təklif edilmişdir

[2] http://users.monash.edu/~lbrumley/hyper.html

[15]. Təklif edilən konseptual modeldə e-dövlətin informasiya infrastrukturunu təşkil edən hər bir informasiya təhlükəsizliyi domenində domenin informasiya təhlükəsizliyi siyasəti əsasında informasiya təhlükəsizliyinin monitorinqi həyata keçirilir. İnformasiya təhlükəsizliyinin monitorinqinə şəbəkə və sistem aktivliyinin, istifadəçilərin davranışının, qorunan resurslara girişlərin, informasiya sistemlərinin fəaliyyətində nasazlıqların izlənilməsi və informasiya axınlarının məzmununun monitorinqi daxildir.

İnformasiya təhlükəsizliyi hadisələri haqqında məlumatlar informasiya təhlükəsizliyi domeninin lokal reyestrində qeydiyyata alınır və informasiya təhlükəsizliyi hadisələrinin vahid monitorinqi mərkəzinə – Milli İnformasiya Təhlükəsizliyi Mərkəzinə ötürülür (MİTM). MİTM bütün informasiya təhlükəsizliyi domenlərindən hadisələr haqqında məlumatları toplayır, onların emalını, analizini (aqreqasiya, korrelyasiya) və vizuallaşdırılmasını həyata keçirir. Bu verilənlərdən istifadə edərək MİTM informasiya təhlükəsizliyi situasiyasının tam mənzərəsini görür, situasiyanı analiz edir və informasiya təhlükəsizliyi hadisəsinin potensial təsirlərini təkcə bir domen səviyyəsində deyil, bir neçə qarşılıqlı əlaqəli informasiya təhlükəsizliyi domeni miqyasında da qiymətləndirməyə imkan verir. MİTM hadisənin emalı üçün uyğun üsulu informasiya təhlükəsizliyi hadisələrinin milli bazasından seçir və tövsiyə edilən həlləri müvafiq təhlükəsizlik domenlərinə ötürür. informasiya təhlükəsizliyi hadisələrinin milli bazası hadisələr və onların emalı üsulları haqqında mərkəzi biliklər bazasıdır, burada informasiya təhlükəsizliyi hadisələrinin emalı üzrə tədbirlərin şablonları da saxlanır. Təhlükəsizlik domenlərində MİTM-in tövsiyə etdiyi həll cari hadisəyə adaptasiya edilir və hadisənin emalı həyata keçirilir. Bu məqsədlə zəruri texniki resurslar ayrılır, texniki və digər mütəxəssislərdən (ekspertlərdən) və qərar qəbul edən şəxsdən ibarət emal qrupu təyin edilir. Hadisənin emalı gedişində emal qrupu adaptasiya olunmuş həllə zəruri dəyişikliklər edə bilər. Hadisənin emalından sonra hadisənin test edilmiş emalı üsulu informasiya təhlükəsizliyi hadisələrinin milli bazasına daxil edilir, hadisəni emal edən ekspertlər qrupu və qərar qəbul edən şəxslər haqqında məlumatlar da bazada saxlanılır.

Presedenti formal olaraq belə müəyyən etmək olar: p presedenti $\langle s, r, h, z \rangle$ kortejindən ibarətdir, burada $s \in S$ situasiyası ilə bağlı $r \in R$ qərarı $z \in Z$ qərar qəbul edən şəxsin rəhbərliyi altında $h \in H$ ekspertlər qrupu tərəfindən yerinə yetirilməsi əks olunur. e informasiya təhlükəsizliyi hadisəsini formal olaraq aşağıdakı şəkildə təsvir etmək olar:

$$e = (Etype, DT, ID, rb, sev, v_1, \ldots, v_n), \quad (42)$$

burada *Etype* – hadisənin növü, *DT* – hadisənin başvermə vaxtı və zamanı, *ID* – hadisənin aşkarlandığı mənbənin identifikatoru, rb – mənbəyə inam dərəcəsi, sev – hadisənin risk dərəcəsi, $v_1, \ldots, v_n$ – hadisənin təsviri üçün tələb edilən digər atributlar (məsələn, IP-ünvan, protokol və s.). Adətən, informasiya təhlükəsizliyi hadisələrinin təsvirinə mətn informasiyası da daxil olur, məsələn, hadisənin təzahürləri, xəbərdarlıq məlumatları və s. Bu verilənlərin təsviri və sorğuya uyğun insidentləri və uyğun emal prosedurlarını tapmaq üçün gizli semantik analiz (Latent Semantic Analysis, LSA) metodundan[3] istifadə edilməsi təklif olunur.

Ümumi halda, qərar dedikdə analoji situasiyalarda yerinə yetirilmiş hərəkətlər və onların nəticələri və ya verilmiş situasiyada yerinə yetiriləcək hərəkətlərin reqlamentləri və ya ekspert tövsiyələri və s. nəzərdə tutulur.

Qərarın tətbiqinin nəticəsinin təsvirinə hadisənin planlaşdırılmış və faktiki emal müddətləri, hadisənin nəticələrinin aradan qaldırılması üçün icra olunmuş hərəkətlər, hadisənin emalının nəticəsi, hadisənin qarşısını almaq üçün zəruri hərəkərlərin siyahısı daxil ola bilər. Nəticənin təsvirində digər hadisələrə (presedentlərə) istinadlar da ola bilər. Bu verilənlərin təsviri üçün də LSA metodu istifadə edilə bilər.

Verilmiş presedentə ən "yaxın" presedentin presedentlər bazasından seçilməsi geniş yayılmış yanaşmaya – əvvəlcədən təyin edilən yaxınlıq metrikaları əsasında klassifikasiya edən ən yaxın qonşular metoduna əsaslanır. Hər bir əlamətə onun nisbi vacibliyini əks etdirən çəki əmsalı verilir (məsələn, PSO (Particle Swarm Optimization) alqoritmi əsasında). Bütün əlamətlər üzrə iki

[3] Evangelopoulos, N. E. Latent semantic analysis // Wiley Interdisciplinary Reviews: Cognitive Science, – 2013, 4 (6), – p. 683-692.

presedentin yaxınlıq dərəcəsini müəyyən etmək üçün aşağıdakı düsturdan istifadə etmək olar:

$$sim(i,k) = \frac{\sum_{j=1}^{n} w_j \cdot sim(e_{ij}, e_{kj})}{\sum_{j=1}^{n} w_j}, \quad (43)$$

burada w_j – j-cu əlamətin çəkisidir; sim – yaxınlıq metrikasıdır; e_{ij} və e_{kj} – e_j əlamətinin uyğun olaraq cari i presedenti və k presedenti üçün qiymətləridir.

sim yaxınlıq metrikasının seçilməsi çox vacib məsələdir, çünki oxşar presedentlərin axtarışı əhəmiyyətli dərəcədə bu seçimdən asılıdır. İnformasiya təhlükəsizliyi hadisələrinin və uyğun emal qərarlarının yuxarıda verilmiş təsvirindən göründüyü kimi, presedentlərin əlamətlərinin bir hissəsi ədədi və nominal qiymətlər qəbul edir, digər hissəsi isə semantik vektorlarla kodlaşdırılan mətn verilənləri ilə təsvir edilir. Bunu nəzərə almaqla, heterogen məsafə funksiyasından[4] istifadə olunması təklif olunur.

Yeddinci fəsildə e-dövlətin informasiya təhlükəsizliyinin qiymətləndirilməsi modelləri və metodları tədqiq olunmuşdur.

E-xidmətlər e-dövlətin vətəndaşlarla və özəl sektorla əsas təmas xəttidir və e-xidmətlərin informasiya təhlükəsizliyinin səviyyəsi əsasında e-dövlətin informasiya təhlükəsizliyinin vəziyyəti və ümumiyyətlə, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin effektivliyi barədə fikir yürütmək mümkündür. E-xidmətlərin informasiya təhlükəsizliyi səviyyəsini qiymətləndirmək üçün aşağıdakı metod təklif edilir [20].

Fərz edək ki, e-xidmətin informasiya təhlükəsizliyi tələbləri m istiqamətdə (təhlükəsizlik servisləri üzrə) qruplaşdırılıb. Hər bir i-ci təhlükəsizlik servisi üçün xüsusi informasiya təhlükəsizliyi indikatorları müəyyənləşdirilir və suallar şəklində formalaşdırılır, suallara cavablar $M_{ij}, i = 1, \dots, m, j = 1, \dots, n$ qiymətlərini verir. Bu qiymətlər isə S_i qrup indikatorlarının qiymətləndirilməsini formalaşdırır.

Xüsusi indikatorlar aşağıdakı şkala ilə qiymətləndirilir:

0 – tələblər yerinə yetirilmir;

[4] Wilson, D., Martinez, T. Improved heterogeneous distance functions // Journal of Artificial Intelligence Research, – 1997, 6 (1), – p. 1-34.

0.25 – tələblər az dərəcədə yerinə yetirilir;
0.5 – tələblər müəyyən dərəcədə yerinə yetirilir;
0.75 – tələblər, demək olar ki, tam yerinə yetirilir;
1 – tələblər tam yerinə yetirilir.

Qrup indikatoru $S_i, i = 1,..,m$ xüsusi indikatorların müxtəlif çəkilərə malik olması halında aşağıdakı düsturla müəyyən edilir:

$$S_i = \sum_{j=1}^{n_j} \alpha_{ij} M_{ij}, \quad (44)$$

burada M_{ij} – i-ci təhlükəsizlik servisi üçün j-ci xüsusi indikatorunun qiyməti; α_{ij} – i-ci təhlükəsizlik servisi üçün j-ci xüsusi indikatorun çəkisidir. İndikatorların çəkiləri eyni olduqda $\alpha_{ij} = \frac{1}{n_i}, j = 1,\dots,n$ götürülür, burada n_i – i-ci təhlükəsizlik servisi üçün indikatorların sayıdır.

E-xidmətin informasiya təhlükəsizliyinin səviyyəsi (SL) ən zəif halqa qaydası ilə tapılır:

$$SL = \min_i S_i. \quad (45)$$

Mövcud kompozit indekslərdə onlara daxil olan fərdi indikatorların çəkiləri ya bərabər götürülür, ya da subyektiv təyin olunur. Bu nöqsanı aradan qaldırmaq üçün kompozit milli kibertəhkükəsizlik indekslərində indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi metodu təklif edilir, həmçinin statik və dinamik kibertəhlükəsizlik indeksləri daxil edilir [27].

Tutaq ki, m ölkənin kibertəhlükəsizlik səviyyəsinin n indikatora görə qiymətləndirilməsi matrisi $D = \left(x_{ij}\right)_{m\times n}$ verilib, burada x_{ij} – i-ci ölkənin j-cu indikatora görə qiymətləndirilməsidir. İndikatorların çəkilərini müəyyən etmək üçün entropiya alqoritmini aşağıdakı kimi ifadə etmək olar:

Addım 1. Qiymətləndirmə matrisinin normallaşdırılması. Nəticədə $R = \left(r_{ij}\right)_{m\times n}$ matrisi alınır, burada $r_{ij} \in [0,1]$ – j-cu ölkənin i-ci indikator üzrə qiymətləndirməsidir. Baxılan məsələdə indikatorun qiyməti böyük olduqca yaxşı hesab edilir, buna görə aşağıdakı normallaşdırma düsturu istifadə edilir:

$$r_{ij} = \frac{x_{ij} - \min\limits_{i}\{x_{ij}\}}{\max\limits_{i}\{x_{ij}\} - \min\limits_{i}\{x_{ij}\}}. \quad (46)$$

Addım 2. Entropiyanın hesablanması. *i*-ci indikatorun entropiyası aşağıdakı kimi müəyyən edilir:

$$H_j = -k \sum_{i=1}^{n} f_{ij} \ln f_{ij}, j = 1,2, \dots, m, \quad (47)$$

burada $f_{ij} = r_{ij} / \sum_{i=1}^{n} r_{ij}$, $k = 1/\ln n$. $f_{ij} = 0$ olduqda, $f_{ij} \ln f_{ij} = 0$ fərz olunur.

Addım 3. Entropiya çəkisinin müəyyən edilməsi. *j*-cu indikatorun entropiya çəkisi belə təyin edilir:

$$w_j = \frac{1 - H_j}{m - \sum_{j=1}^{m} H_j}, \quad (48)$$

burada $0 \le w_j \le 1, \sum_{j=1}^{m} w_j = 1$.

Cədvəl 4-də (47)-(49) düsturları ilə MDB ölkələrinin 2017-ci il üçün qlobal kibertəhlükəsizlik indekslərinə aid verilənlərin[5] əsasında hesablanmış indikatorların entropiyaları və çəkiləri verilmişdir. Göründüyü kimi, entropiya yanaşmasında "Texniki" və "Potensialın inkişafı" indikatorlarına daha yüksək çəkilər verilir.

Cədvəl 4. İndikatorların entropiya çəkiləri

İndikator	**Entropiya əsasında çəki**
Hüquqi	0.108
Texniki	0.273
Təşkilati	0.147
Potensialın inkişafı	0.296
Əməkdaşlıq	0.176

Tutaq ki, x_{ij}^{t} – *j*-cu indikatorun *i*-ci ölkə üçün *t* zamanında qiymətidir ($j = 1, \dots, m; i = 1, \dots, n; t = t_0, t_1$). Statik kibertəhlükəsizlik indeksini (Static Cybersecurity Index, SCI) aşağıdakı kimi təyin etmək olar:

$$SCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^t}{x_{rj}^t} \right)^{\frac{1}{m}}, \quad (49)$$

[5] GCI 2017 Regional Report: CIS Region Report, 2017, 36 p. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIS_GCIv2_report.pdf

burada x_{rj}^{t} – j-cu indikatorun t zamanında istinad (baza) qiymətidir, məsələn, indikatorun dünya üzrə orta qiymətidir.

Hər bir ölkə üçün t_0 anından t_1-ə aşağıdakı düsturla verilən "dinamik" kibertəhlükəsizlik indeksi (Dynamic Cybersecurity Index, DCI) qurmaq olar:

$$DCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^{t_1}}{x_{ij}^{t_0}} \right)^{\frac{1}{m}}. \quad (50)$$

E-dövlətin informasiya təhlükəsizliyi səviyyəsini qiymətləndirmək üçün əks-əlaqə ölçüsü kimi istifadəçilərin rəylərini nəzərə alan indikatorların işlənməsi də məqsədəuyğundur. Bu ideyanı həyata keçirmək üçün təklif edilən modeldə e-dövlətin informasiya təhlükəsizliyinə etimad vətəndaşın informasiya əldə etdiyi müxtəlif mənbələr əsasında qiymətləndirilir [19]:

- Şəxsi təcrübə (*I*);
- Sosial şəbəkə (qonşuların və dost-tanışların) rəyləri (*W*);
- KİV-lərdə ifadə olunan rəylər (*M*);
- Dövlət orqanlarının təqdim etdiyi sertifikat və öhdəliklər (*S*).

İnformasiya mənbələri (komponentlər) üzrə etimad qiymətləri bütün reytinqlərin çəkili ortası kimi hesablanır:

$$T_K(a, c) = \frac{\sum_{r_i \in R_K(a,c)} w_K(r_i) \cdot v_i}{\sum_{r_i \in R_K(a,c)} w_K(r_i)}, \quad (51)$$

burada $T_K(a, c)$ – a agentinin e-dövlətin informasiya təhlükəsizliyinə etimadının c faktoruna nəzərən K komponenti üzrə hesablanmış qiymətidir. $R_K(a, c)$ – K komponenti üzrə etimadı hesablamaq üçün toplanmış reytinqlər çoxluğudur. $w_K(r_i) \geq 0$ – r_i reytinqinin relevantlıq (etibarlılıq) dərəcəsini hesablamaq üçün reytinq çəki funksiyasıdır. v_i – r_i reytinqinin qiymətidir. Çəkilərin cəminə bölməklə etimad qiyməti $[-1, 1]$ diapazonuna normallaşdırılır. $w_K(r_i)$ reytinq çəki funksiyası hər bir komponent üçün ayrıca müəyyən olunur. Ümumi etimad qiyməti

$$T(a, c) = \frac{\sum_{K \in \{I,W,M,S\}} W_K \cdot T_K(a, c)}{\sum_{K \in \{I,W,M,S\}} W_K}, \quad (52)$$

kimi hesablanır, burada W_K baxılan məsələ üçün komponentlərin vacibliyinə uyğun seçilmiş çəki əmsallarıdır.

Dissertasiya işinin **nəticələrində** dissertasiya işində qoyulmuş məsələlərin həlli zamanı əldə olunmuş əsas elmi-nəzəri və elmi-praktiki nəticələri göstərilmişdir:

1. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi problemlərinin müasir vəziyyəti analiz və tədqiq edilərək bu sahədə aktual multidissiplinar elmi-nəzəri və elmi-praktiki problemlər müəyyən edilmişdir [1, 2, 3, 5, 8]. Bu nəticə informasiya təhlükəsizliyi sahəsində gələcək elmi-praktiki tədqiqatların planlaşdırılması və təşkili və müvafiq təhsil pilləsi üçün resursların yaradılması üçün sistemləşdirilmiş informasiya bazası kimi əhəmiyyətlidir.
2. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə konseptual model [9] və e-dövlətin informasiya təhlükəsizliyi sisteminin konseptual arxitekturası [6] təklif edilmişdir. Nəticənin elmi-praktiki əhəmiyyəti e-dövlətin informasiya təhlükəsizliyi sisteminin arxitekturasının və strukturunun təkmilləşdirilməsi üçün konseptual əsaslar yaratmasıdır.
3. İnformasiya sahəsində milli maraqlara strateji risklərin konsensus ranqlaşdırılması metodu işlənmiş [28, 21], qarşılıqlı asılı kritik informasiya infrastrukturlarında risklərin qiymətləndirilməsi metodu [31, 13] və İnternet infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri [30] təklif edilmişdir. Nəticənin elmi-praktiki əhəmiyyəti informasiya təhlükəsizliyinin təmin edilməsi üzrə strateji planlaşdırma və kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin edilməsi üzrə əsas istiqamətlərin müəyyən edilməsi üçün təklif edilən yanaşmalarla şərtlənir.
4. E-dövlətin biometrik identifikasiya sistemi üçün biometrik sistemlərdə informasiyanın aqreqasiyası metodu [4] və barmaq izlərinin həqiqiliyinin aşkarlanması metodu [7] təklif edilmiş və barmaq izlərinin tekstur deskriptorları əsasında biometrik kriptosistemlərin sintezi metodu [10] işlənmişdir. Nəticənin elmi-praktiki əhəmiyyəti elektron identifikasiya (o cümlədən, e-pasport) sistemləri üçün yeni xidmətlər və məhsullara imkan yaradan texniki konsepsiyanın eksperimental isbatıdır.

5. İnformasiya təhlükəsizliyi insidentlərinin aşkarlanması metodu [24] işlənmiş, insidentlərin çoxmeyarlı prioritetləşdirilməsi metodu [12] və insidentlərin emalı üzrə işlərin optimal planlaşdırılması metodu [29] təklif edilmişdir. Nəticənin praktiki əhəmiyyəti milli CERT sisteminin təkmilləşdirilməsi və müvafiq xidmətlərin təşkilində metodoloji baza təklif etməsi ilə əsaslanır.
6. E-dövlətin informasiya təhlükəsizliyi sahəsində koordinasiya səviyyəsinin qiymətləndirilməsi modeli [32, 16], informasiya təhlükəsizliyinin ikisəviyyəli iyerarxik idarəetmə sistemində investisiyaların koordinasiyası modeli [25] işlənmiş, beynəlxalq koalisiyaların formalaşdırılması modeli [33, 17] təklif edilmişdir. Nəticənin elmi-praktiki əhəmiyyəti informasiya təhlükəsizliyinin təmin edilməsinə cəlb edilmiş və müxtəlif maraqlar güdən tərəflərin fəaliyyətini səmərəli əlaqələndirməyə imkan verəcək iqtisadi əsaslı yanaşmaların təklif edilməsidir.
7. E-dövlətin informasiya təhlükəsizliyinin strateji idarə edilməsi üçün qeyri-səlis koqnitiv model [18], kibermüdafiə taktikasının seçilməsi üçün hiperoyun modeli [11] və operativ idarəetmə üçün situativ idarəetmə modeli [15] təklif edilmişdir. Nəticənin elmi-praktiki əhəmiyyəti təklif edilmiş modellərin idarələrarası informasiya təhlükəsizliyi şuraları və situasiya mərkəzləri üçün konkret prosedurlar şəklində reallaşdırıla bilməsi imkanı ilə şərtlənir.
8. E-xidmətlərin informasiya təhlükəsizliyi səviyyəsinin qiymətləndirilməsi metodu [20], kompozit statik və dinamik kibertəhlükəsizlik indekslərində çəkilərin qiymətləndirilməsi metodu [27] və e-dövlətin informasiya təhlükəsizliyinə vətəndaş etimadının qiymətləndirilməsi modeli [19] işlənmişdir. Nəticənin praktiki əhəmiyyəti informasiya təhlükəsizliyi üzrə milli statistik hesabatlılıq sisteminin formalaşdırılması və müxtəlif statistik analizlərin aparılmasında tətbiqi imkanları ilə əsaslanır.

Dissertasiyanın əsas müddəaları aşağıdakı elmi işlərdə dərc edilmişdir:

1. İmamverdiyev, Y. N. Etibarlı və təhlükəsiz elektron hökümət yaradılmasının bəzi məsələləri // **Proc. of the 1st International**

Conference "Problems of Cybernetics and Informatics", – Baku: – 26-28 October, – 2006, – c. 2, – p. 80-82.
2. Abdullayeva, F., Imamverdiyev, Y., Musayev, V., Wayman, J. Analysis of security vulnerabilities in biometric systems // **Proc. of the 2nd International Conference "Problems of Cybernetics and Informatics",** – Baku: – 10-12 September, –2008, – p. 60-63.
3. Alguliev R., Imamverdiyev Y. E-government information security management research challenges // **IEEE International Conference on Application of Information and Communication Technologies (AICT),** – Baku: – 14-16 October, – 2009, – p.1-5. **(Scopus)**
4. Imamverdiyev, Ya. N. A model of fusion of information on image quality based on the Dempster-Shafer theory for biometric systems interoperability // – Redding (USA): **Journal of Automation and Information Sciences**, – 2010. 42(2), – p. 66-74. **(Web of Science; Impact Factor: 0.024)**
5. Əliquliyev, R.M., İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyi: Aktual tədqiqat istiqamətləri // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2010. №1, – s. 3-13.
6. Imamverdiyev Y. Architecture of e-government information security management system // **Proc. of the 3rd International Conference "Problems of Cybernetics and Informatics",** – Baku: – 6-9 September, – 2010, – p.79-82.
7. Имамвердиев, Я.Н. Метод обнаружения переделанных отпечатков пальцев на основе фрактальных характеристик // – Москва: **Информационные технологии**, – 2012. № 9, – с. 11-16.
8. İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatların müasir vəziyyətinin analizi // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2012. № 2, – s. 19-26.
9. İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2013. № 1, – s. 20-31.
10. Imamverdiyev, Y., Teoh, A., Kim, J. Biometric cryptosystem based on discretized fingerprint texture descriptors // **Expert**

Systems with Applications, – 2013. 40, – p.1888–1901. **(Web of Science, Impact Factor: 4.292)**
11. Imamverdiyev, Y. A hypergame model for information security // **6th International Conference on Information Security and Cryptology (ISCTurkey)**, – Ankara: – 20-21 September, – 2013, – p. 65-70.
12. Imamverdiyev, Y. An information security incident prioritization method // **IEEE 7th International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 23-25 October, – 2013, – p.183-187. **(Web of Science)**
13. Imamverdiyev, Y. An application of extreme value theory to e-Government information security risk assessment // **IEEE 7th International Conference on Application of Information and Communication Technologies (AICT),** – Baku: – 23-25 October, – 2013, – p.349-352. **(Web of Science)**
14. İmamverdiyev, Y.N. Yeni nəsil milli kibertəhlükəsizlik strategiyaları // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2013. № 2, – s. 42-51.
15. Имамвердиев, Я.Н. Модель ситуационного управления информационной безопасностью электронного правительства // – Москва: **Информационные технологии**, – 2014. №8, – с. 24-33.
16. İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya problemləri // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2014. № 2, – s. 24-30.
17. Musayev, V.Y., İmamverdiyev, Y.N. İnformasiya təhlükəsizliyi sahəsində beynəlxalq çağırışlar, təşəbbüslər və öhdəliklər // **İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** – Bakı: – 17-18 may, – 2015, – s. 102-105.
18. Имамвердиев, Я.Н. Нечеткая когнитивная модель стратегического управления информационной безопасностью электронного правительства // – Москва: **Информационные технологии**, – 2015. №6, – с. 440-447.
19. Imamverdiyev, Y. E-government information security trust assessment model // – (India) **International Journal of Research**

Studies in Computer Science and Engineering, – 2016. 3(2), – p. 1-6.
20. Imamverdiyev, Y. E-services security assessment model // **IEEE 10th International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 12-14 October, – 2016, – p. 595-598. **(Web of Science)**
21. Imamverdiyev, Y.N. Consensus ranking method of information security threats of a nation state // **II Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології"** ("Information Security and Computer Technologies"), – Kropyvnytskyi: – 20-22 April, – 2017, p. 12-13.
22. İmamverdiyev, Y.N. İnformasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması problemləri // **İnformasiya təhlükəsizliyi üzrə III respublika elmi-praktiki seminarı,** – Bakı: – 08 dekabr, – 2017, – s. 77-80.
23. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. Cyber-physical systems and their security issues // – Amsterdam: **Computers in Industry**, – 2018. 100, – p. 212–223. **(Web of Science; Impact Factor: 4.769)**
24. Imamverdiyev, Y., Abdullayeva, F. Deep learning method for denial of service attack detection based on restricted Boltzmann machine // – (New Rochelle, NY, USA) **Big Data**, – 2018. 6(2), – p. 1-17. **(Web of Science, Impact Factor: 2.106)**
25. Имамвердиев, Я.Н. Модель координации инвестиций в двухуровневых иерархических системах управления информационной безопасностью // – Москва: **Экономическая безопасность и качество**, – 2018. №3 (32), – с. 41-47.
26. İmamverdiyev, Y.N. APT (Advanced Persistent Threat)-hücumların aşkarlanması üçün konseptual yanaşma // – Bakı: **Milli təhlükəsizlik və hərbi elmlər**, – 2018. №1 (4), – s. 93-103.
27. İmamverdiyev, Y.N. Milli kiber-təhlükəsizlik üçün entropiya çəkiləri və dinamik indeks // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2018. №2, – s.16-27.
28. İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyi təhdidlərinin konsensus ranqlaşdırılması metodu // – Bakı:

İnformasiya texnologiyaları problemləri, – 2018. №2, – s. 34-45.
29. İmamverdiyev, Y.N. İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərinin optimal planlaşdırılması modeli // – Bakı: **İnformasiya texnologiyaları problemləri**, – 2018. №2, – s. 80-91.
30. Имамвердиев, Я.Н. Модели оценки живучести национальной инфраструктуры Интернета // – Москва: **Телекоммуникации**, – 2018. №12, – с.36-45.
31. Имамвердиев, Я.Н. Метод оценки рисков информационной безопасности в взаимосвязанных информационных инфраструктурах // – Орел: **Информационные системы и технологии**, – 2019. № 1 (111), – с. 102-112.
32. İmamverdiyev, Y.N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi modeli // – Bakı: **İnformasiya texnologiyaları problemləri,** – 2019. № 1, – s. 47-58.
33. İmamverdiyev, Y.N. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiya modeli // – Bakı: **İnformasiya cəmiyyəti problemləri**, – 2019. № 1, – s. 14-20.

Həmmüəlliflərlə dərc olunmuş işlərdə iddiaçının şəxsi rolu:

[2] – biometrik sistemdə modullar üzrə boşluqların analizi aparılmışdır;

[3] – mövzu üzrə aktual tədqiqat istiqamətləri analiz edilmişdir;

[5] – tədqiqatın metodikası işlənmiş və aktual istiqamətlər araşdırılmışdır;

[10] – biometrik kriptosistemin arxitekturası və komponentləri işlənmiş, effektiv həllin tapılması üzrə eksperimentlər aparılmışdır;

[17] – tədiqat metodikası işlənmiş və beynəlxalq təcrübə analiz edilmişdir;

[23] – hücum vektorları ağacı modeli təklif edilmişdir;

[24] – məsələnin qoyuluşu və tədqiqat metodikası iddiaçıya məxsusdur.

Dissertasiyanın müdafiəsi **27 may 2021**-ci il tarixində saat **14^{00}**-da Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunun nəzdində fəaliyyət göstərən ED 1.35 Dissertasiya şurasının iclasında keçiriləcək.

Ünvan: AZ1141, Bakı şəhəri, B. Vahabzadə küç., 9A.

Dissertasiya ilə Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunun kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunun rəsmi internet saytında yerləşdirilmişdir.

Avtoreferat **23 aprel 2021**-ci il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb: 22.04.2021
Kağızın formatı: $60 \times 80\ ^{1}/_{16}$
Həcm: 79083 simvol
Tiraj: 100 nüsxə