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

Elmlər doktoru
elmi dərəcəsi almaq üçün təqdim olunmuş

DİSSERTASİYA

İddiaçı: texnika üzrə fəlsəfə doktoru, dosent
_____ Yadigar Nəsib oğlu İmamverdiyev

Elmi məsləhətçi: AMEA-nın həqiqi üzvü, tex.e.d., professor
_____ Rasim Məhəmməd oğlu Əliquliyev

Bakı – 2021

MÜNDƏRİCAT

səh.

GİRİŞ

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 dövlət siyasətinin formalaşdırılması və reallaşdırmasına vətəndaşlar daha geniş cəlb edilir, dövlətin, özəl sektorun və vətəndaş cəmiyyətinin arasında qarşılıqlı təsirin və əməkdaşlığın effektiv sistemi qurulur, dövlət idarəçiliyinin səmərəliliyi və göstərilən xidmətlərin keyfiyyəti yüksəlir. Son on ildə dünyanın bir çox ölkəsində e-dövlətə keçid üzrə bir sıra milli və beynəlxalq proqramlar yerinə yetirilir [288, s. 13-44].

Lakin e-dövlət quruculuğu sahəsində öz həllini gözləyən bir sıra ciddi problemlər də vardır. E-dövlət ideyasının həyata keçirilməsində müəyyən mərhələləri arxada qoymuş ölkələrin təcrübəsi sübut edir ki, e-dövlət quruculuğunda qarşıya çıxan əsas və ən çətin məsələlərdən biri yeni şəraitdə fəaliyyət göstərən dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsidir [303, s.350, 247, s.65, 117, s. 98]. İnformasiya təhlükəsizliyi e-dövlətin effektivliyinə və vətəndaşların dövlətə inamına birbaşa və həlledici təsir edir.

Aydındır ki, ölkənin informasiya cəmiyyəti mərhələsinə keçməsi onun informasiya və kommunikasiya sistemlərindən və informasiya texnologiyalarından asılılığını daha da gücləndirir. İKT-nin geniş tətbiqi bəşəriyyətin inkişafını sürətləndirməklə yanaşı milli, regional və qlobal təhlükəsizliyə yeni təhdidlər də yaradır, onları aşağıdakı kimi xarakterizə etmək olar [7, s.3, 19, s.19]:

1) Dövlətlərarası ziddiyyətlər və münaqişələr kiberfəzaya keçir və bu fəzada informasiya müharibəsi əməliyyatlarının aparılması ilə peşəkar şəkildə məşğul olan kiber-qoşunlar formalaşdırılır. İnformasiya əməliyyatları müasir

silahlı qüvvələrin hərbi doktrinalarında artıq özünə yer tapmaqdadır [24, s.15].

2) İnformasiya fəzası transmilli xarakteri daşıyır, bu qlobal informasiya infrastrukturunda milli komponenti ayırmağa imkan vermir, eyni zamanda informasiya-kommunikasiya sistemləri qloballaşır və milli səviyyədə nəzarətdən çıxır. Eləcə də informasiya texnologiyalarının, sistemlərinin və proqram təminatının yaradılması tədricən transmilli səviyyəyə qalxır. İKT məhsulları bazarında bir neçə ölkə şirkətlərinin inhisarçı vəziyyətində olması müəyyən siyasi məqsədlərin əldə edilməsi üçün istifadə edilə bilər. Həmçinin kütləvi informasiya vasitələrinin beynəlxalq inhisara alınması və ictimai şüurla manipulyasiya edilməsi də güclənir.
3) Qlobal informasiya-kommunikasiya şəbəkələrində səhvlər və ya qəzalar nəticəsində fəlakətlərin yeni növü – infogen fəlakətlər meydana çıxır.
4) 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.
5) Kibercinayətkarlığın yeni növləri yaranır, fərdi məlumatların cinayətkar məqsədlər üçün toplanması geniş vüsət alır, mütəşəkkil kibercinayətkarlıq inkişaf edir. Cinayətkar və terrorçu təşkilatlar çətin nəzarət edilən qlobal informasiya infrastrukturları yaradırlar, ən yüksək ixtisaslı kadrları işə cəlb etmək, elmi-tədqiqatlara və layihə-konstruktor işlərinə böyük həcmdə investisiyalar yatırmaq imkanları vardır.
6) Beynəlxalq təhlükəsizlik təhdidlərinin transformasiyası ilə əlaqədar yeni müharibə konsepsiyaları – "asimmetrik müharibə", "şəbəkə müharibəsi" və "dövlətsiz müharibə" konsepsiyaları meydana çıxır [7, s.3]. Asimmetrik təhdidlərin aktorları qeyri-ənənəvi, lakin təsirdə geri qalmayan yanaşmalardan istifadə edirlər, informasiya təhlükəsizliyinin təmin edilməsinə ənənəvi yanaşmalar belə aktorlara qarşı tamamilə səmərəsiz ola bilər, onlara qarşı tamamilə yeni əks-tədbir strategiyası tələb edilir.

7) Kiberhücumlar daha mürəkkəb, məqsədyönlü, və irimiqyaslı olur və milli informasiya infrastrukturunun kritik elementlərini tez-tez təhdid edir [272, s. 54]. Bu hücumların əsas hədəfləri dövlət orqanları, biznes strukturları və onların vəzifəli şəxsləri, ictimai-siyasi təşkilatlar, fərdlərdir. Eyni zamanda, dövlət orqanlarına və siyasi aktorlara qarşı siyasi motivli hücumlar da artır. Belə kiberhücumların qarşısının uğurla alınması ayrı-ayrı təşkilatların gücü xaricindədir, özəl sektor və cəmiyyət də daxil olmaqla bütün maraqlı tərəflərin arasında sıx əməkdaşlığı tələb edir.

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 [53, s.24]. Buna görə e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi sisteminin idarə edilməsi aktualdır.

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

Ölkədə informasiya cəmiyyətinin, e-hökumətin və e-dövlətin qurulması, informasiya təhlükəsizliyinin etibarlı təmin edilməsi Azərbaycan Respublikasında dövlət siyasətinin prioritet istiqamətlərindəndir [1, 3, 5]. Ölkəmizdə informasiya təhlükəsizliyi sahəsində dövlət siyasətinin həyata keçirilməsi istiqamətində normativ və hüquqi bazanın təkmilləşdirilməsi, informasiya təhlükəsizliyinin təmin edilməsi sisteminin təşkilati strukturunun formalaşdırılması [6], informasiya təhlükəsizliyi siyasətinin işlənməsi, informasiya təhlükəsizliyi sahəsində kadr hazırlığı, elmi-tədqiqat işləri üzrə bir sıra tədbirlər sistemli şəkildə müvafiq dövlət qurumları tərəfindən həyata keçirilir [12, s.3, 31].

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 kiber-müdafiə mexanizmləri yenilənir. Meydana çıxan yeni

təhlükəsizlik 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-dövlərin informasiya təhlükəsizliyinin idarə edilməsinin elmi-metodoloji əsaslarının işlənməsi məsələlərinə həsr edilmişdir.

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

Tədqiqat obyekti e-dövlətin informasiya təhlükəsizliyi, **tədqiqatın predmeti** e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi proseslərinin idarə edilməsinin model və metodlarıdır.

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

- e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modelinin və arxitekturasının 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 məntiq, oyunlar nəzəriyyəsi, ehtimal nəzəriyyəsi, kombinator optimallaşdırma, qraflar nəzəriyyəsi, sosial şəbəkə analizi, maşın təlimi metodları istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar:

- e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli;
- informasiya sahəsində milli maraqlara təhdidlərin konsensus ranqlaşdırılması metodu;
- e-dövlətin qarşılıqlı asılı infrastukturunda risklərin qiymətləndirilməsi metodu;
- milli İnternet infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri;
- biometrik sistemlərin tanıma göstəricilərinin və təhlükəsizliyinin təkmilləşdirilməsi metodları;
- informasiya təhlükəsizliyi insidentlərinin aşkarlanması, prioritetləşdirilməsi və emalının optimal planlaşdırılması metodları;
- 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;

- informasiya təhlükəsizliyi insidentlərinin dərin təlim əsasında aşkarlanması, çoxmeyarlı prioritetləşdirilməsi və emalının optimal planlaşdırılması üçün metodların işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin ikisəviyyəli iyerarxik idarəetmə sistemində investisiyaların koordinasiyası modelinin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması modelinin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin strateji, taktiki və operativ səviyyələrdə idarə edilməsi üçün riyazi və konseptual modellərin işlənməsi;
- e-dövlətin informasiya təhlükəsizliyinin e-xidmətlər, kibertəhlükəsizlik və vətəndaş etimadı üzrə qiymətləndirilməsi modellərinin işlənməsi.

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

- milli kibertəhlükəsizlik strategiyası 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 mərkəzində.

İşin nəticələrinin reallaşdırılması və tətbiqi. Əsas nəticələr 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" mövzusu 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 və bir sıra digər təşkilatların kompüter şəbəkələrinin 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;
- 6th International Conference on Information Security and Cryptology (ISCTurkey), 2013;
- İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 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.

Müəllif müxtəlif işçi qruplarının tərkibində informasiya təhlükəsizliyi üzrə normativ-hüquqi sənədlərin işlənməsində və icrasında bilavasitə iştirak etmişdir.

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

Dissertasiya işinin yerinə yetirildiyi təşkilatın adı: Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutu.

İşin strukturu və həcmi. Dissertasiya işi girişdən, 7 fəsildən, nəticədən, 313 adda ədəbiyyat siyahısından ibarətdir. İşin əsas məzmunu 40 şəkil və 45 cədvəl daxil olmaqla 246 səhifədə şərh edilmişdir.

Dissertasiyanın işarə ilə ümumi həcmi: 518667 işarə.

Dissertasiyanın struktur bölmələrinin ayrılıqda həcmi:

Titul səhifəsi – 574 işarə

Mündəricat – 5180 işarə.

Giriş – 13995 işarə.

Dissertasiyanın əsas məzmunu (fəsil, paraqraf, bənd) – 411791 işarə.

Nəticə – 3836 işarə.

İstifadə edilmiş ədəbiyyat siyahısı – 59637 işarə.

İxtisarların və şərti işarələrin siyahısı – 2490 işarə.

I FƏSİL. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ PROBLEMLƏRİ

E-dövlətin İnT-nin idarə edilməsi olduqca mürəkkəb məsələdir və çətin formallaşdırılan məsələlər sinfinə aiddir [109, s.315, 7, s.3]: 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 (sosial, texnoloji, siyasi, hüquqi və s.) baş verir, onlar arasında olduqca mürəkkəb səbəb-nəticə əlaqələri mövcuddur. Proseslərin xarakteri zamana görə dəyişir və proseslərin dinamikası haqqında kifayət qədər kəmiyyət informasiyası yoxdur, qeyri-müəyyənliyin müxtəlif növləri iştirak edir və s.

Çətin formallaşdırılan belə mürəkkəb məsələlərin həllində ilkin mərhələ kimi konseptual (latınca *conceptus* – anlayış) modelin qurulması çox faydalıdır [18, s.20]. Konseptual modellər sistemin dinamikası haqqında bilikləri inteqrasiya etməyə, əsas prosesləri identifikasiya etməyə, proseslərin vəziyyətləri və identifikatorları arasında əlaqələri göstərməyə, mürəkkəb qarşılıqlı əlaqələrdə koordinasiyanı sürətləndirməyə imkan verir.

Konseptual modellərin bu imkanlarından çıxış edərək, bu fəsildə e-dövlətin İnT-nin idarə edilməsinin konseptual modeli qurulur [18, s. 20] və qurulmuş konseptual modeldə müəyyən edilən idarəetmə funksiyaları əsas götürülməklə e-dövlətin İnT sahəsində elmi-tədqiqatların müasir vəziyyəti tədqiq və analiz edilir [7, s. 3, 19, s. 19]. Nəhayət, dissertasiya işində araşdırılacaq e-dövlətin İnT-nin idarə edilməsinin aktual elmi-praktiki problemləri müəyyən edilir [7, s. 3].

1.1. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli

Bu bölmədə təqdim olunan e-dövlətin İnT-nin idarə edilməsinin konseptual modelində [18, s. 20] e-dövlətin İnT-nin mahiyyəti, idarəetmənin məqsədləri, predmeti, obyektləri, subyektləri, prinsipləri, funksiyaları, e-dövlətin İnT-ni idarəetmə sisteminin tərkibini və strukturunu müəyyən edən əsas faktorlar. Qeyd etmək zəruridir ki, təklif edilən model İnT-nin hüquqi, siyasi, hərbi, sosial, iqtisadi və

s. problemlərin bütün aspektlərini əhatə etməyə cəhd etmir. Onun əsas məqsədi – e-dövlətin fəaliyyətinin üsul və vasitələri çərçivəsində reallaşdırılan İnT sisteminin əsas elementlərini – altsistemlərini aşkarlamaqdır.

1.1.1. Konseptual modelin əsas konseptləri

"Elektron dövlət" anlayışı

Analiz göstərir ki, hələlik elmi ədəbiyyatda "elektron dövlət" və "informasiya təhlükəsizliyi" anlayışlarının müəyyən edilməsində vahid yanaşma formalaşmayıb.

Qeyd edək ki, rusdilli elmi ədəbiyyatda ingilisdilli "electronic government" (e-government) anlayışının "elektron hökumət" kimi tərcüməsi geniş yayılıb. Lakin ingilis dilində "government" termini ilə yalnız icra hakimiyyəti orqanı kimi hökumət deyil, bütövlükdə dövlət (dövlət idarəçiliyi) nəzərdə tutulur. Məsələn, Avropa İttifaqının Komissiyası "electronic government" terminini «*xidmətlərin və demokratik proseslərin yaxşılaşdırılması və dövlət siyasəti üçün dəstəyin möhkəmləndirilməsi üçün İKT-nin dövlət idarəetməsində təşkilati dəyişikliklər və yeni vərdişlərlə əlaqələndirməklə istifadəsi*» kimi müəyyən edir [40, s. 5].

"Elektron dövlət" texnologiyasının tətbiqi dünyada 1990-cı illərdə dövlət idarəçiliyin islahatlarından başlayır. E-dövlətin məqsədi İKT istifadə edilməklə dövlət sektoru təşkilatlarının işini yaxşılaşdırmaqdır. İslahatların siyasi motivasiyası dövlətə cəmiyyətə xidmət edən və cəmiyyətin özü üçün zəruri səlahiyyətləri icra etməyi tapşırdığı institut kimi baxan konsepsiyanın yaranmasına şərait yaradır [40, s. 5]. Beləliklə, "e-government" anlayışı "elektron dövlət idarəçiliyi"ni bildirir və İKT-nin yalnız icra orqanlarında deyil, hakimiyyətin qanunvericilik və idarəetmə qollarında da tətbiqini əhatə edir.

Müxtəlif müəlliflər e-dövlət üçün: "şəbəkələrarası dövlət", "*biznes tranzaksiyalarını onlayn yerinə yetirməkdən ötrü vətəndaşlar, dövlət qulluqçuları və digər maraqlı tərəflər üçün xərclər baxımından effektiv modellərin reallaşdırılması*", "*strategiya, proses, təşkilat və texnologiyanı inteqrasiya edən konsepsiya*" [299, s. 70] və s. kimi fərqli təriflər təklif edirlər.

Palvia və Sharma e-dövlətin müxtəlif təriflərini analiz edərək onu m-dövlət (dövlət xidmətlərinin göstərilməsi üçün simsiz texnologiyalardan istifadə) və e-idarəçilikdən (idarəetmənin təkmilləşdirilməsi məqsədi ilə dövlət və özəl sektor tərəfindən İKT-nin istifadəsi) fərqləndirirlər [251, s.1-12].

BMT-yə görə "*e-dövlət insanlara informasiyanın və dövlət xidmətlərinin təqdim edilməsi üçün dövlət tərəfindən İKT-nin istifadəsi və tətbiqidir. Bu səbəbdən, e-dövlətin məqsədi vətəndaşlara informasiya xidmətlərinin effektiv dövlət idarəetməsi, vətəndaşlara daha yaxşı xidmətlər təqdim edilməsi, informasiyaya çıxış və dövlət siyasətinin qəbulunda iştirak yolu ilə insanlara səlahiyyət verilməsidir*" [188, s. 78].

Dünya Bankının tərifində "*e-dövlət dövlət agentlikləri tərəfindən vətəndaşlarla, özəl sektorla və dövlətin digər qolları ilə münasibətləri transformasiya etmək imkanı olan texnologiyaların istifadəsi*" kimi müəyyən edilir [155, s. 718].

Başqa tərifl ərdə e-dövlət məhsuldarlığı və səmərəliliyi artırmaq üçün vətəndaşlar və kommersiya institutları arasında informasiya, xidmətlər və malların mübadiləsində informasiya texnologiyalarından istifadə edən dövlət modeli kimi müəyyən edilir [18, s.20]. Daha geniş mənada e-dövlət daha yaxşı dövlət strukturunun yaradılmasına çalışır, bu o deməkdir ki, e-dövlət "e" üzərində yox, daha çox "dövlət"də fokuslanır [169, s. 6]. Oxşar şəkildə "e-dövlət" anlayışı ənənəvi dövlət modelindən daha inkişaf etmiş və daha güclü IT potensiala və əlaqələrə əsaslanan "daha yaxşı dövlət strukturunu" bildirir.

Richard Heeks "e-idarəçilik" terminini təklif edir, bu bütün İKT-ni əhatə etməlidir, lakin əsas innovasiyalar intranetdən İnternet-ə kimi kompüter şəbəkələrinə, yeni rəqəmsal birləşmələr yaradan hissəsinə aiddir. Heeks fərz edir ki, e-idarəçiliyin fokusu e-idarəçilik hissələrindən e-vətəndaşlar, e-xidmətlər və e-cəmiyyətə doğru dəyişir [162, s. 1].

"Virtual dövlət" termini siyasi elmlər üzrə alim Jane E. Fountain tərəfindən informasiya texnologiyalarının təsiri nəticəsində dövlət və təşkilatların təbiətində baş verən fundamental dəyişiklikləri ifadə etmək üçün daxil edilmişdir. Fountain qeyd edir ki, "*Virtual dövlət termini, rəqəmsal informasiya və kommunikasiya sistemləri ilə daha da dərinləşən dövlət strukturlarına və proseslərinə diqqəti cəlb etmək üçün*

nəzərdə tutulmuş bir metafordur. Verilənlərin və kommunikasiyaların rəqəmsallaşması dövlət institutlarına verilənlərin mənbəyi, qərarların qəbul edilməsi, xidmətlər və proseslərinə təkcə hökumət təşkilatlarını deyil, qeyri-kommersiya və özəl təşkilatları da qoşmaq üçün bu məsələləri yenidən nəzərdən keçirməyə imkan verir" [142, s. 149].

"Elektron hökumət", "elektron dövlət" və "informasiya cəmiyyəti" anlayışları arasında münasibətlərin araşdırılması da maraqlı mövzudur [40, s.5]. Müəllif nəticəyə gəlir ki, "*informasiya cəmiyyəti və dövlət onun geosiyasi aspektində üst-üstə düşürlər. …İnformasiya cəmiyyəti və elektron dövlət eynitərtibli anlayışlardır*" [40, s. 5].

XXI əsrin başlanğıcında ictimai proseslərin artmaqda olan riskləri və qeyri-müəyyənliyi şəraitində dövlət idarəçiliyində islahatlar inzibati aparatın işinin optimallaşdırılması və xidmətlərin göstərilməsindən tədricən vətəndaşların dövlət siyasətinin işlənməsinə və həyata keçirilməsinə cəlb edilməsinə, dövlət və vətəndaş cəmiyyətinin daha effektiv qarşılıqlı əlaqə sisteminin qurulmasına, dövlətin özəl sektor və qeyri-hökumət təşkilatları ilə əməkdaşlığının təmin edilməsinə yönəlir. E-dövlət ona elektron demokratiyanın qoşulması ilə zənginləşir. E-dövlətin G2C (vətəndaşlara xidmətlər), G2B (government to business – biznesə xidmətlər) və G2G (inzibati sistemin effektivliyi) kimi ilkin blokları ilə yanaşı yeni C2C bloku – şəbəkə vətəndaş cəmiyyəti meydana çıxmağa başlayır.

"E-dövlətin informasiya təhlükəsizliyi" anlayışı

Anlayışın düzgün, dəqiq və tam müəyyən edilməsinin həm nəzəri, həm də praktiki əhəmiyyəti vardır. "E-dövlətin informasiya təhlükəsizliyi" anlayışının dəqiq və tam açılması infomasiya təhlükəsizliyinin vəziyyətini düzgün qiymətləndirməyə, bu sahədə siyasəti düzgün qurmağa, təşkilatlanmağa, resursları qiymətləndirməyə və müvafiq potensialı inkişaf etdirməyə, beynəlxalq əməkdaşlığın prioritetlərini müəyyənləşdirməyə imkan verir.

İnformasiya təhlükəsizliyi kifayət qədər mürəkkəb və geniş anlayışdır, onun vahid, birmənalı elmi tərifi yoxdur [45, s. 68]. "İnfomasiya təhlükəsizliyi" anlayışı

müxtəlif müəlliflər tərəfindən müxtəlif cür müəyyən edilir, bu terminlər bir-biri ilə uzlaşmırlar və metodoloji işin nəzəri əsaslandırılması üçün yararsız olurlar. M. Styuqin [67, s. 102]-da infomasiya təhlükəsizliyinin nəzəri əsaslarını tədqiq edən müəlliflərdən birinin – Moskva Dövlət Universiteti, informasiya təhlükəsizliyi kafedrasının dosenti Q. V. İvaşşenkonun yekun fikrini iqtibas gətirir [67, s. 102]: "*Təhlükəsizlik sahəsində müasir nəşrlərin əhəmiyyətli hissəsi predmeti sistemsiz və səthi təsvir edir. Onların müəllifləri tez-tez ideallaşdırmağa, mif yaratmağa meyl edirlər, mövcud olanın izahından arzuolunanın izahına keçirlər*."

İnfomasiya təhlükəsizliyinin predmeti çox zaman infromasiyanın konfidensiallığnın, tamlığının və əlyetənliyinin təmin edilməsi kimi başa düşülür. Lakin infomasiya təhlükəsizliyinin predmeti daha genişdir. İnformasiya təhlükəsizliyi təkcə kompüter təhlükəsizliyindən və şəbəkə təhlükəsizliyindən ibarət deyil. Müasir cəmiyyətdə İnT cəmiyyətin bütün sosial proseslərinə nüfuz edir, istənilən dövlətin milli təhlükəsizliyinin ayrılmaz tərkib hissəsinə çevrilir [7, s. 3, 13, s. 93].

Elmi nəşrlərin icmalı göstərir ki, İnT sahəsində işlərin əksəriyyəti iki əsas yanaşma ərtafında qruplaşır. Birinci yanaşmanı texnoloji yanaşma kimi qəbul etmək olar, bu yanaşmada dövlətin informasiya sferasında təhlükəsizliyinin təmin edilməsinə yalnız informasiyanın və informasiya (kommunikasiya) sistemlərinin mühafizəsi bucağından baxılır.

İkinci yanaşma *dövlətin, cəmiyyətin və şəxsiyyətin maraqlarının* informasiyanın zərərli təsirlərindən qorunması zəruriliyindən çıxış edir. Məsələn, bəzi rəsmi sənədlərdə təhlükəsizlik – "*şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarının daxili və xarici təhdidlərdən mühafizəlilik vəziyyəti*" kimi müəyyən edilir [5, 6]. Lakin "təhlükəsizlik" terminə "mühafizəlilik" vasitəsilə tərif vermək qüsurludur, çünki bu sözlər müəyyən mənada sinonimdirlər.

"İnformasiya təhlükəsizliyi" anlayışının "idarəetmə (menecment)" anlayışı ilə əlaqəsinin aydınlaşdırılması "e-dövlətin informasiya təhlükəsizliyi" anlayışının məzmununa daxil olan əsas əlamətlərin aşkarlanmasına imkan verir.

İnformasiya təhlükəsizliyi termini həmişə müəyyən şəraitdə (mühitdə) olan konkret idarəetmə obyekti ilə bağlı olur. Təhlükəsizlik obyektin müəyyən

vəziyyətidir və onu müvafiq keyfiyyət xarakteristikalarını göstərməklə müəyyən etmək olar. Təhlükəsizlik haqqında danışarkən obyektin varlığının müəyyən məqsəd funksiyası nəzərdə tutulur və təhlükəsizlik subyektin bu funksiyanı reallaşdırmaq qabiliyyəti kimi başa düşülür [67, s.102-123].

Beləliklə, idarəetmə nəzəriyyəsi baxımından e-dövlətin İnT-nə "e-dövlətin normal qəbul edilmiş vəziyyətini pozmağa cəhd edən məqsədyönlü daxili və xarici təsirlər şəraitində e-dövlətin normal vəziyyətdən məqbul kənarlaşmalar çərçivəsində idarə edilməsi prosesi kimi" tərif vermək olar.

Digər konseptual model anlayışları. İnformasiya təhlükəsizliyinə sistemli yanaşma onun obyektlərinin, subyektlərinin, prinsiplərinin, vasitələrinin, təhdidlərin və onların mənbələrinin müəyyən edilməsini tələb edir.

E-dövlətin İnT-nin obyektləri insanların şüuru, psixikası, müxtəlif miqyaslı və təyinatlı informasiya sistemləri ola bilər. E-dövlətin İnT-nin obyektlərinə aşağıdakıları aid etmək mümkündür:

- milli informasiya infrastrukturu – ölkənin dövlət və qeyri-dövlət informasiya resurslarının, təşkilati-texniki strukturların, sistem və şəbəkələrin, onların təminat vasitələrinin toplusu;
- kritik informasiya infrastrukturu – sıradan çıxması və ya məhv olması müdafiə, iqtisadiyyat, səhiyyə və milli təhlükəsizlik sahəsində fəlakətli nəticələrə səbəb ola bilən vacib fiziki və ya virtual sistemlərin və vasitələrin toplusu;
- ictimai şüurun (dünyagörüşü, siyasi baxışlar, mənəvi dəyərlər və s.) kütləvi informasiya və təbliğat vasitələrinə əsaslanan formalaşdırılması sistemi;
- vətəndaşların, hüquqi şəxslərin və dövlətin informasiyanın əldə edilməsi, yayılması və istifadəsi hüquqları, konfidensial informasiyanın və intellektual mülkiyyətin qorunması.

E-dövlətin İnT-nin subyektləri onun təmin edilməsi ilə məşğul olan orqanlar və strukturlar hesab olunur. E-dövlətin İnT-nin subyektləri dövlət, cəmiyyət və vətəndaşlardır.

E-dövlətin İnT-nin idarə edilməsi prinsiplərinə aşağıdakılar aiddir: qanuna əsaslanmaq, fərdin, cəmiyyətin və dövlətin maraqlarının balanslaşdırılması,

komplekslilik, sistemlilik, beynəlxalq təhlükəsizlik sistemləri ilə inteqrasiya, iqtisadi effektivlik və s.

E-dövlətin İnT təhdidləri – informasiya sferasında şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarına təhlükə yaradan şərtlərin və faktorların toplusudur.

Tədqiq olunan predmet sahəsinə müxtəlif baxışların icmalı göstərir ki, hazırda e-dövlətin İnT-nə təhdidlərin və onların mənbələrinin kifayət qədər əsaslandırılmış və təfsilatlı ümumi təsnifatı yoxdur.

Sistemin vəziyyəti hər bir zaman anında sistemin malik olduğu əhəmiyyətli xassələrin toplusuna deyilir. Sosial-texniki sistemlərdə çox zaman "zəif bənd" insan olur, buna görə də e-dövlətin İnT-nin vəziyyətini insan faktorunu nəzərə almadan qiymətləndirmək olmaz. E-dövlətin İnT vəziyyətini İnT-ni və onun əlaqələrini xarakterizə edən faktorların bütün müxtəlifliyini əhatə edən indikatorlar sistemi əsasında kəmiyyət və keyfiyyət səviyyələrində adekvat qiymətləndirilməsi olduqca çətindir. E-dövlətin İnT vəziyyətinin qiymətləndirilməsini vəziyyət sinifləri müəyyən etmək və bu siniflər üzrə aparmaq daha məqsədəuyğundur.

1.1.2. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi funksiyaları

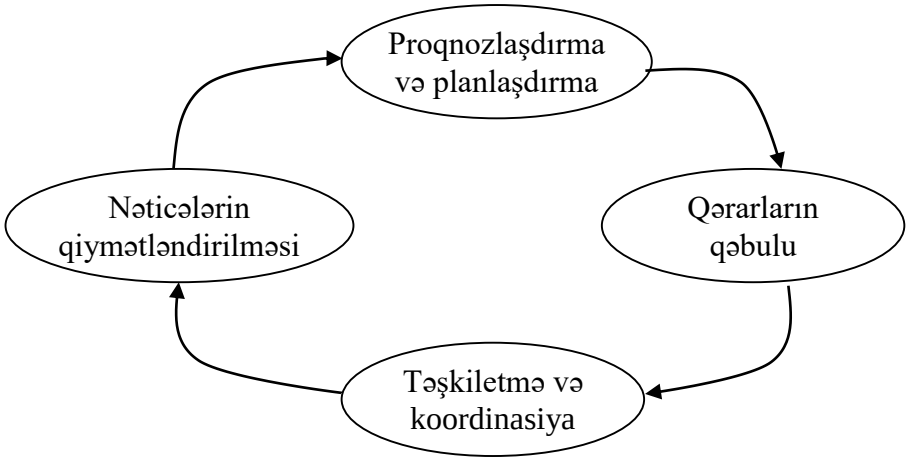
İdarəetmə – idarəetmə subyektinin idarəetmə obyektinə məqsədyönlü və davamlı təsiri prosesidir. İdarəetmə funksiyaları və hər bir funksiya üzrə işlərin həcminin müəyyən edilməsi idarəetmə sisteminin strukturunun formalaşdırılması və onun komponentlərinin qarşılıqlı təsiri üçün əsas rolunu oynayır. İdarəetmə funksiyası dedikdə, idarə edən sistemdə əməliyyatların əmək bölgüsünə əsaslanan nizamlı toplusu başa düşülür. İdarəetmə funksiyaları bu növ fəaliyyətin müəyyən ehtiyacların ödənilməsinə yönəlmiş əsas istiqamətlərini təşkil edir [68, s. 76].

İdarəetmə funksiyalarının, onların idarəetmədə əhəmiyyətinin və xüsusi çəkisinin müəyyən edilməsinin bir neçə metodu vardır. Onlardan biri – müvafiq ədəbiyyatın analizi və orada təsvir edilən idarəetmə məsələlərinin seçilməsidir. Belə prosedur həyata keçirildikdən sonra aşkarlanmış məsələlərin siyahısı onları vaciblik dərəcəsinə görə sıralamaq üçün menecerlərə təqdim edilir və bunun əsasında da əsas

idarəetmə funksiyaları və onların əhəmiyyəti müəyyən edilir. Seçilmiş funksiyalar toplusu *idarəetmə sisteminin konsepsiyasını* təşkil edir.

Funksional ixtisaslaşma idarəetmə fəaliyyətinin spesifik növlərinə və ya idarəetmə funksiyalarına əsaslanır. Ənənəvi olaraq idarəetmədə idarəçilik fəaliyyətinin funksiyalarının formalaşdırılması üçün əsas kimi idarəetmə prosesinin məntiqi mərhələləri götürülür: layihələndirmə (informasiyanın toplanması və emalı, proqnozlaşdırma, planlaşdırma), təşkiletmə (qərarların qəbulu, məsələlərin və resursların paylanması, operativ rəhbərlik), qiymətləndirmə (uçot, nəzarət, tənzimləmə, sərəncamvermə).

İdarəetmə funksiyalarının xüsusiyyəti onların vahid idarəetmə tsikli çərçivəsində davamlı və fasiləsiz həyata keçirilmələridir. Klassik idarəetmə tsikli bütün funksiyaların ardıcıl və mütləq yerinə yetirilmələrini nəzərdə tutur (şəkil 1.1.1).



Şəkil 1.1.1. Klassik idarəetmə tsikli

Müasir ədəbiyyatda kifayət qədər çox idarəetmə funksiyası müəyyən edilir. Dövlət idarəçiliyi və İnT üzrə mövcud ədəbiyyatın analizi əsasında e-dövlətin İnT-nin idarə edilməsinin aşağıdakı funksiyalarını ayırmaq olar [68, s. 76; 39, s. 186; 42, s.105; 7, s. 3, 10, s. 32]:

Proqnozlaşdırma – sistemin gələcəkdə mümkün strukturu, xassələri və ya fəaliyyət qanunları haqqında qeyri-müəyyənliyin aradan qaldırılması vasitəsidir. Proqnoz – sistemin gələcəkdə mümkün vəziyyətləri, nəzərdə tutulmuş vəziyyətin əldə edilməsinin alternativ yolları və müddətləri haqqında elmi əsaslandırılmış fikirlərdir. Proqnozlaşdırma vacib idarəetmə qərarlarının qəbulunda zəruri alətdir, onsuz sosial

proseslərin nəticələrini, gələcək vəziyyəti, fəaliyyətin effektivliyini müəyyən etmək mümkün deyil.

Planlaşdırma – e-dövlət maraqlarının və ətraf mühitin analizi nəticəsində məqsədlər sistemi müəyyən edilir, məqsədlər, ətraf mühitin və daxili mühitin vəziyyətləri əsasında alternativ strategiyalar işlənilir və seçilir, strategiyaların reallaşdırılması üçün taktika və prosedurlar işlənilir, onların əsasında operativ planlarla yerlərdə müvafiq işlər həyata keçirilir.

Təşkiletmə – nəzərdə tutulmuş məqsədlərin effektiv əldə edilməsini təmin etmək üçün sistemin bütün elementləri arasında daimi və müvəqqəti əlaqələrin qurulmasından, onların fəaliyyət nizamının və şərtlərinin müəyyən edilməsindən, sistemin komponentlərinin və resurslarının birləşdirilməsindən ibarətdir. Təşkiletmə – müəyyən edilmiş prinsiplər və yanaşmalar əsasında idarəetmə sisteminin formalaşdırılması, idarəedən və idarə edilən sistemlərin strukturunun müəyyən edilməsidir.

Koordinasiya – sistemin məqsədlərinə, idarəetməyə uyğun olaraq altsistemlərin hərəkətlərinin razılaşdırılması və bu razılaşmanın idarəetmə tsikli ərzində saxlanmasıdır.

Bir neçə idarəetmə obyektinin və altsistemlərin varlığı onların özəl məqsədləri arasında ziddiyyətə gətirib çıxarır. Bu da öz növbəsində, hərəkətlər arasında əlaqəsizliyə səbəb olur. Bu ziddiyyətlərin aradan qaldırılması – koordinasiyanın əsas məsələsidir. Koordinasiya və təşkiletmə funksiyalarına çox zaman operativ idarəetmə məsələləri çərçivəsində baxırlar. İnT-nin dövlət miqyasında təmin edilməsi müxtəlif icra hakimiyyəti orqanları arasında üfüqi və şaquli qarşılıqlı əlaqələrin inkişafını tələb edir.

Nəzarət – idarəetmə obyektinin vəziyyətinin müəyyən edilməsini (idarəetmə obyekti haqqında verilənlərin ölçülməsi, toplanması, dəqiqləşdirilməsi) və verilmiş effektivlik meyarları üzrə cari vəziyyətin tələb ediləndən uzaqlaşma dərəcəsini qiymətləndirməyi təmin edən funksiyalar sistemidir.

İnformasiya təhlükəsizliyinin təmin edilməsi – informasiya və telekommunikasiya sistemlərinin fəaliyyətinin təhlükəsizliyi, terrorizm, ekstremizm

ideologiyalarının yayılmasına, zorakılığın təbliğinə əks-təsir, konfidensial məlumatların, o cümlədən fərdi məlumatların təhlükəsizliyi üzrə tədbirlərin həyata keçirilməsidir.

İnsidentlərin idarə edilməsi – irimiqyaslı insidentlərə hazırlığın yüksəldilməsi, reaksiya vaxtının azaldılması, qəzalardan sonra bərpa planının işlənməsi (məsələn, xüsusi şəraitdə milli fəaliyyət planı, kiberfəzada davranış qaydası, situasiya barəsində məlumatlandırma) nəzərdə tutulur.

Hüquq-mühafizə – kibercinayətkarlıqla mübarizə üçün dövlətin potensial imkanlarının inkişafı və zəruri qanunvericilik bazasının müəyyən edilməsi nəzərdə tutulur.

Tənzimləmə – idarəetmə sisteminin təşkili və fəaliyyəti prosesində idarəetmə obyekti və müxtəlif hüquq subyektləri üçün məcburi tələblərin və prosedurların müəyyən edilməsidir.

Beynəlxalq əməkdaşlıq – qanunvericilik tədbirləri, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının sertifikatlaşdırılması və s. kimi sahələrdə qarşılıqlı faydalı beynəlxalq əməkdaşlığın təmin edilməsidir.

Təhsil – İnT sahəsində zəruri bilik, bacarıq və səriştəyə malik kadrların hazırlanması və əhalinin maarifləndirilməsi funksiyasıdır.

Elmi tədqiqatlar – həm mövcud, həm də gələcək sistemlərin və xidmətlərin təhlükəsizliyini təmin etmək üçün fundamental nəzəri tədqiqatların və yeni texnologiyaların prioritet inkişafının təmin edilməsidir.

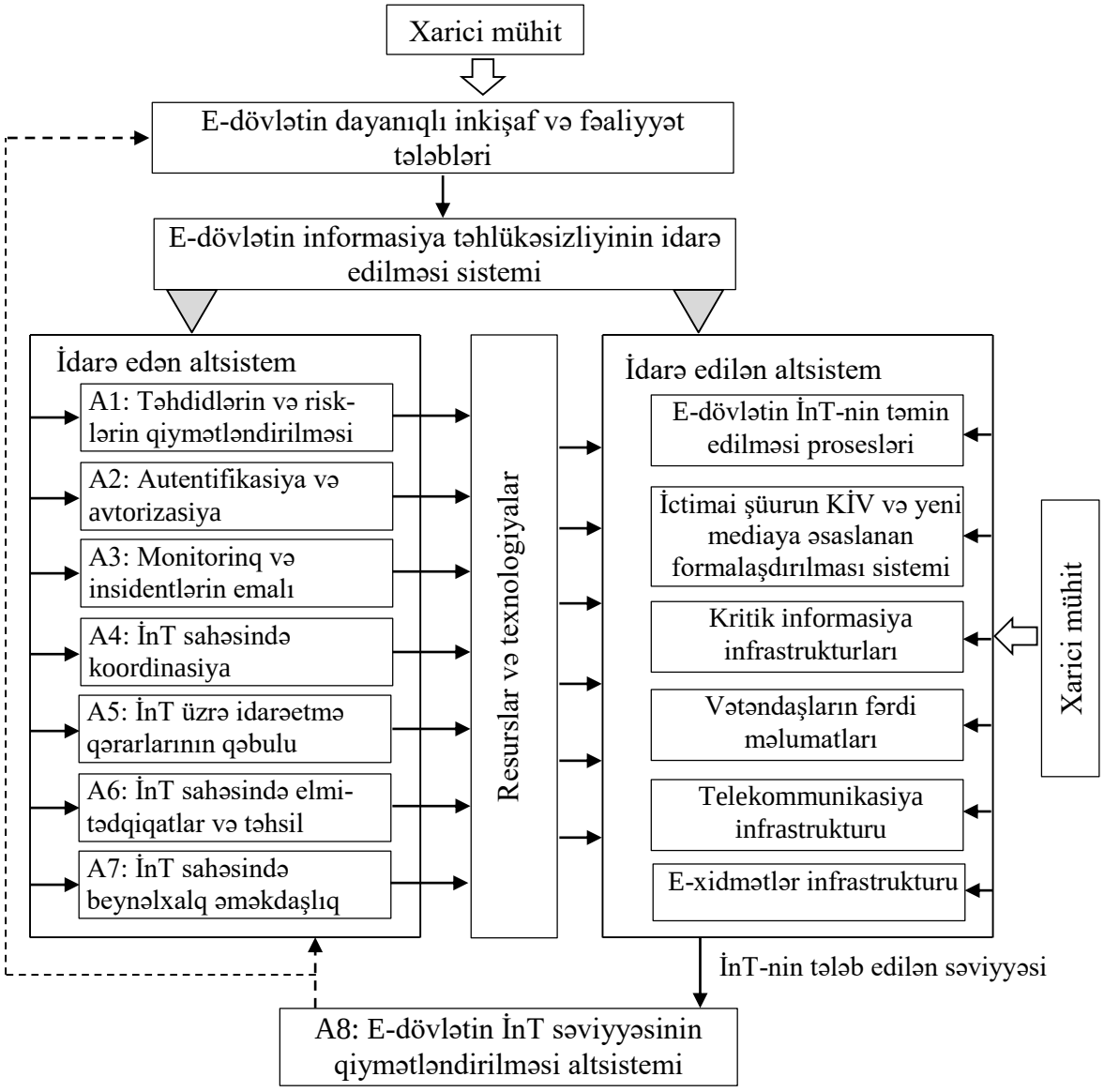
Mədəni-tərbiyəvi – İnT mədəniyyətinin, yüksək mənəviyyatın və vətəndaşlıq mövqeyinin formalaşdırılmasına yönəlmiş funksiyadır.

İdarəetmənin informasiya təminatı – idarəetmə fəaliyyətinin həyata keçirilməsi üçün zəruri olan informasiyanın toplanması, emalı və analizidir.

Sadalanmış funksiyalar idarəetmə funksiyalarının tam siyahısını əhatə etmir. Onlar qismən kəsişə də bilərlər. Lakin sadalanmış funksiyalar da idarəetmə fəaliyyətinin spesifik növü kimi e-dövlətin İnT-nin idarə edilməsinin məzmunu və predmeti haqqında yetərli təsəvvür yaradır.

İnformasiya təhlükəsizliyinin idarə edilməsi funksiyaları müəyyən təşkilati, texnoloji, inzibati, iqtisadi və sosial-psixoloji və s. metodların əsasında həyata keçirilir.

Yuxarıda müəyyən edilmiş idarəetmə funksiyalarından çıxış edərək e-dövlətin İnT-nin idarə edilməsi sistemini aşağıdakı altsistemlərə dekompozisiya etmək təklif olunur (şəkil 1.1.2):



Şəkil 1.1.2. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sistemi

A1: Təhdidlərin və risklərin qiymətləndirilməsi altsistemi – İnT-in idarə edilməsində əsas nəzarət parametri İnT riskidir. İnT riski təhdidin başvermə ehtimalı ilə təhdidin reallaşması nəticəsində vurula bilən potensial ziyanın kombinasiyası kimi müəyyən olunur. Bu altsistemdə İnT-nə əhəmiyyətli dərəcədə təsir edən aktivlərin

uçotu üzrə işlərin aparılması, İnT təhdidlərinin analizi və proqnozlaşdırılması, risklərin analizi və qiymətləndirilməsi həyata keçirilir.

A2: Autentifikasiya və avtorizasiya altsistemi – E-dövlət ilə vətəndaşların, biznes-sektorun, dövlət orqanlarının qarşılıqlı təsiri zamanı bütün iştirak edən tərəflərin etibarlı autentifikasiyası və avtorizasiyası təmin edilməlidir. Vətəndaş məhz öz e-dövlətinə müraciət etdiyinə, e-dövlət də bədniyyətli ilə deyil, e-xidmət üçün müraciət etmiş vətəndaşla ünsiyyətdə olduğuna əmin olmalıdır. Bu məsələnin həlli təsəvvür edildiyi kimi asan deyil. Adi həyatda dövlət hakimiyyəti nümayəndəsi vətəndaşın şəxsiyyətini onun pasportuna görə yoxlayır. Virtual mühitdə autentifikasiya daha çətindir: burada şəxsiyyəti təsdiq edən sənədlərin skan edilmiş surətlərindən istifadə etmək mümkün deyil. Vətəndaşların e-dövlət xidmətlərindən təhlükəsiz və rahat istifadəsi üçün şəxsiyyəti müəyyən edən elektron identifikatorlar (eID) əsas autentifikasiya vasitəsi kimi çıxış edir. Ölkələrin geniş istifadə etdiyi eID sxemi İnternet mühitində biometrik texnologiyalar ilə e-imza texnologiyalarını birləşdirən şəxsiyyəti təsdiq edən yeni nəsil sənədlərdən (e-pasportlardan) istifadə edir. Bu məqsədlə "Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı" həyata keçirilmişdir [2]. Hazırda e-imza ilə təsdiqlənmiş biometrik məlumatlar yeni nəsil şəxsiyyət vəsiqələrinə də daxil edilir [4].

A3: Monitorinq və insidentlərin emalı altsistemi – e-dövlətin İnT vəziyyətinin fasiləsiz monitorinqinin həyata keçirilməsi və aşkarlanmış insidentlərin koordinasiya edilərək effektiv şəkildə aradan qaldırılması məsələlərinə cavabdehdir. E-dövlətin İnT-nin monitorinqi sistemi İnT tələblərinin yerinə yetirilməsi vəziyyəti barəsində məlumatların ölkə miqyasında müvafiq nəzarət nöqtələrindən toplanmasını və İnT üzrə situasiyaların analizini həyata keçirir, e-dövlət infrastrukturuna hücumları aşkarlayır və təhlükəsizliyin pozulması haqqında real zamanda xəbərdarlıq verir, İnT-nin təmin edilməsində "zəif" yerləri müəyyən edir. E-dövlətin İnT-nin vəziyyəti barədə müxtəlif domenlərə məxsus antivirus sistemləri, IDS (Intrusion Detection System – müdaxilələri aşkarlama sistemi), SIEM (Security Information and Event

Management), SOC (Security Operations Center) sistemlərindən və digər İnT vasitələrindən daxil olan monitorinq məlumatlarının vahid informasiya fəzasında birləşdirilməsi nəzərdə tutulur [13, s. 93].

İnformasiya təhlükəsizliyinin təmin edilməsi vasitələri mükəmməl deyil, informasiya texnologiyalarında dinamik dəyişikliklər baş verir və İnT-nin təmin edilməsinə zəruri resurslar ayırmaq mümkün olmur. Təəssüf ki, bu və digər səbəblərdən İnT-ni tam təmin etmək mümkün deyil və İnT-nin pozulması halları – İnT insidentləri baş verir. Cəmiyyətin informasiyalaşdırılması səviyyəsi artdıqca, bu insidentlər nəticəsində mümkün maliyyə itkilərinin və risklərin səviyyəsi daha da artır. Buna görə təşkilatların İnT insidentlərinə tez və adekvat reaksiya verməsi vacib əhəmiyyət daşıyır. Çox zaman insidentlərin keyfiyyətli və effektiv cavablandırılmasını təmin etməklə təşkilat insidenti zərərlə deyil, fayda ilə aradan qaldıra bilər [8, s. 35]. İnT insidentlərinin idarə edilməsi sahəsində mövcud elmi tədqiqatlar əsasən təşkilati və arxitektura məsələlərini əhatə edir.

A4: İnT üzrə koordinasiya altsistemi – İnT sahəsində dövlət siyasətinin həyata keçirilməsi üzrə fəaliyyətin təşkili və koordinasiyasını həyata keçirir. E-dövlətin İnT-nin idarə edilməsi sistemi qarşılıqlı əlaqəli sosio-texniki sistemlərin mürəkkəb çoxsəviyyəli sistemidir və koordinasiya bu sistemin bütün funksiyalarının həyata keçirilməsində fövqəladə vacib rol oynayır. E-dövlət texnologiyaları inkişaf etdikcə kəskinləşən İnT mühitində koordinasiya məsələləri daha da mürəkkəbləşir və koordinasiyanın rolu daha da artır. Müasir şəraitdə e-dövlətin İnT-ni yalnız bütün maraqlı tərəflərin – dövlət orqanlarının, biznes strukturlarının, vətəndaş cəmiyyəti institutlarının və vətəndaşların səylərini koordinasiya etməklə təmin etmək mümkündür.

E-dövlətin İnT-nin idarə edilməsi sahəsində koordinasiya məsələləri olduqca çeşidli və müxtəlif xarakterlidir [16, s. 24]. E-dövlətin İnT sahəsində koordinasiya məsələləri milli İnT strategiyası və onun həyata keçirilməsi üzrə proqramların işlənməsi, İnT üzrə birgə tədbirlərin və təşəbbüslərin vahid mərkəzdən idarə edilməsi, İnT sahəsində elmi-tədqiqat işlərinin koordinasiyası və prioritetlərin müəyyən

edilməsi, kiber-hücumların qarşısının alınması, İnT insidentlərinin emalı, müvafiq normativ hüquqi aktların işlənməsi, kapitaltutumlu İnT sistemlərindən kollektiv istifadənin təşkili və s. məsələləri əhatə edir.

Dövlət İnT sahəsində səyləri birləşdirmək üçün müxtəlif koordinasiya mexanizmləri tətbiq edir, bu istiqamətdə müxtəlif tədbirlər həyata keçirir, dövlət, özəl və ictimai sektorlar üçün kibertəhlükəsizlik üzrə koordinasiya mərkəzləri yaradır [11, s. 92, 279 s. 35-41]. Bu mərkəzlərin vəzifəsi infrastruktur obyektlərinin, e-xidmətlərin, intellektual mülkiyyətin, fərdi məlumatların kiberhücumlardan müdafiəsi üçün göstərilən səylərin konsolidasiyasıdır.

A5: İnT üzrə idarəetmə qərarlarının qəbulu altsistemi – müxtəlif səviyyələrdə idarəetmə qərarlarının qəbul edilməsini təmin edir. Təşkilatda olduğu kimi, e-dövlətin İnT-nin idarə edilməsinə də üç müxtəlif səviyyədə baxmaq olar: strateji, taktiki və operativ. Strateji səviyyə korporativ strategiyaya təsir edir, taktiki səviyyə İnT-nin idarə olunmasında istifadə edilən proseslərə və metodologiyalara aiddir, operativ səviyyəyə İnT alətlərinin və tədbirlərinin realizəsi və istismarı daxildir. Qeyd etmək zəruridir ki, təşkilatda İnT-nin idarə edilməsi əsasən operativ səviyyədə cəmləşir.

Müasir kiberhücumlar demərkəzləşmiş, avtomatlaşdırılmış, gizli, intellektual və kooperativdir, buna görə qəbul edilmiş qərarlar və əks-tədbirlər də çoxölçülü, əlaqələndirilmiş, kooperativ olmalı, İnT vasitələrinin ortaq istifadəsini və məlumat mübadiləsini nəzərdə tutmalıdır.

A6: İnT sahəsində elmi-tədqiqatlar və təhsil altsistemi – Həm mövcud, həm də gələcək sistem və servislərin təhlükəsizliyi problemlərinin həllinə yönəlmiş kompleks elmi-praktiki tədqiqatların aparılması və İnT sahəsində yüksək ixtisaslı kadrların hazırlanmasına məsuldur. Hazırki reaktiv metodlar (şəbəkələrarası ekranlar, anivirus skanerləri, CERT-lər (Computer Emergency Response Team – kompüter insidentləri ilə mübarizə komandası) və digər reaksiya strukturları) kiberhücumlarla adekvat mübarizə apara bilmirlər, buna görə baxılan altsistem üçün innovativ texnologiyaların hazırlanması prioritet ola bilər. Bu altsistem İnT sahəsində konseptual yanaşmaların və prioritet istiqamətlərin müəyyən edilməsi, elmi-tədqiqatlar üçün strateji siyasətin,

proqramların, strateji planların, investisiya layihələrinin hazırlanmasını, elmi-tədqiqatların koordinasiyasını da həyata keçirir. Bəzi ölkələrdə İnT üzrə tədqiqatlar sahəsində aparıcı mərkəzlərin təyin edilməsi və onların müvafiq büdcə ilə təmin edilməsi təcrübəsi vardır [99, s. 3]. Hazırki kiberfəzanı, kibertəhlükəsizliyi, şəbəkələşmiş informasiyanın bəşəriyyətə açdığı imkanları və onun qarşısında qoyduğu çağırışları başa düşmək üçün fundamental və tətbiqi elmi-tədqiqatların aparılması da zəruridir.

İnT bütün ölkələr üçün prioritet məsələdir və bu məsələnin həllində əsas elementlərdən biri İnT sahəsində yüksək ixtisaslı, öz biliklərini real şəraitdə tətbiq etməyə və zamanın tələblərinə çevik cavab verməyə qabil mütəxəssislərin hazırlanmasıdır [28, s.129]. Hazırda kiber-qoşunların formalaşdırılması, kiber-təhlükəsizlik sənayesinin qurulması, e-xidmətlərin genişləndirilməsi, 4-cü sənaye inqilabının gətirdiyi yeni texnologiyalar nəticəsində bütün ölkələrdə belə mütəxəssislərə kəskin tələbat vardır.

İnT sahəsində yüksək ixtisaslı kadr hazırlığı üçün bu sahədə əlaqədar qurumlar arasında kooordinasiyanın gücləndirilməsi, onların səylərinin birləşdirilməsi, təcrübə mübadiləsi, tədris proqramlarının və elektron resursların, virtual laboratoriyaların yaradılması, kiber-hücum və müdafiə üzrə yarışların təşkili, kibertəhlükəsizlik sahəsində tədris aparan pedaqoji kadrların ixtisasının artırılması, elmi tədqiqatların daha da intensivləşdirilməsi olduqca vacibdir.

A7: Beynəlxalq əməkdaşlıq altsistemi – Milli kiber təhlükəsizliyin təmin edilməsində beynəlxalq əməkdaşlıq həyati əhəmiyyət daşıyır, çünki hamı bir kiberfəzadan asılıdır və bir ölkədə olan kibertəhlükəsizlik boşluqları digər ölkələrə təsir edə bilər. Beynəlxalq əməkdaşlıq qanunvericilik tədbirləri, kibercinayətkarlıqla mübarizə, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının sertifikatlaşdırılması kimi sahələri əhatə edə bilər [32, s. 102].

İnfornasiya təhlükəsizliyi sahəsində qlobal miqyasda əməkdaşlığa misal IMPACT (International Multilateral Partnership Against Cyber Threats – Kibertəhdidlərə qarşı Beynəlxalq Çoxtərəfli Əməkdaşlıq) misal ola bilər. IMPACT

Beynəlxalq Telekommunikasiya İttifaqının nəzdində İnT üzrə xüsusi qurumdur [23, s.14]. 2018-ci ilin sentyabrına olan vəziyyətdə 152 dövlət bu qurumun üzvü idi. IMPACT ölkələrə İnT-nin qiymətləndirilməsi, insidentlərin emalı, mütəxəssislərin hazırlığı və treninqi, kibertəlimlərin təşkili kimi xidmətlər göstərir.

A8: E-dövlətin İnT səviyyəsinin qiymətləndirilməsi altsistemi – Şəkil 1.1.2-dən göründüyü kimi, bu altsistem "İdarə edən altsistemlər" konturuna daxil deyil, ondan asılı deyil və İnT səviyyəsinin alınmış qiymətini bu altsistemlərə təqdim edir (əks-əlaqəni təmin edir). Bu, "İdarə edən altsistemlərin" qiymətləndirmənin nəticələrinə hər hansı təsirini neytrallaşdırmaq üçündür, çünki bu sistemlər İnT-nin səviyyəsinin yüksək qiymətləndirilməsində maraqlı ola bilərlər.

Təbii olaraq, e-dövlətin İnT-nin idarə edilməsinin effektivliyinin qiymətləndirilməsi məsələsi meydana çıxır.

"İdarəetmənin effektivliyi" anlayışı hələlik elmi ədəbiyyatda aydın müəyyən edilməyib [42, s. 111]. İdarəetmənin effektivliyini müxtəlif kriteriyalar üzrə qiymətləndirmək olar:

- *funksional effektivlik* – tədbirlərin keyfiyyəti və nəticəliliyini xarakterizə edir;
- *sosial effektivlik* – vətəndaşların dövlətin zəmanət verdiyi həcmdə xidmətlə təmin edilməsi səviyyəsini əks etdirir;
- *iqtisadi effektivlik* – maddi, maliyyə və insan resurslarının rasional istifadə səviyyəsini göstərir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin effektivliyi ilk növbədə qərarların vaxtında qəbul olunması, məqsədəuyğunluğu, adekvatlığı və qərarların həyata keçirilməsinin nəticələrinə görə qiymətləndirilə bilər. Eyni zamanda, informasiya təhlükəsizliyi insidentlərindən vurulan ziyanın azaldılması, informasiya təhlükəsizliyinə xərclərin optimallaşdırılması, informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi, informasiya təhlükəsizliyinin idarə edilməsi yetkinliyinin yüksəlməsi də informasiya təhlükəsizliyinin idarə edilməsi effektivliyinin kriteriyaları kimi istifadə edilə bilər.

1.2. E-dövlətin informasiya təhlükəsizliyi üzrə elmi-tədqiqatların müasir vəziyyətinin analizi

İnT bir praktiki fəaliyyət sahəsi və bir elmi tədqiqat istiqaməti kimi son bir neçə onillikdə formalaşmışdır [123, s.33], "verilənlərin mühafizəsi", "kompüter təhlükəsizliyi", "şəbəkə təhlükəsizliyi" və nəhayət, "informasiya təhlükəsizliyi" adlarını daşımışdır. Solms son 40-50 il ərzində İnT-nin idarə edilməsi sistemlərinə yanaşmaların inkişafını analiz edir və onları "dörd dalğa"ya bölür [290, s.165]. Hər dalğa verilmiş zaman kəsiyində informasiya texnologiyalarına və onların idarə edilməsinə ümumi yanaşmanı təsvir edir. İlkin yanaşmalarda hansısa bir texnoloji həll vasitəsi ilə problemləri həll etməyə çalışırdılar, belə həllər çoxaldıqca bu yanaşmanın problemi həll edə bilmədiyi meydana çıxdı. Hazırda əsas yanaşma İnT-nin idarə edilməsi yanaşmasıdır. Bu yanaşmada İnT sisteminin əsas komponentləri kimi texniki aspektlər deyil, idarəetmə (menecment) komponentləri götürülür.

İnformasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatlar 1970-ci illərin sonlarından başlanmışdır, 1990-cı illərin sonuna doğru ilk milli və beynəlxalq standartlar (ISO/IEC 17799) qəbul edilmişdir [19, s. 19]. Lakin bu standartlar və tədqiqatlar İnT-nin əsasən, təşkilatlar səviyyəsində idarə edilməsini nəzərdə tutur. Son dövrlər İnT-nin milli (və regional, beynəlxalq) səviyyədə idarə edilməsi məsələləri ön plana çıxır [126, s.127, 135, s. 130, 300, s. 2942]. Bu səviyyələrin hər biri İnT-nin idarə edilməsi üçün özünəməxsus metodoloji bazanın işlənilməsini tələb edir.

Bunu nəzərə alaraq, aşağıda e-dövlətin İnT-nin idarə edilməsi sahəsində elmi-praktiki tədqiqatların müasir vəziyyəti analiz edilir, mövcud yanaşmaların üstün və çatışmayan cəhətləri müəyyən edilir [19, s.19, 77, s.1-5].

E-dövlətin İnT modelləri. E-dövlətin multi-domen mühitinin əsas xüsusiyyətləri və komponentləri [191, s. 66]-də analiz edilir, bu mühitdə İnT sistemlərinin yaradılması zamanı əsas tələblərin rahat girişin təmin edilməsi ilə müfəssəl monitorinq icazələri arasında diqqətli balanslaşdırma olduğu göstərilir.

E-dövlətdə qarşılıqlı əlaqənin üç modeli (C2G, G2G və G2C) əsasında dövlət strukturları çərçivəsində İnT, təhlükəsizliyin xarakteristikaları və təhlükəsizlik tələblərinin reallaşdırılması məsələləri [164, s. 336]-də analiz edilir.

E-dövlətin İnT-nin müxtəlif aspektlərinə hərtərəfli baxış üçün vahid konsepsiya [303, s.350]-də irəli sürülür. Bu vahid yanaşma 4 səviyyədən ibarətdir: strateji, proses, qarşılıqlı əlaqə və informasiya. Burada təhlükəsizlik aspektləri strateji səviyyədən verilənlər səviyyəsinə kimi inteqrasiya edilir.

E-dövlət mühitində fəaliyyət göstərən korporativ şəbəkələrin İnT-nin təmin olunmasının adaptiv sistemlərinin yaradılmasının elmi-nəzəri və metodoloji əsaslarının işlənməsi problemlərinə [35, s.1-40]-də baxılmışdır. Belə sistemlərin tərkibinə daxil olan, İnT-nin təmin olunmasını həyata keçirən və qarşılıqlı əlaqəli fəaliyyət göstərən altsistemlərin sintezi üçün çoxsaylı riyazi model və metodlar işlənmişdir.

E-dövlət sistemləri də e-kommersiya sistemlərinin məruz qaldığı təhdidlərə məruz qalır, lakin e-dövlət sistemləri başqa məhdudiyyətlər çərçivəsində işləyirlər. E-kommersiya sistemlərinin çoxu yalnız əhalinin bir hissəsi ilə işləyir, onlar özləri bunu necə və nə vaxt edəcəklərini seçirlər. Bundan fərqli olaraq, e-dövlət bütün vətəndaşlarla işləyir. İstifadəçilərin və tranzaksiyaların sayının olduqca çox olması, vətəndaşların fərdi məlumatlarının və dövlətin konfidensial məlumatlarının həssaslığı və bir sıra digər məsələlər nəticəsində e-dövlətin İnT-nin təmin edilməsi daha vacib olur.

E-kommersiya üçün geniş istifadə edilən təhlükəsizlik yanaşmaları e-dövlətə də tətbiq edilə bilər, lakin e-dövlət e-kommersiyadan xeyli fərqlidir. Adətən, e-dövlət şəbəkələri bir-biri ilə kommersiya şəbəkələrinə nisbətən daha yaxşı kommunikasiya yaradırlar, çünki onların çoxunda informasiyanın ötürülməsi prosesləri inteqrasiya edilib, kommersiya şəbəkələri isə rəqibdirlər və öz konfidensial informasiyalarını paylaşmırlar. Bu məsələlər [303, s.350]-də müzakirə edilir, e-dövlətin İnT problemləri texnoloji və qeyri-texnoloji baxımdan analiz edilərək təhlükəsizliyin müxtəlif tələbləri üçün kompleks həllər təklif edilir.

E-dövlət və e-kommersiya sistemləri arasındakı fərqlər [117, s. 98, 132, s. 589]-də daha detallı şəkildə müzakirə edilir və müvafiq modellər işlənilir. E-dövlətin realizəsinin dövlət tələblərinə uyğunluğunu qiymətləndirmək üçün kompüter təhlükəsizliyi üzrə məlumatların toplanması sistemi təklif edilir.

E-dövlətin İnT-nin idarə edilməsinin əsas faktorları [271, s.23, 293, s.483]-də analiz edilir, bu faktorlar təhlükəsizlik mədəniyyəti, idarəetmə, İnT infrastrukturu və dəyişikliklərin idarə edilməsi kimi qruplaşdırılır. Müəlliflərin təqdim etdiyi ranqlaşdırma nəticələrinə görə, uğurlu təhlükəsizlik prosesləri üçün üç əsas faktor yüksək rəhbərliyin fəal dəstəyi, yetərli maliyyələşdirmə və kadrların səriştəsi/treninqidir.

E-dövlətin İnT üçün workflow modelə [98, s.398]-də baxılır. Modelin komponentləri e-xidmətlərin təhlükəsizliyinin təmin edilməsinə yönəlib, bu komponentlər İnT-nin təmin edilməsi üçün siyasi qərarın qəbulu, bu qərarın reallaşdırılması üçün İnT-nin analizi, müvafiq qanunvericilik bazasının formalaşdırılması, istifadəçilərin inamının qiymətləndirilməsi, təhlükəsizlik strategiyalarının müəyyən edilməsi ilə yanaşı, fərdi məlumatların qorunması, girişin idarə edilməsi, autentifikasiya və şəbəkə təhlükəsizliyinin təmin edilməsi mexanizmləri kimi texnoloji məsələləri də əhatə edir.

İnT-nin idarə edilməsi üçün [246, s.1-27]-da metamodel təklif edilir, metamodelə müxtəlif komponentlər daxildir. Metamodelin elementləri (meta-primitivlər) İnT-nin idarə edilməsinin biznes-strategiyası və missiyası, idarəetmə məqsədləri və idarəetmə strategiyası, təhlükəsizliyin idarə edilməsi sistemi, təhlükəsizliyin idarə edilməsi proqramı, təhlükəsizliyin idarə edilməsi strukturu, modelin təkmilləşdirilməsi və onu dəstəkləyən metodologiya və müəssisənin biznes-sistemləridir.

İnT-nin idarə edilməsi proqramı təhlükəsizlik idarəçiliyinin, təhlükəsizliyin idarə edilməsi sisteminin, təhlükəsizlik siyasətinin, texnologiyanın, infrastrukturun və risk menecmentinin aqreqasiyasıdır. İnT-nin idarə edilməsi sistemi təhlükəsizliyin idarə edilməsinin proses modelindən, proses metodologiyasından və təhlükəsizlik proseslərinin təkmilləşdirilməsi modelindən ibarətdir.

İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi. İnformasiya təhlükəsizliyinin idarə edilməsi risklərin identifikasiyası və risklərin nəticələrinin azaldılması üçün adekvat nəzarət mühitinin yaradılmasını təmin edir. Bu ideya [166, s.755]-da öz təsdiqini tapır, müəlliflər bildirir ki, İnT təhlükəsizlik siyasətini, risklərin analizini, risklərin idarə edilməsini, fəaliyyətin fasiləsizliyinin planlaşdırılmasını və qəzadan sonra bərpanı nəzərdə tutur. İnformasiya təhlükəsizliyinin idarə edilməsinə praqmatik baxış fəaliyyətin fasiləsizliyini təmin etmək, ziyanı minimumlaşdırmaq və təhlükəsizlik üzrə fəaliyyəti xərclər baxımından effektiv təşkil etməkdən ibarətdir.

Hazırda İnT risklərinin idarə edilməsi üçün bir sıra standart beynəlxalq və milli metodologiyalar var: ISO/IEC 27005, NIST 800-30, OCTAVE, CRAMM və s. Analiz göstərir ki, İnT risklərinin idarə edilməsi metodologiyalarının çoxsaylı nöqsanları mövcuddur [33, s.6]: risklərin qiymətləndirilməsində əhəmiyyətli subyektivlik, risk qiymətləndirməni aparan mütəxəssislərin peşəkarlığına yüksək tələblər, qiymətləndirmənin nəticələrinin interpretasiyasında çətinlik, müdafiənin müxtəlif variantlarının obyektiv müqayisəli analizinin mümkün olmaması, müxtəlif metodlarla əldə edilmiş risk qiymətlərinin zəif korrelyasiyası, qalıq risklərin idarə edilməsi mexanizmlərinin yoxluğu, İnT insidentlərinə reaksiya proseslərinin keyfiyyətinin qiymətləndirilməsinin mümkün olmaması və s. Hətta böyük olmayan korporativ şəbəkələr üçün də riskin qısa müddətdə hesablanması problematikdir. Riskin dinamik hesablanması, riskin yayılması, riskin azaldılması üzrə uzlaşdırılmış qərar qəbul edilməsi modelləri olduqca vacibdir [33, s.6, 75, s. 10].

Daha bir nöqsan kimi risklərin idarə edilməsi üzrə mövcud metodların (və standartların, metodikaların) müəssisələr üçün nəzərdə tutulmasını qeyd edək. Bu metodların e-dövlət üçün ümumiləşdirilməsi problemlidir (və ya qeyri-mümkündür). Bu fikri belə bir fakt da sübut edir ki, hətta eyni bir metodologiyanın müəssisənin növündən (dövlət, özəl, hərbi və s.) və ölçülərindən (böyük, orta, kiçik) asılı olaraq müxtəlif variantları (məsələn, OCTAVE-S, OCTAVE-M və s.) vardır [75, s. 33]. Riskin reallaşması nəticəsində vurilan ziyanın (sosial, siyasi, maddi və s.) kəmiyyətcə qiymətləndirilməsi məsələsi də e-dövlət üçün çətindir.

Autentifikasiya və avtorizasiya metodları. E-dövlətdə elektron şəxsiyyət vəsiqəsi rolunu e-imza oynayır. Hazırda əksər ölkələrdə e-imza infrastrukturu yaradılmışdır və onun mobil texnologiyalar və bulud texnologiyaları əsasında təkmilləşdirilməsi üçün işlər görülür [14, s.138].

Vətəndaşların e-xidmətlərdən təhlükəsiz istifadəsini və mobilliyini təmin etmək üçün yeni nəsil fiziki şəxsiyyət vəsiqələrinə də e-imzaları yaratmaq və yoxlamaq üçün zəruri məlumatların daxil edilməsi nəzərdə tutulur. Lakin e-imza ilə onun sahibini əlaqələndirən məlumatlar təsadüfi generasiya edilmiş gizli açardır, onun imza sahibi ilə heç bir fiziki bağlılığı yoxdur. İmza sahibinin öz e-imzasından imtina etməməsi sənədi imzalamaq üçün istifadə edilmiş gizli açarın yalnız imza sahibinə məlum olmasına əsaslanır. Praktikada gizli və açıq açarların yaradılması və daşıyıcılara yazılması zamanı imza sahibi bilavasitə iştirak etmir. Eyni zamanda, çox zaman imza sahibinin texnoloji bilikləri yetərli olmadığından, imza prosesində kənar şəxslərin köməyindən istifadə edir. Burada müəyyən neqativ hallar, inamdan sui-istifadə halları ola bilər ki, bunların qarşısını almağın yeganə üsulu autentifikasiya üçün biometrik texnologiyalardan istifadə edilməsi [59, s.17, 277, s.410], avtorizasiya prosesində isə biometrik texnologiyalar ilə e-imza texnologiyalarının birləşdirilməsidir. Ümumiyyətlə, biometrik texnologiyalar ilə kriptoqrafik sistemlərin birləşdirilməsi aktual tədqiqat istiqamətləridir [46, s.18, 185, s.1888].

eID sisteminin idarə edilməsi informasiya cəmiyyətində mobillik, əlyetənlik və interoperabellik üçün əsas problemlərdən biridir. Bir sıra ölkələr müxtəlif eID sxemləri tətbiq edirlər. Bu işlərin sərhədlər boyunca yeni rəqəmsal baryerlər əmələ gətirməsinin qarşısını almaq, eID həllərin uyuşan olmasını təmin etmək üçün minimum tələblərin və ümumi standartların qəbul edilməsi vacibdir.

eID texnologiyalarının, o cümlədən e-imza və biometrik texnologiyaların, irimiqyaslı eID sistemlərinin qurulması problemlərinin, eID sistemlərinin kibercinayətkarlığa qarşı mübarizədə istifadə edilməsinin tədqiqi aktual tədqiqat istiqamətləridir [55, s.1-20, 125, s.24]. Hazırda şəbəkə vasitəsi ilə müxtəlif xidmətlər göstərən informasiya sistemlərinə ən geniş yayılmış təhdid "şəxsiyyət identifikatorlarının oğurlanması" (ing. ID-theft) hücumlarıdır. ABŞ Federal Ticarət

Nazirliyi hər il ID-theft üzrə statistik məlumatları dərc etdirir. Bir ID-theft zamanı orta hesabla 3 257 dollar ziyan vurulur [205, s.199].

Mürəkkəb sistemlərdə koordinasiya nəzəriyyəsi. Koordinasiya mürəkkəb sistemlərin idarə edilməsində mərkəzi funksiyalardan biridir və altsistemlərin hərəkətlərinin sistemin məqsədlərinə və idarəetməyə uyğun olaraq uzlaşdırılmasından və bu uzlaşmanın bütün idarəetmə tsikli ərzində saxlanılmasından ibarətdir.

Təəssüf ki, koordinasiya nəzəriyyəsi hazırda hələlik başlanğıc inkişaf mərhələsindədir. Müəlliflər [69, s.12]-də koordinasiyanın nəzəri əsaslarının yaradılması məsələsinə yetərli tədqiqatların həsr edilmədiyini vurğulayırlar. Koordinasiya modelləri qərar qəbuletmə nəzəriyyəsi və multiagent sistemləri çərçivəsində işlənilir [282, s.1-12]. Tədqiqatçıların əksəriyyəti M. Mesaroviç, D. Mako və İ. Takaharanın klassik "İyerarxik çoxsəviyyəli sistemlərin nəzəriyyəsi" kitabına istinad edirlər [63, s. 109]. Bu kitabda texnoloji və təşkilati proseslərin timsalında ikisəviyyəli sistemlərdə koordinasiya məsələlərinə və alınmış nəticələrin çoxsəviyyəli iyerarxik sistemlərə ümumiləşdirilməsinin mümkünlüyünə baxılır. Orada həmçinin mürəkkəb çoxsəviyyəli sistemlərdə koordinasiyanın üç baza prinsipi də formalaşdırılır. Onlara: 1) qarşılıqlı əlaqələrin proqnozlaşdırılması; 2) qarşılıqlı əlaqələrin həyata keçirilməsi və 3) qarşılıqlı əlaqələrin qiymətləndirilməsi aiddir. Bu prinsiplər konkret riyazi model və konkret tətbiq sahəsi çərçivəsində konkret alqoritmik formaya düşür. Onların arasında ən geniş məlum olan koordinasiya alqoritmləri, məsələn, lokal keyfiyyət göstəricilərinin təyin edilməsinə və razılaşdırılmasına əsaslanır ki, onların optimallaşdırılması qlobal göstəricinin optimallaşdırılmasına, ümumi resursun paylanmasına, ortaq dəyişənlərin qiymətlərinin razılaşdırılmasına və s. gətirib çıxarır.

Mürəkkəb iyerarxik sistemlərin koordinasiyasında aşağıdakı optimallaşdırma yanaşmaları istifadə edilir: iterasiyasız alqoritmlər, iterativ alqoritmlər və evristik metodlar.

Mövcud iterativ alqoritmlərdə optimal həll mərkəzlə elementlər arasında iterativ informasiya mübadiləsi gedişində müəyyən edilir, iterativ prosesin hər bir addımında isə altsistemlərin və koordinatorun lokal-optimal məsələləri həll edilir. Çoxsəviyyəli

iyerarxik sistemlərdə qərarların koordinasiyası üçün iterativ alqoritmlər böyük informasiya axını səbəbindən informasiya mübadiləsi üçün böyük zaman tələb edir.

İterasiyasız alqoritmlər layihələndirmə, planlaşdırma, resursların optimal paylanması məsələlərinin həllində, həmçinin real zamanda idarəetmə, optimallaşdırma, qərar qəbuletmə sistemlərində tətbiq edilir, onların əsas üstünlüyü iyerarxik səviyyələr arasında qlobal optimuma qədər informasiya ötürülməsinin azaldılmasıdır. İterasiyasız alqoritmlər, əsasən, effektiv həllər çoxluğunun qurulmasına gətirilir.

Evristik optimallaşdırma məsələləri çoxölçülü mühəndislik məsələlərində geniş yayılıb, onlarda ikisəviyyəli sistemlərin koordinasiya məsələlərində olduğu kimi, bir neçə axtarış fəzası var. Ən geniş yayılmış evristik metodlar genetik alqoritmlər, tabu axtarış alqoritmləri, evolyusiya alqoritmlərinin müxtəlif növləridir.

[37, s. 43]-də koordinasiya məsələlərinin lokal optimallaşdırma məsələləri, çoxsəviyyəli iyerarxik sistemin elementləri kimi həlli üçün yanaşma təqdim edilmiş və sənaye sistemləri üçün iterativ və qeyri-iterativ koordinasiya alqoritmləri təklif edilmişdir. [38, s. 164-195]-da qeyri-səlis çoxluqlara əsaslanan koordinasiya alqoritmləri təklif olunur. [37, 38]-də təklif olunan koordinasiya modelləri və metodları olduqca spesifikdir və koordinasiya məsələsinin həlli üçün altsistemlərin uyğun riyazi modellərinin olması və ya optimallaşdırma məsələsinin formalaşdırılması tələb olunur. [16, s.24]-da e-dövlətin İnT-nin təmin edilməsi sahəsində konseptual koordinasiya modeli təklif edilir və koordinasiyanın aktual problemləri analiz edilir.

İnformasiya təhlükəsizliyinin qiymətləndirilməsi metodları. İnformasiya təhlükəsizliyinin qiymətləndirilməsi, adətən, risklərin qiymətləndirilməsi ilə əlaqədardır, lakin İnT-nin təmin edilməsi üzrə fəaliyyət geniş məsələləri əhatə edir və qiymətləndirməni yalnız risk qiymətləndirməsi ilə məhdudlaşdırmaq düzgün deyil.

Ümumiyyətlə, İnT-nin qiymətləndirilməsi üzrə elmi tədqiqatlar və praktiki təşəbbüslər 2000-ci ildən bəri intensivləşmişdir. Müvafiq elmi-tədqiqat və praktik fəaliyyət istiqamətləri İnT metrikaları kimi müəyyən edilir [29, s.75]. Son illərdə İnT metrikaları və ölçmə modelləri üzrə bir sıra tədqiqat işləri aparılmışdır.

İnformasiya təhlükəsizliyinin idarə edilməsinin yetkinlik modelləri də təklif edilmişdir [197, s.1-9], bu modellərdə əsas diqqət təşkilatlara təklif edilən təhlükəsizlik servislərinə yönəldilir. Yetkinlik modeli müxtəlif səviyyələrdə tələb edilən təhlükəsizlik elementlərinin strukturlaşdırılmış toplusunu təqdim edir, bu elementlər təşkilatlara mövcud təhlükəsizlik nöqsanlarını identifikasiya etməyə və anlamağa, təhlükəsizliyin təmin edilməsinin gedişini müşahidə (monitorinq) etməyə, təhlükəsizlik siyasətlərini, ən yaxşı təcrübələri, keyfiyyəti, investisiyaları, təşkilati auditi monitorinq etməyə imkan yaradır.

İnT metrikaları üzrə bir sıra milli və beynəlxalq standartların işlənməsini də qeyd etmək olar. Məsələn, NIST SP 800-55 – informasiya sistemləri üçün təhlükəsizlik metrikalarının prinsipləri, NIST SP 800-80 – İnT üçün məhsuldarlıq metrikalarının işlənməsi prinsipləri, ISO/IEC 21827 – sistemlərin təhlükəsizlik mühəndisliyi potensialının yetkinlik modelini qeyd etmək olar.

E-dövlətin İnT-nin idarə edilməsi mürəkkəb məsələdir, e-dövlət texnologiyası inkişaf etdikcə təhlükəsizliyə daha yüksək tələblər irəli sürülür. E-dövlətin İnT olduqca dinamikdir və sürətlə inkişaf edir, o, innovativ yanaşma tələb edir, təhlükəsizlik periodik monitorinq edilməli, müvafiq texnologiyalar səmərəli tətbiq edilməli və İnT-nin idarə edilməsi daim təkmilləşdirilməlidir. Buna görə də, e-dövlətin İnT problemlərinin geniş tədqiq edilməsi və onların həlli üçün müvafiq yanaşmaların işlənilməsi zəruridir.

1.3. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin aktual elmi-praktiki problemləri

E-dövlətin İnT-nin idarə edilməsinin elmi problemlərini humanitar, elmi-texnoloji və kadr təminatı problemləri kimi üç əsas istiqamətdə qruplaşdırmaq olar. E-dövlətin İnT-nin idarə edilməsi üzrə aktual elmi-tədqiqat problemlərinə [7, s.3]-də baxılmış və onların müasir vəziyyəti analiz edilmişdir, İnT-nin qlobal aspektləri, informasiya müharibəsi, informasiya cəmiyyətinə olan təhdidlər, e-dövlətin etibarlı informasiya təminatı məsələləri geniş araşdırılmışdır. E-dövlətin İnT-nin idarə edilməsinin aktual multidissiplinar elmi-nəzəri problemləri, o cümlədən siyasi,

hüquqi, iqtisadi, sosial, mədəni-etik və kadr hazırlığı aspektləri [10, s.32]-də tədqiq olunmuş, həmin sahələr üzrə aktual elmi tədqiqat istiqamətləri müəyyənləşdirilmişdir.

Aşağıda e-dövlətin İnT-nin idarə edilməsi istiqamətində əsas elmi tədqiqat problemləri identifikasiya edilir. Problemlərin identifikasiyası zamanı vacib idarəetmə funksiyalarının nəzərə alınması, elmi ədəbiyyatda formalaşmış istiqamətlərə və İnT-nin idarə edilməsi üzrə beynəlxalq standartlar seriyasına mümkün qədər uyğunluq əsas meyarlar olaraq götürülmüşdür.

A1.1. İnformasiya sahəsində milli maraqlara təhdidlərin ranqlaşdırılması metodlarının işlənməsi

Təhdidlərin ranqlaşdırılması İnT üçün çox vacib prosesdir [9, s.46]. O, İnT-nin təmin edilməsinə ayrılmış resurslar çərçivəsində uyğun tədbirlərin prioritetini müəyyənləşdirməyə imkan verir. Siyasi və intellektual elitanın ölkənin İnT haqqında baxışlarında uzlaşmanın olmaması özlüyündə problemdir və təəssüf ki, az tədqiq olunmuşdur. Bu baxışları aşkarlamağın geniş yayılmış metodu anket sorğusu metodudur və ekspert sorğusu verilənlərinin statistik analizi, o cümlədən klaster analizi və korrelyasiya analizi, verilənlərin ümumiləşdirilməsi və nəticələrin interpretasiyası üzrə tədqiqatların aparılması aktualdır. Milli İnT-nin əsas təhdidlərinin ranqlaşdırılması zamanı siyasi və intellektual elitanı təmsil edən ekspertlərin qiymətləndirməsində uzlaşmama dərəcəsini minimallaşdırmaq olduqca vacibdir və dissertasiya işində konsensus ranqlaşdırma metodu təklif edilir [15, s.34].

A1.2. Qarşılıqlı asılı informasiya infrastrukturlarında İnT risklərinin modelləşdirilməsi

Bu işdə diqqət İnT risklərinin qiymətləndirilməsi metodlarının e-dövlət səviyyəsi üçün aşağıda göstərilən nöqsanına yönəldilir.

Mövcud metodologiyalarda risklər ayrı-ayrı komponentlər üzrə hesablanır və komponentlərin qarşılıqlı əlaqələrinin və asılılıqlarının nəzərə alınması problemi açıq qalır. Qarşılıqlı asılılıq ilə əlaqələndirilən ən mühüm parametr qarşılıqlı asılılığın təhlükəsizlik insidentlərinə bir neçə infrastruktura kaskad keçməsinə və onlara

əhəmiyyətli potensial təsir etmək imkanı verməsidir [49, s.102]. Məsələn, ilkin olaraq təsiri nisbətən kiçik və məhdud qiymətləndirilən bir hadisə əslində digər infrastrukturlar üçün əhəmiyyətli problemlər yarada bilər.

E-dövlətin informasiya infrastrukturu güclü qarşılıqlı asılılıqlara malik təhlükəsizlik domenlərindən ibarətdir. Bu domenlərdən birində baş verən riskin (məsələn, fəaliyyətin müvəqqəti, qismən və ya tam dayandırılması) kaskad təsirlə digər domenlərə yayılması, irimiqyaslı ziyan vurulması (sosial, siyasi, maddi və s.), fövqəladə halların və hətta milli təhlükəsizlik üçün təhdidin yaranması təhlükəsi var. Buna görə e-dövlətin informasiya infrastrukturu kimi mürəkkəb şəbəkə mühitində risklərin yayılmasının qiymətləndirilməsi məsələsi meydana çıxır.

A1.3. Milli İnternet infrastrukturunun dayanıqlığının modelləşdirilməsi

İnternet informasiyanın və biliklərin yayılmasının, innovasiyaların və iqtisadi inkişafın, elektron xidmətlərin göstərilməsinin güclü və olduqca effektli vasitəsidir. Qlobal şəbəkə dövlət orqanları, biznes sektoru və geniş əhali təbəqələri üçün böyük iqtisadi və sosial üstünlüklər təmin edir. Yüksək keyfiyyətli genişzolaqlı şəbəkə infrastrukturunun qurulması və onun əsasında təhlükəsiz, ucuz, keyfiyyətli İnternet xidmətlərinin təqdim olunması, əhalinin bu xidmətlərə çıxış imkanlarının yaradılması ölkəmizdə informasiya cəmiyyəti quruculuğunun əsas vəzifələrindən biridir. Nəhayət, İnternet hazırda baş verməkdə olan 4-cü sənaye inqilabının, kiber-fiziki-sosial sistemlərin meydana çıxmasının əsas hərəkətverici qüvvəsidir [79, s.212].

İnternet – mürəkkəb sistemdir, onun fəaliyyəti hər biri özünün spesifik məsələlərini həll edən müxtəlif komponentlər tərəfindən təmin edilir. İlkin yanaşmada, İnternetin infrastrukturunu kommunikasiya, ünvanlama və informasiya infrastrukturlarının məcmusu kimi təsəvvür etmək olar. Bu komponentlərin birinin normal fəaliyyətinə bədniyyətli müdaxilə edilməsi İnternetə əsaslanan xidmətlərin əlyetərliyinin pozulması ilə nəticələnir. Belə insidentlər olduqca təhlükəlidir, onların cəmiyyət həyatına təsirləri çox geniş ola bilər, bir sıra xidmətlərin işi uzun müddətə pozula bilər, iqtisadi itkilərə, neqativ siyasi, sosial nəticələrə səbəb ola bilər və s. Buna görə İnternet infrastrukturunun kiberhücumlara, kompüter viruslarının

yayılmasına, infrastruktur elementlərinin təsadüfi sıradan çıxmalarına qarşı dayanıqlığının modelləşdirilməsi aktual məsələdir [273, s.705, 70, s.190].

A2.1. Biometrik sistemlərdə informasiyanın aqreqasiyası metodlarının işlənməsi

Biometrik sistemlərin bir sıra çatışmazlıqları vardır ki, onlar biometrik sistemlərin irimiqyaslı tətbiqləri zamanı ciddi çətinliklər yaradır [73, s.60]. Bu nöqsanlar arasından spufinq hücumlarına (sistemin saxta biometrik nümunələrlə aldadılmasına) yüksək həssaslığı [73, s. 60, 34, s.16], bəzi insanlarda biometrik xarakteristikaların olmaması və ya biometrik sistemlərin işi üçün arzulanan keyfiyyətdə olmamasını, səhv qəbul faizinin (False Acceptance Rate, FAR) və səhv imtina faizinin (False Rejection Rate, FRR) nisbətən yüksək olmasını qeyd etmək olar.

Aydındır ki, biometrik sistemin qəbul və ya imtina barəsində qəbul etdiyi qərarın dəqiqliyi biometrik nümunənin keyfiyyətindən asılıdır. Buna görə, biometrik sistemlərin tanıma qabiliyyətini yaxşılaşdırmaq üçün qərar qəbulu zamanı biometrik nümunələrin keyfiyyət göstəricilərini nəzərə almağa imkan verən modellərin işlənməsi aktualdır.

A2.2. Biometrik sistemlərin təhlükəsizliyinin təkmilləşdirilməsi metodlarının işlənməsi

Biometrik texnologiyaların geniş yayılması ilə əlaqədar olaraq onların təhlükəsizliyi daha aktual olur. Son illər saxta biometrik nümunələrin aşkarlanması metodları və biometrik verilənlərin mühafizəsi metodları daxil olmaqla biometrik texnologiyaların təhlükəsizliyi məsələləri kifayət qədər intensiv tədqiq olunsa da, bəzi məsələlər lazımi diqqətdən kənarda qalmışdır, məsələn, süni dəyişilmiş barmaq izlərinin aşkarlanması məsələlərinə elmi ədəbiyyatda yalnız 2009-cu ildə baxılmışdı [47, s.11]. Süni dəyişilmiş barmaq izləri şəxsiyyətin gizlədilməsi məqsədi ilə barmaq izi naxışlarının qəsdən dəyişilməsini bildirir. Süni dəyişilmiş barmaq izləri saxta (mulyaj) barmaq izlərindən fərqlənirlər. Saxta barmaq izləri jelatin, lateks, silikon və s. düzəldilir və adətən özünü başqa şəxs kimi təqdim etmək üçün istifadə olunur. Süni

dəyişilmiş barmaq izlərini bədniyyətlilər çoxdan istifadə edirlər və dəfələrlə miqrasiya və hüquq-mühafizə orqanlarının təcrübəsində dəfələrlə təsadüf edilib, bir neçə belə hadisə haqqında mətbuatda da məlumat verilib [47, s.11].

Saxta barmaq izlərinin aşkarlanması üçün aparat və proqram təminatı əsasında müxtəlif yanaşmalar mövcuddur, [34, s.16]-də bu metodların icmalı verilib. Barmaq izlərini tanıma sistemlərinin dünyada ən geniş yayılmış sistemlər olduğunu, bu sistemləri aldatmaq üçün süni dəyişilmiş barmaq izlərinin praktikada istifadəsinin mümkünlüyünü [47, s.11, 307, s.451, 256, s.45] və onların aşkarlanması metodlarının hələlik geniş öyrənilmədiyini nəzərə alaraq, süni dəyişilmiş barmaq izlərinin aşkarlanması üçün metodların işlənməsi aktualdır.

A2.3. Biometrik kriptosistemlərin sintezi metodlarının işlənməsi

Biometrik sistemlər üçün olduqca aktual məsələlərdən biri biometrik şablonların etibarlı qorunmasıdır. Zəif qorunan və ya müdafiəsiz biometrik şablondan istifadə etməklə bədniyyətli biometrik autentifikasiya sistemindən keçə bilər, ilkin biometrik verilənləri bərpa edərək bu verilənlərdən fərd barəsində özəl məlumatlar əldə edə bilər. Biometrik şablonların qorunması üçün çoxsaylı metodlar təklif edilsə də, [239, s.1-4]-un müəlliflərinə görə "mövcud şablon mühafizəsi üsullarının əksəriyyəti praktiki biometrik sistemlərə olan bərpaetmə, təhlükəsizlik, gizlilik və yüksək tanıma dəqiqliyi kimi arzulanan tələblərin hamısını ödəyə bilmirlər." Bu nəticə praktikada ən geniş istifadə edilən barmaq izi sistemləri üçün də tam doğrudur.

Biometrik kriptosistem biometrik şablonların qorunması üçün ən ümidverici üsul hesab olunur [185, s.1888]. Biometrik kriptosistemlər biometrik nümunədən açar generasiya etməklə və ya açarı nümunəyə bağlamaqla biometrik şablonun mühafizəsi üçün həllər təqdim edir. Lakin mövcud biometrik kriptosistemlərin iş məhsuldarlığı adi biometrik sistemlərlə müqayisədə olduqca aşağıdır [200, s.555]. Praktiki tətbiqlər üçün yüksək göstəricilərə malik biometrik kriptosistemlərin işlənməsinə təxirəsalınmaz ehtiyac vardır.

A3.1. DDoS hücumlarının aşkarlanması metodunun işlənməsi. DDoS (Distributed Denial of Service – xidmətdən paylanmış imtina) hücumlarının

aşkarlanması uzun müddət araşdırılan sahələrdəndir və bir sıra maşın təlimi metodları işlənmişdir. DDoS hücumları aşkarlamaq üçün neyron şəbəkələr, dayaq vektor maşınları kimi maşın təlimi üsulları istifadə olunur [105, s.1-58]. Ənənəvi maşın təlimi alqoritmlərinin nöqsanlarından biri tanıma məsələsi üçün insan tərəfindən hazırlanmış əlamətlərdən istifadə etməsidir, əlamət mühəndisliyi adlı xüsusi bir tədqiqat istiqaməti vardır. Bu "həqiqi" mənada maşın təlimi deyil. Hücumların aşkarlanması üçün əlamətləri maşınının özünün aşkarlaması və strukturlaşdırılması arzu edilir.

Hazırda dərin təlim süni intellekt sahəsində ən intensiv tədqiqat istiqamətlərindən biridir [83, s.1-12] və ənənəvi maşın öyrənmə üsullarının məhdudiyyətlərini aradan qaldırmaq üçün geniş imkanlar açır. Ənənəvi maşın öyrənmə alqoritmləri tədqiqatçının köməyi ilə öyrənilir, istifadə olunacaq əlamətlər və bu əlamətlərin istifadə edilməsi üsulu tədqiqatçı tərəfindən müəyyən edilir. Dərin təlim metodları nitqin tanınması, təbii dilin emalı, kompüter görməsi və digər sahələrdə alternativ metodlardan daha yaxşı nəticələr verir [83, s.1-12].

Dərin təlim metodlarının müxtəlif sahələrdə uğurlu tətbiqləri kibertəhlükəsizlik sahəsində də diqqəti çəkir. Dərin təlim çox zaman dərin neyron şəbəkələri ilə eyniləşdirilir. Dərin neytral şəbəkələrin ümumi qəbul edilən bir tərifi yoxdur, adətən, birdən çox gizli layı olan neyron şəbəkələri dərin neyron şəbəkələri adlanır. Dərin neyron şəbəkələrinin uğurlu tətbiqinin səbəblərindən biri bu şəbəkələrin kiber hücumların aşkarlanması üçün lazım olan vacib əlamətlərin avtomatik çıxarmasıdır. Böyük verilənlərin email zamanı dərin neyron şəbəkələri əlamət çıxarışında insandan daha yaxşı işləyir. Dərin neyron şəbəkəsi bir neçə emal layından istifadə edərək verilənlərin çoxsəviyyəli abstraksiya ilə təsvirini öyrənir. Hər bir laydakı təsvir özündən əvvəlki layın təsviri əsasında formalaşdırılır.

Hələlik dərin təlim metodları DDoS hücumların aşkarlanması üçün az tətbiq olunur, yalnız bir neçə tədqiqat dərc edilmişdir [183, s.1-17]. DDoS hücumların real zamanda aşkarlanması dəqiqliyini artırmaq üçün dərin neyron şəbəkələrinə əsaslanan yanaşmaların işlənməsi aktualdır.

A3.2. İnformasiya təhlükəsizliyi insidentlərinin çoxmeyarlı prioritetləşdirilməsi

Müasir informasiya sistemlərində hər gün onlarla İnT insidenti baş verir. İnsidentlərin emalı ilə məşğul olan CERT komandalarının insan, texniki və maliyyə resursları məhdud olduğundan bir neçə insidentin eyni zamanda emalı zamanı insidentlərə müəyyən kriteriyalar əsasında prioritet təyin olunur və resurslar bu prioritetlərə uyğun olaraq insidentlər arasında paylanır. Prioritet insidentin emal növbəsini və reaksiya vaxtının standart normasını təyin edir. İnsidentlər təsadüfi zamanlarda baş verdiyi üçün onların prioritetlərinin dinamik müəyyən edilməsi və resursların yenidən paylanması məsələsi də meydana çıxa bilər (insidentin emalı dayandırıla və resurs daha təcili insidentə yönəldilə bilər). Mövcud metodologiyalarda prioritet yalnız iki kriteriya əsasında əvvəlcədən məlum olan matris əsasında təyin olunur [189, s. 278-283]. İnT insidentlərinin prioritetləri məyyən edilərkən digər kriteriyaların da nəzərə alınmasına, bu kriteriyalara çəkilər verilməsinə, insidentlərin prioritetlərinin təyin olunmasının çoxkriteriyalı qərar qəbuletmə məsələsi kimi həll edilməsinə ehtiyac vardır.

A3.3. İnformasiya təhlükəsizliyi insidentlərinin emalının optimal planlaşdırılması modelinin işlənməsi

İnformasiya təhlükəsizliyi insidentlərinin sayı sürətlə artır, lakin CERT-lərin büdcəsi yetərli sayda yüksək ixtisaslı mütəxəssis saxlamağa imkan vermir. Bunun nəticəsində bütün CERT-lərin qarşısında duran əsas problem insidentlərin emalı üzrə artan iş yükünü məhdud insan resursları şərtində optimal planlaşdırmaq məsələsidir. Buna görə, emal prioritetləri nəzərə alınmaqla insidentləri qısa müddətdə aradan qaldırmaq üçün CERT-qrupların işini optimal planlaşdırmağa imkan verən modellərin işlənməsi aktual məsələdir.

A4.1. İnT üzrə koordinasiya sisteminin qiymətləndirilməsi modellərinin işlənməsi

Hazırda e-dövlətin İnT-nin təmin edilməsi strategiyasının işlənməsində, qərarların qəbul edilməsində, İnT tədbirlərinin planlaşdırılmasında və həyata

keçirilməsində maraqlı tərəflərin cəlb edilməsi və onların fəaliyyətinin sinxronlaşdırılması və koordinasiyası üçün müxtəlif mexanizmlər istifadə edilir. Mövcud koordinasiya sisteminin adekvatlığını yoxlamaq, onun təşkilati effektivliyini yüksəltmək üsullarını tapmaq üçün koordinasiya strukturunu analiz etmək, koordinasiyada aparıcı rol oynayan aktorlarla yanaşı, strukturdakı boşluqları, "darboğaz"ları, funksional və təşkilati sərhədlərdəki maneələri aşkarlamaq üçün koordinasiya strukturunun adekvat modelləşdirilməsi aktual məsələlərdəndir.

A4.2. İnformasiya təhlükəsizliyi sistemlərində investisiyaların koordinasiyası

Koordinasiya həm də İnT sistemləri arasında qarşılıqlı asılılıqlardan qaynaqlanan uzlaşdırma problemlərini həll etmək, İnT sahəsində işlərin təkrarlanmasının qarşısını almaq, kapitaltutumlu İnT sistemlərindən kollektiv istifadəni təşkil etmək üçün də əhəmiyyətlidir. E-dövlətin İnT sistemi sıx qarşılıqlı əlaqədə olan İnT domenlərindən ibarətdir və bir domendə təhlükəsizliyin səviyyəsi onunla əlaqəsi olan domenlərə də təsir göstərir. Lakin domenlər qonşularının təhlükəsizlik vəziyyətini nəzərə almadan yalnız öz təşkilati maraqlarından çıxış edirlər və mərkəzi maliyyələşdirmə orqanından daha çox büdcə cəlb etməyə cəhd edirlər. Buna görə e-dövlətin İnT sistemində domenlərə ayrılan İnT investisiyaları koordinasiya edilməli, domenlərin qarşılıqlı əlaqəsi mütləq nəzərə alınmalıdır. Bu məqsədlə müvafiq modelləşdirmə metodlarının və vasitələrinin işlənməsi məsələsi qarşıya qoyulur.

A5.1 İnformasiya təhlükəsizliyi üzrə strateji qərarların qəbul edilməsi

E-dövlətin İnT-nin idarə edilməsi sistemində bir-biri ilə əhəmiyyətli qarşılıqlı təsirdə olan çoxsaylı (sosial, siyasi, texnoloji) proseslər baş verir. Bu proseslər zamana görə dəyişir, onlarada qeyri-müəyyənliyin müxtəlif növləri iştirak edir, lakin proseslərin dinamikası haqqında kəmiyyət informasiyası əlyetər olmur. Belə şəraitdə idarəetmə qərarları qəbul etmək üçün özünü doğrultmuş vasitələrdən biri qeyri-səlis yanaşmadır və e-dövlətin İnT-nin idarə edilməsinin müxtəlif strategiyalarının nəticələrini qabaqcadan analiz etmək üçün qeyri-səlis yanaşmalar əsasında müvafiq modelləşdirmə üsullarının işlənməsi də aktual məsələdir.

A5.2. Kibermüdafiə taktikalarının seçilməsi metodunun işlənməsi

Müasir yüksək dərəcədə şəbəkələşmiş dünyada İnT ilə bağlı qərarların əhəmiyyəti çox böyükdür və bu çox sayda maraqlı tərəflərin mənafeyinə toxunur. Buna görə də belə qərarlar yaxşı şəkildə qurulmalı, yaxşı öyrənilmiş nəzəri modellərə və ən yaxşı təcrübəyə əsaslanmalıdır. Belə nəzəri modelləşdirmə vasitələrindən biri oyunlar nəzəriyyəsidir.

Oyunlar nəzəriyyəsi iqtisadi agentlərin qarşılıqlı təsirlərini analiz etmək üçün əlverişli bir vasitədir və ilk olaraq iqtisadiyyata tətbiq olunmuşdu, hazırda hərbi strategiyalara, beynəlxalq münasibətlərə, siyasi elmlərə, təkamül biologiyasına və s. geniş tətbiq olunur [144, s. 31-75, 238, s. 19-54]. Oyunlar nəzəriyyəsi İnT-nin strateji və taktiki idarə edilməsi üzrə qərarların qəbulunda qiymətli yanaşmalar təqdim edə bilər. İnT-ndə bədniyyətlilərlə müdafiə tərəfinin qarşılıqlı təsir prosesinə də oyun prosesi kimi baxmaq olar. Oyunlar nəzəriyyəsini hücum davranışlarını proqnozlaşdırmaq və qərarların qəbul edilməsini dəstəkləmək üçün istifadə etmək olar.

A5.3. İnformasiya təhlükəsizliyinin situasiya idarəetməsi

Situasiya baxılan zamanda obyektin fəaliyyətinə əhəmiyyətli dərəcədə təsir göstərən hadisələrin konkret toplusudur. E-dövlətin İnT-nin etibarlı təmin edilməsi üçün mürəkkəb dinamiki situasiyaları fasiləsiz və avtomatik identifikasiya etmək və onlara real zaman rejimində reaksiya vermək zəruri şərtdir. Buna görə situasiyaların tanınması, proqnozlaşdırılması, analizi və idarə edilməsinin effektiv metodlarının işlənməsi tələb edilir, sadalanan əməliyyatlar birlikdə situasiya idarəetməsi adlanır. E-dövlətin İnT-nin situasiyalar üzrə idarə edilməsi modelini presedentlər nəzəriyyəsi əsasında reallaşdırmaq məqsədəuyğundur. İnformasiya təhlükəsizliyi situasiyası və bu situasiyada qəbul edilmiş qərarlar haqqında biliklərin presedentlər kimi təsviri, cari situasiyaya uyğun presedentlərin seçilməsi, presedent əlamətlərinin çəkilərinin optimallaşdırılması və s. üçün yanaşmaların işlənməsi zəruridir. Təklif ediləcək yanaşmanı idarəetmənin taktiki və strateji səviyyələri üçün də ümumiləşdirmək olar.

A7.1. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiyaların formalaşdırılması

İnT-nin təmin edilməsi üçün dövlətlər arasında beynəlxalq koordinasiya da olduqca vacib əhəmiyyət daşıyır. Bir çox ölkə kiberfəzada oxşar kibertəhdidlərlə qarşılaşır və öz kibertəhlükəsizliyini təmin etmək üçün yetərli resurslara malik deyillər. Bu vəziyyətdə ölkələrin qarşılıqlı faydalılıq əsasında öz səylərini birləşdirməsi və kibertəhlükəsizlik sahəsində koalisiya şəklində mübarizə aparması daha məqsədəuyğundur. Lakin ölkələrin siyasi, iqtisadi və milli təhlükəsizlik maraqları bu məsələnin həllinə maneə ola bilər. Fərz olunur ki, müəyyən ölkələrin bu maraqları antaqonist deyil və onlar zəruri zəmanətlərlə ortaq İnT xidmətləri təşkil etmək üçün danışıqlar yolu ilə koalisiyalar təşkil edə bilərlər. Belə koalisiyaların formalaşdırılmasını, xərclərin və uduşun koalisiya ölkələri arasında bölgüsünü modelləşdirmək üçün yanaşmaların təklif edilməsi aktualdır.

A8.1. E-xidmətlərin İnT-nin qiymətləndirilməsi metodunun işlənməsi

E--xidmətlərin İnT-nin səviyyəsi əsasında e-dövlətin İnT-nin idarə edilməsinin effektivliyi barədə fikir söyləmək olar. E-xidmətlər (və digər paylanmış sistemlər) yüksək heterogenliyi, dinamik təbiəti, demərkəzləşdirilmiş idarəetməsi, istifadəçilərin məsafədən girişləri, müxtəlif təhlükəsizlik siyasətlərinə malik bir neçə inzibatə domenə səpələnməsi, lokal və qlobal əməliyyatlardan istifadə etməsi səbəbindən başqa sistemlərə nisbətən İnternetdə müxtəlif təhdidlərə qarşı daha həssasdır. Müasir e-xidmətlər qorunması lazım olan böyük həcmli konfidensial məlumatların (fərdi məlumatlar, billinq məlumatları, e-tibb məlumatları və s.) istifadə olunması ilə xarakterizə olunur. Belə sistemlərdə İnT-nin təmin edilməsi trivial məsələ deyil və e-xidmətlərin geniş ictimaiyyət tərəfinfən qəbul edilməsi üçün vacib şərtdir [181, s.1-6].

E-xidmət provayderlərini və istifadəçilərini daima bir sual maraqlandırır: e-xidmətlər hansı səviyyədə təhlükəsizdir? Buna görə də e-xidmətlərin təhlükəsizliyinin modelləşdirilməsi və kəmiyyət qiymətləndirilməsi üsulları tələb olunur [103, s.17].

A8.2. Milli kibertəhlükəsizlik indeksinin qiymətləndirilməsi metodunun işlənməsi

Hazırda kibertəhlükəsizlik milli İnT-nin vacib komponentlərindən birinə çevrilmişdir [26, s.16]. Kibertəhlükəsizlik sürətlə dəyişən sahədir, dinamik bazar yeni texnologiyaların meydana çıxmasına və kibertəhdidlər mühitinin inkişafına güclü təkan verir. Dövlətlər kibertəhlükəsizliyin təmin edilməsinə ayrılan resursları artırmağa məcbur olurlar. Lakin "Nəticədə nə dərəcədə təhlükəsizik?" sualına cavab tapmaq olduqca çətindir. Buna görə də, dövlətin kibertəhlükəsizliyinin ölçülməsi aktual məsələdir.

Kibertəhlükəsizliyin ölçülməsi özlüyündə məqsəd deyildir, kibertəhlükəsizliyin effektiv idarə edilməsinə xidmət edir. Milli kibertəhlükəsizlik indeksi ölkələrin kibertəhlükəsizlik təşəbbüsləri baxımından vəziyyətlərini müqayisə etmək, effektiv kibertəhlükəsizlik siyasətləri və strategiyaları işləmək üçün zəruri alətlərdən biridir. Lakin milli kibertəhlükəsizlik indeksinin işlənməsi sahəsində elmi tədqiqatlar və praktiki işlər erkən mərhələdədir, onların metodoloji əsaslandırılması qənaətbəxş və tam deyil [26, s.16]. Milli kiber-təhlükəsizlik səviyyəsini necə ölçmək, hansı ölçmə indikatorlarını əsas götürmək, mümkün ölçmələrin nə dərəcədə adekvat olması kimi məsələlərə aydınlıq gətirilməlidir. Milli kibertəhlükəsizlik indeksi kibertəhlükəsizliyin cari səviyyəsini də əks etdirməlidir.

A8.3. E-dövlətin İnT-nə vətəndaş etimadının qiymətləndirilməsi metodunun işlənməsi

Elmi tədqiqatlar və ölkələrin e-dövlət quruculuğu təcrübəsi göstərir ki, vətəndaşların e-dövlətə inamının vacib komponentlərindən biri e-dövlətin informasiya təhlükəsizliyidir [97, s.165]. Vətəndaşlar təhlükəsizliyi şübhəli olan veb-saytdan istifadə etməkdənsə, ənənəvi üsullardan istifadə etməyi üstün tuturlar. Buna görə vətəndaşların e-dövlətin İnT-nə etimadının təmin edilməsi e-dövlətin həqiqi potensialından tam istifadə edilməsi üçün xüsusi əhəmiyyət daşıyır və e-dövlətin inkişafının yeni mərhələsində daha aktual problemə çevrilir. Bu baxımdan e-dövlətin İnT-nə vətəndaşların etimadına təsir edən faktorları və etimadın qurulması

mexanizmlərini analiz etmək, etimadın səviyyəsini qiymətləndirmək üçün modellər işləmək tələb edilir.

I fəsil üzrə nəticələr

- E-dövlətin İnT-nin idarə edilməsi problemlərinin müasir vəziyyəti analiz və tədqiqi edilərək bu sahədə aktual multi-dissiplinar elmi-nəzəri və elmi-praktiki problemlər müəyyən edilmişdir [7, s.3-13, 10, s.32-43, 19, s.19-26, 30, s.80-82, 73, s.60-63, 77, s.1-5, 78, s.644-648, 79, s.212-223].
- E-dövlətin İnT-nin idarə edilməsinin məqsədlərini, əsas idarəetmə funksiyalarını və e-dövlətin İnT-nə təsir edən əsas faktorları müəyyən konseptual modeli təklif edilmişdir [18, s.20-31];
- E-dövlətin İnT-nin idarə edilməsi üzrə aktual elmi-tədqiqat problemləri müəyyən edilmiş və onların müasir vəziyyəti analiz edilmişdir [7, s.3-13];
- E-dövlətin İnT-nin idarə edilməsi üzrə elmi-tədqiqatların prioritet istiqamətləri müəyyən edilmişdir [19, s.19-26].

II FƏSİL. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ RİSKLƏRİNİN QİYMƏTLƏNDİRİLMƏSİ METODLARI VƏ MODELLƏRİ

E-dövlətin İnT-nə yönəlmiş strateji risklər informasiya sahəsində milli maraqları hədəfə alır. İnformasiya sahəsində milli maraqlara çoxsaylı təhdidlər mövcuddur və kibermüdafiəyə ayrılan resursların məhdudluğu şəraitində bu təhdidlərə qarşı effektiv əks-tədbirlər görmək üçün bu təhdidlərin çoxkriteriyalı konsensus ranqlaşdırılması zəruridir [15, s.34].

E-dövlətin infrastrukturu güclü qarşılıqlı asılılıqları olan kritik informasiya infrastrukturlarından ibarətdir. E-dövlət inkişaf etdikcə bu qarşılıqlı asılılıq daha da güclənir, bu, e-xidmətlərin keyfiyyətini daha da yüksəltməyə imkan verir. Lakin bu qarşılıqlı asılılıq həm də e-dövlətin İnT üçün böyük təhdidlərdən birinə çevrilir. Məsələ ondadır ki, bu infrastrukturlardan birinin fəaliyyətinin pozulması bütün e-dövlət ekosisteminə katastrofik təsir göstərə bilər. Bir infrastrukturda baş verən kiçikmiqyaslı riskin digər infrastrukturlara kaskad şəklində yayılması, irimiqyaslı maddi, sosial, siyasi və s. ziyan vurması, fövqəladə halların yaranması təhlükəsi mövcuddur. Lakin mövcud metodlarda İnT riskləri ayrı-ayrı informasiya infrastrukturları üzrə hesablanır və bir qayda olaraq, infrastrukturların qarşılıqlı asılılıqları nəzərə alınmır. Buna görə e-dövlət mühitində İnT risklərinin qiymətləndirilməsi zamanı infrastrukturların qarşılıqlı asılılıqları mütləq nəzərə alınmalıdır [49, s.102].

Kritik infrastrukturların əsas kommunikasiya və idarəetmə magistralı isə İnternetdir və buna görə ölkənin İnternet infrastrukturunun dayanıqlığını e-dövlətin təhlükəsizliyinin olduqca vacib komponenti hesab etmək olar. Buna görə, bu fəsildə İnternetin milli infrastrukturunun irimiqyaslı kiberhücumlara və təsadüfi qəzalara qarşı dayanıqlığının qiymətləndirilməsi məsələsinə də baxılır [25, s.15, 51, s.36].

2.1. E-dövlətin informasiya təhlükəsizliyi təhdidlərinin konsensus ranqlaşdırılması metodu

İnformasiya təhlükəsizliyinin təmin edilməsi istənilən dövlətin daxili və xarici siyasətinin ən vacib məsələlərindən biridir. Dövlətin İnT-nə informasiya sahəsində

milli maraqların təmin olunduğu vəziyyət kimi baxmaq olar. İnformasiya sahəsi – informasiyanı, dövlətin informasiya infrastrukturunu, informasiyanın toplanmasını, formalaşdırılmasını, yayılmasını və istifadəsini həyata keçirən subyektləri və onlar arasındakı ictimai münasibətləri tənzimləyən sistemi əhatə edir. Müasir şəraitdə dövlət mürəkkəb və dinamik dəyişən İnT mühiti ilə qarşılaşır, bu mühit digər dövlətlərdən, transmilli terrorçuluq və cinayətkarlıq şəbəkəsindən, yeni texnologiyalardan qaynaqlanan təhdidlərlə xarakterizə edilir. Belə təhdidlərə informasiya müharibəsi [220, s. 15-49], kiberterroizm, kibercinayətkarlıq, kibercasusluq, kibersabotaj, fərdi məlumatların oğurlanmasını və s. aid etmək olar [136, s.25-27].

İnformasiya sahəsinin müasir təhdidlərdən qorunması hazırki zamanda milli təhlükəsizliyin təmin edilməsinin prioritet istiqamətlərindən biridir [204, s.20]. İnformasiya təhlükəsizliyi təhdidlərinin bütün spektri izlənməli, zamanında aşkarlanmalı və qiymətləndirilməli, onların təsirini yolverilən səviyyədə saxlamaq üçün səmərəli tədbirlər həyata keçirilməlidir. Lakin praktikada, xüsusilə müxtəlif resursların məhdudluğu şəraitində, İnT-nin təmin edilməsi riskin müəyyən qiymətinə yol verməklə, təhlükəsizliyin tələb edilən səviyyəsinin optimallaşdırılması yolu ilə həyata keçirilir. Buna görə, təhdidlər güman edilən nəticələr əsasında prioritetlərinə görə ranqlaşdırılmalı, strukturlaşdırılaraq təhdidlərin və müvafiq reaksiyaların iyerarxiyası işlənməlidir [15, s.34].

E-dövlətin İnT-nə təhdidlərin ranqlaşdırılması bu təhdidlərə qarşı təxirəsalınmaz tədbirlərin görülməsi üçün vacibdir. Belə əks-tədbirlər sistemli yanaşma və siyasi, iqtisadi, təşkilati və texniki vasitələrin istifadəsini nəzərdə tutur. Lakin baxılan məsələlərin elmi və praktiki əhəmiyyətinə baxmayaraq, elmi ədəbiyyatda təhdidlərin qiymətləndirilməsinə və ranqlaşdırılmasına hələlik hamılıqla qəbul edilmiş yanaşmalar işlənməmişdir [19, s.19].

Bu bölmənin məqsədi e-dövlətin İnT-nə təhdidlərin ranqlaşdırılması üçün metodoloji yanaşmanın işlənməsidir [15, s.34]. Yanaşmanın əsası kimi çoxkriteriyalı qərar qəbulu metodologiyası götürülür və bu metodologiyanın əsas mərhələlərinə uyğun olaraq, təhdidlərin (alternativlərin) siyahısının müəyyən edilməsi,

kriteriyaların seçilməsi, kriteriyaların çəkilərinin müəyyən edilməsi və təhdidlərin qiymətləndirilməsi məsələlərinə baxılır. Təhdidlərin konsensus ranqlaşdırılması üçün optimallaşdırma modeli təklif edilir və ədədi nümunədə eksperimentlərin nəticələri təqdim edilir.

Tədqiqat məsələsinin qoyuluşu

Fərz edək ki, n sayda A_i $(i = 1,2, \dots, n)$ milli kibertəhlükəsizlik təhdidlərinin siyahısı tərtib edilib (rəsmi sənədlərin [3, 5], elmi tədqiqatların və kütləvi informasiya vasitələrində olan məlumatların əsasında). Tutaq ki, İnT-nin siyasi, hüquqi, iqtisadi, hərbi, texnoloji aspektlərini öyrənən alimlər, İnT-nin təmin edilməsində böyük iş təcrübəsi olan praktiklər, jurnalistlər, ictimai xadimlər, hüquq müdafiəçiləri kimi vətəndaş cəmiyyəti nümayəndələri arasından p sayda DM_k $(k = 1,2, \dots, p)$ ekspert seçilmişdir. 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 qiymətləndirilməsi 6-ballıq şkala ilə aparılır: 0 – Təhdid yoxdur; 1 – Aşağı; 2 – Məqbul; 3 – Orta; 4 – Əhəmiyyətli; 5 – Yüksək.

Qiymətləndirmə hər bir ekspert tərəfindən həyata keçirilir və $\mathrm{X}^k = \left(X_{ij}^k\right)_{n\times m}$ $k = 1,2, \dots, p$ 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 x_{ij}^k-da yuxarıdakı k indeksi yazılmır):

$$x_{ij} = \frac{X_{ij}}{\sum_{i=1}^{n} X_{ij}} \qquad (2.1.1)$$

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.

İnformasiya sahəsində milli maraqlar və onlara təhdidlər. İnformasiya təhlükəsizliyinin təmin edilməsi üzrə dövlətin daxili və xarici siyasətinin strateji və cari məsələləri informasiya sahəsində ölkənin milli maraqları əsasında formalaşdırılır. Buna görə e-dövlətin İnT-nə təhdidlərin müəyyən edilməsi və onların qiymətləndirilməsi üçün kriteriyaların seçilməsi üçün informasiya sahəsində ölkənin milli maraqları identifikasiya edilməlidir. İnformasiya sahəsində ölkənin milli maraqlarını rəsmi dövlət sənədləri (milli təhlükəsizlik konsepsiyası [5], İnT konsepsiyası, doktrinası, müvafiq qanunvericilik sənədləri) əsasında identifikasiya etmək olar. Məsələn, Rusiya Federasiyasının 2000-ci ildə qəbul edilmiş İnT doktrinasında informasiya sahəsində ölkənin milli maraqlarının aşağıdakı komponentləri müəyyən edilir (2016-cı ildə qəbul edilmiş yeni doktrinada fərqli siyahı verilir) [15, s.34]:

- informasiya azadlığının təmin edilməsi;
- ölkənin milli mənəvi dəyərlərinin və ənənələrinin, mədəni və elmi potensialının qorunması və inkişafı;
- dövlət siyasətinin informasiya təminatı;
- informasiya resurslarının icazəsiz girişlərdən qorunması, informasiya və telekommunikasiya sistemlərinin təhlükəsizliyinin təmin edilməsi.

Ölkələrdə İKT-nin yetkinlik səviyyəsi müxtəlifdir, ona görə konkret ölkələr üçün informasiya sahəsində milli maraqların və onlara olan təhdidlərin fərqli kateqoriyaları identifikasiya edilə bilər. Lakin qloballaşma nəticəsində bir çox İnT problemi əksər ölkələr üçün eynidir.

E-dövlətin İnT təhdidlərinin ranqlaşdırılması məsələsinə operativ, taktiki və strateji idarəetmə səviyyələrində, qısa- və uzunmüddətli perspektivdə baxmaq olar. Bu işdə strateji təhdidlərə baxılır. E-dövlətin İnT-nə strateji təhdidlər milli miqyasda insidentlərlə nəticələnə bilən təhdidlərdir. Strateji təhdidlərin iki əsas kateqoriyasını fərqləndirmək olar [15, s.34]:

- Baxılan zaman kəsiyində İnT-nə davamlı təhlükə yaradan təhdidlər;

- Nəticəsi böyük, ehtimalı qeyri-müəyyən olan təhdidlər – hazırki trendlərin dramatik inkişafı nəticəsində meydana çıxan daha əhəmiyyətli təhdidlər.

E-dövlətin İnT-nə strateji təhdidlərin yuxarıdakı əsas kateqoriyalarını onlara uyğun sub-kateqoriyalarda da strukturlaşdırmaq olar.

Son dövrlər əksər qabaqcıl ölkələrdə milli kibertəhlükəsizlik strategiyaları qəbul edilmişdir [27, s.42]. Bu strategiyalar ölkələrin informasiya sahəsindəki milli maraqlarından çıxış edərək yaxın 5-10 ildə əsas potensial təhdidləri identifikasiya edərək onların neytrallaşdırılması üzrə fəaliyyətin əsas istiqamətlərini müəyyən edirlər. Milli kibertəhlükəsizlik strategiyalarının analizi göstərir ki, bu strategiyalarda aşağıdakı əsas təhdid sinifləri müəyyən edilir [204, s.34-43]: kibercasusluq, kiberterrorizm, kiberekstremizm, kibercinayətkarlıq, kritik infrastruktura kiberhücumlar, fərdi verilənlərə kiberhücumlar.

Strateji təhdidlərin qiymətləndirilməsinin periodikliyinə gəlincə, misal olaraq göstərmək olar ki, milli səviyyədə risklərin qiymətləndirilməsinin Birləşmiş Krallıqda qəbul edilmiş qaydasına görə belə risklərin qiymətləndirilməsi hər beş ildən bir həyata keçirilməlidir [249, s. 267].

Təhdidlərin qiymətləndirilməsi üçün kriteriyalar

Təhdidlərin idarə edilməsinin həyat tsiklinə aşağıdakı iterativ mərhələləri aid etmək mümkündür: potensial təhdidlərin aşkarlanması, təhdidlərin analizi, təhdidlərin qiymətləndirilməsi, təhdidlərin dəyərləndirilməsi – prioritetlərinin müəyyən edilməsi (ranqlaşdırılması) və təhdidin potensial təsirlərinin azaldılması istiqamətində uyğun əks-tədbirlərin seçilməsi və həyata keçirilməsi.

Təhdidin aşkarlanması (identifikasiyası) – fasiləsiz prosesdir, sistemi əhatə edən daxili və xarici mühit real təhdidlərin mövcudluğunu müəyyənləşdirmək üçün fasiləsiz monitorinq edilir. Təhdidlər təhdidin əsas komponentləri istifadə edilməklə analiz edilir: təhdidin aktorları, təhdidin aktorlarının məqsədləri və potensial imkanları, təhdid aktorlarının hədəfləri, təhdidin istifadə etdiyi boşluqlar, təhdidin reallaşma texnologiyası və təhdidin fəsadları.

Təhdid aktorlarına dövlətlər, terrorçular (kiber və ya digər), sənaye casusları, cinayətkarlar, haktivistlər, əyləncə hakerləri və s. aid ola bilər. E-dövlətin İnT-nə təhdidlərin xarici və daxili mənbələrini fərqləndirmək olar.

Təhdidlər boşluqlar vasitəsilə reallaşdırılır (kiberhücum edilir), boşluqlara yenilənməmiş proqram təminatı, yüksək vəzifəli əməkdaş və s. aid ola bilər. Kiberhücumlara DDoS hücumları, kibercasusluq və s. nümunə ola bilər.

Təhdidin qiymətləndirilməsi zamanı təhdidin əsas faktorları – təhdidin başvermə ehtimalı və təhdidin hədəfə nə dərəcədə təsir etdiyi qiymətləndirilir. Təhdidin başvermə ehtimalı təhdid aktorunun potensialından və niyyətindən asılıdır. Təsir iqtisadi ziyan, insan tələfatı, sosial və struktur dəyişiklikləri şəklində özünü göstərə bilər. Təhdidin potensial təsiri bu faktorlar nəzərə alınmaqla ölçülməli, təhdidin əməliyyatlara və strateji maraqlara olan təsirinin səviyyəsini əks etdirməlidir. Dövlətin informasiya təhlükəsizliyinə təhdidlərin təsiri irimiqyaslı və ehtimalı qeyri-müəyyən ola bilər. Lakin bu kəmiyyətlərin praktikada qiymətləndirilməsi problemlidir [66, s.34]. Buna görə təhdidin vurduğu mütləq zərər əvəzinə nisbi zərər kriteriyasından istifadə etmək daha məqsədəuyğundur, o, mahiyyətcə təhdidin müəyyən milli maraq üçün yaratdığı təhlükəni xarakterizə edir. Təhdidin milli maraq üçün nisbi təhlükəliliyi ekspertlər tərəfindən verbal əlamətlər üzrə qiymətləndirilir. Təhdidlərin nisbi təhlükəliliyini qiymətləndirmək üçün qeyri-səlis məntiq əsasında çoxkriteriyalı qərar qəbulu metodlarından istifadə etmək olar [15, s.34].

Məsafə əsasında kriteriya çəkilərinin müəyyən edilməsi metodu

Kriteriyaların çəkilərinin müəyyən edilməsinin ənənəvi metodlarına ekspert metodları, Delphi metodu, AHP metodu, variasiya əmsalı metodu və entropiya əsasında metodlar daxildir [308, s.307]. Bu yanaşmalardan ilk üçündə qərar qəbul edənlərin subyektiv təsiri mövcuddur. Son iki metodda isə çəkilər ekspertlərin birbaşa iştirakı olmadan müəyyən edilir. Əvvəlki üç metodla müqayisədə onların əsas üstünlüyü kriteriyaların çəkilərinin müəyyən edilməsində ekspertlərin subyektivliyinin aradan qaldırılmalarıdır. Bu ekspertlərin çəkilərin qiymətlərində uzlaşmadıqları hallarda çox faydalıdır.

Kriteriya çəkilərinin müəyyən edilməsi üçün entropiya əsasında metodu. Entropiya əsasında kriteriyaların çəkilərinin hesablanması prosesi aşağıdakı addımlardan ibarətdir:

(a) *j*-cu kriteriya üçün entropiyanın hesablanması. Hər bir C_j kriteriyası üçün entropiya qiyməti aşağıdakı kimi hesablanır:

$$E_j = -k \sum_{i=1}^{n} x_{ij} log(x_{ij}) \tag{2.1.2}$$

burada k sabitdir və $k = 1/\log(m)$ münasibəti ilə müəyyən edilir, m kriteriyaların sayıdır.

(b) Hər bir C_j kriteriyası üçün dispersiya ölçüsü. *j*-cu kriteriya entropiya metodunda dispersiya ölçüsü belə müəyyən edilir:

$$\varphi_j = 1 - E_j \tag{2.1.3}$$

(c) Kriteriya çəkilərinin müəyyən edilməsi. Hər bir *Cj* kriteriyası üçün çəki aşağıdakı kimi hesablanır:

$$w_j^C = \frac{\varphi_j}{\sum_{j=1}^{m} \varphi_j} \tag{2.1.4}$$

Kriteriya çəkilərinin məsafə əsasında müəyyən edilməsi metodu. Məsafə əsasında çəkilərin hesablanması metodu aşağıdakı kimi işləyir:

(a) *j*-cu kriteriya üçün optimist/pessimist qiymətlərin müəyyən edilməsi. Hər bir C_j kriteriyası üçün optimist və pessimist qiymətlər belə müəyyən edilir:

$$\text{Optimist qiymətlər: } U^+ = (U_1^+, U_2^+, \dots, U_m^+) \tag{2.1.5}$$

$$\text{Pessimist qiymətlər: } U^- = (U_1^-, U_2^-, \dots, U_m^-) \tag{2.1.6}$$

burada

$$U_j^+ = \begin{cases} \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{2.1.7}$$

$$U_j^- = \begin{cases} \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{2.1.8}$$

burada J_1 pozitiv kriteriyaları (məsələn, gəlir), J_2 neqativ kriteriyaları (məsələn, xərc) təsvir edir.

(b) Kriteriya qiymətləri ilə optimist/pessimist qiymətlər arasında məsafələrin hesablanması. j-cu kriteriyanın (j = 1, 2, ..., m) qiymətləri ilə optimist/pessimist kriteriya qiymətləri arasındakı məsafə belə hesablanır:

$$d_j^+ = \sqrt{\sum_{i=1}^{n} \left(x_{ij} - U_j^+\right)^2} \tag{2.1.9}$$

$$d_j^- = \sqrt{\sum_{i=1}^{n} \left(x_{ij} - U_j^-\right)^2} \tag{2.1.10}$$

(c) Hər bir C_j kriteriyası üçün dispersiya ölçüsü belə müəyyən edilir:

$$\xi_j = \frac{d_j^+}{d_j^+ + d_j^-} \tag{2.1.11}$$

(d) Kriteriya çəkilərinin hesablanması. Dispersiya ölçüsünün əsasında hər bir *Cj* kriteriyasının çəkisi müəyyən edilir:

$$w_j^C = \frac{\xi_j}{\sum_{j=1}^{m} \xi_j} \tag{2.1.12}$$

Kriteriya çəkiləri müəyyən edildikdən sonra i-ci alternativin qərar qiyməti aşağıdakı additiv formada hesablana bilər:

$$z_i = \sum_{j=1}^{m} w_j^C x_{ij}, i = 1,2, \dots, n \tag{2.1.13}$$

Konsensus ranqlaşdırma üçün optimallaşdırma metodu

Hər bir ekspert standart MCDM prosesini yerinə yetirərək özünün verdiyi qiymətlər əsasında alternativlərin yekun ranqlarını ala bilər. Məsələ bu fərdi ranqları qrup konsensus ranqlarında aqreqasiya etməkdən ibarətdir [15, s.34, 180, s.12].

Çəkili konsensus ranqlaşdırma məsələsini 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. Məqsədimiz $\boldsymbol{r}^*$ 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:

$$argmin_{\boldsymbol{w},\boldsymbol{r}^*}(1-\lambda)\sum_{i=1}^{p} w_i\|\boldsymbol{r}^* - \boldsymbol{r}_i\|^2 + \lambda\|\boldsymbol{w}\|^2, \qquad (2.1.14)$$

$$\text{Şərtlər: } \sum_{i=1}^{p} w_i = 1, w_i \geq 0, \forall i, \qquad (2.1.15)$$

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 ranq vektoru ilə $\boldsymbol{r}^*$ arasındakı çəkili məsafəni ölçür və (2.14) tənliyindəki birinci həddhər bir ekspert üçün bu məsafəni minimallaşdırmaq üçün istifadə olunur. (2.14) tənliyindəki ikinci toplanan çəkilərin hamarlığını təmin edən requlyarlaşdırma həddidir.

Bu məsələ xətti məhdudiyyətlərlə kvadratik funksiyanın optimallaşdırılması məsələsidir və onun sürətli həlli üçün [291, s.513]-də təklif edilmiş alqoritmi istifadə etmək olar.

Eksperimental analiz

Bu bölmədə təklif edilmiş konsensus ranqlaşdırma metodunun reallaşdırılması prosesini izah etmək üçün illüstrativ ədədi misal təqdim olunur. Fərz edək ki, aşağıdakı beş təhdid verilib:

- A_1 – kibercasusluq;
- A_2 – kiberterrorizm;
- A_3 – kibercinayətkarlıq;
- A_4 – kritik infrastruktura kiberhücumlar;
- A_5 – fərdi verilənlərə kiberhücumlar.

Fərz edək ki, üç ekspert bu təhdidləri aşağıda verilmiş kriteriyalara nəzərən qiymətləndirir:

- C_1 – e-dövlət servislərinin işinin pozulması dərəcəsi;
- C_2 – intellektual mülkiyyətə vurulan ziyanın səviyyəsi;
- C_3 – fərdi məlumatlara təhlükəlilik dərəcəsi.

Cədvəl 2.1.1-də bu üç kriteriya və beş təhdid üçün hər bir ekspertin verdiyi qiymətlər əsasında qurulmuş normallaşdırılmış qiymətləndirmə matrisləri verilib. Qeyd edək ki, baxılan qiymətləndirmə kontekstindən hər üç kriteriya pozitiv kriteriyadır.

Cədvəl 2.1.1.

Çoxkriteriyalı qərar qəbulu üçün ədədi misal

Təhdidlər	DM_1			DM_2			DM_3		
	C_1	C_2	C_3	C_1	C_2	C_3	C_1	C_2	C_3
A_1	0,43	0,43	0,14	0,23	0,38	0,39	0,20	0,50	0,30
A_2	0,17	0,33	0,50	0,17	0,42	0,41	0,50	0,25	0,25
A_3	0,29	0,14	0,57	0,23	0,38	0,39	0,27	0,27	0,46
A_4	0,33	0,25	0,42	0,40	0,30	0,30	0,62	0,13	0,25
A_5	0,45	0,36	0,18	0,25	0,33	0,42	0,10	0,40	0,50

Cədvəl 2.1.2-də hər bir ekspertin verdiyi qiymətləri əsasında kriteriyaların çəkilərinin müxtəlif metodlar ilə müəyyən edilməsinin nəticələri göstərilir.

Cədvəl 2.1.2.

Müxtəlif yanaşmalarla müəyyən edilmiş kriteriya çəkiləri

Ekspert	Kriteriya	Entropiya əsasında metod		Məsafə əsasında metod	
		φ_j	w_j^C	ξ_j	w_j^C
DM_1	C_1	-0,4197	0,3548	0,2437	0,4238
	C_2	-0,4110	0,3474	0,1555	0,2704
	C_3	-0,3524	0,2978	0,1758	0,3058
DM_2	C_1	-0,4268	0,3174	0,2437	0,5804
	C_2	-0,4587	0,3112	0,1198	0,2853
	C_3	-0,4590	0,3414	0,0564	0,1343
DM_3	C_1	0,3742	0,3618	0,2679	0,4739
	C_2	0,3394	0,3282	0,1765	0,3122
	C_3	0,3204	0,3101	0,1209	0,2139

Cədvəl 2.1.2-də verilmiş kriteriya çəkilərindən istifadə etməklə (2.1.13) düsturu ilə təhdidlərin qiymətləndirilməsini almaq olar, nəticələr Cədvəl 2.1.3-də təqdim olunur. Cədvəl 2.1.3-dən göründüyü kimi, müxtəlif ekspertlər konkret təhdid üçün kriteriya çəkilərinin təyin edilməsi metodundan asılı olaraq müxtəlif qiymətlər ala bilər. Bundan başqa, hətta eyni ekspert çəkilərin tapılmasının müxtəlif metodlarından

istifadə etdikdə qiymətləndirmə nəticələri müxtəlif ola bilər. Buna görə müxtəlif səviyyələrdə iki aqreqasiya variantı vardır: müxtəlif ekspertlərin qərarlarının aqreqasiyası və eyni ekspertin müxtəlif çəki təyinetmə metodu ilə aldığı qərar nəticələrinin aqreqasiyası.

Cədvəl 2.1.3.

Standart MCDM prosesində alınmış qərar qiymətləri

Çəki metodu	Ekspert	A_1	A_2	A_3	A_4	A_5
Entropiya əsasında metod	$DM_1(z_1)$	0,3436	0,3239	0,3213	0,3290	0,3383
	$DM_2(z_2)$	0,3244	0,3246	0,3244	0,3227	0,3254
	$DM_3(z_3)$	0,3295	0,3405	0,3289	0,3445	0,3225
Məsafə əsasında metod	$DM_1(z_1)$	0,3413	0,3142	0,3351	0,3359	0,3431
	$DM_2(z_2)$	0,2943	0,2736	0,2943	0,3580	0,2957
	$DM_3(z_3)$	0,3151	0,3685	0,3106	0,3879	0,2792

Cədvəl 2.1.3-dəki təsviri bir qədər dəyişməklə Cədvəl 2.1.4-də belə aqreqasiya senarisini asanlıqla almaq olar.

Cədvəl 2.1.4.

Müxtəlif çəki təyinetmə metodları üzrə qiymətləndirmənin nəticələri

Qərar qəbul edən	Çəki metodu	A_1	A_2	A_3	A_4	A_5
DM_1	Entropiya əsasında metod	0,3436	0,3239	0,3213	0,3290	0,3383
	Məsafə əsasında metod	0,3413	0,3142	0,3351	0,3359	0,3431
DM_2	Entropiya əsasında metod	0,3244	0,3246	0,3244	0,3227	0,3254
	Məsafə əsasında metod	0,2943	0,2736	0,2943	0,3580	0,2957
DM_3	Entropiya əsasında metod	0,3295	0,3405	0,3289	0,3445	0,3225
	Məsafə əsasında metod	0,3151	0,3685	0,3106	0,3879	0,2792

Cədvəl 2.1.5-də müxtəlif çəki təyinetmə metodlarının nəticələrinin hər bir ekspert üzrə aqreqasiyası göstərilib.

Cədvəl 2.1.5.

Müxtəlif çəki təyinetmə metodlarının nəticələrinin aqreqasiyası

	A_1	A_2	A_3	A_4	A_5
DM_1	0,3459	0,3107	0,3290	0,3336	0,3464
DM_2	0,3149	0,3086	0,3149	0,3391	0,3102
DM_3	0,3314	0,3486	0,3178	0,3535	0,3068

Növbəti məsələ üç müxtəlif ekspertin alınmış aqreqasiya nəticələrinin yekun qərarda birləşdirilməsidir. Burada əsas məsələ ekspertlərin çəkilərinin müəyyən edilməsidir. Baxılan misal üçün (2.1.14)-(2.1.15) məsələsinin həllindən tapılmış ekspertlərin çəkilərindən istifadə etməklə hesablanmış yekun qərar nəticələri cədvəl 2.1.6-da göstərilib.

Cədvəl 2.1.6.

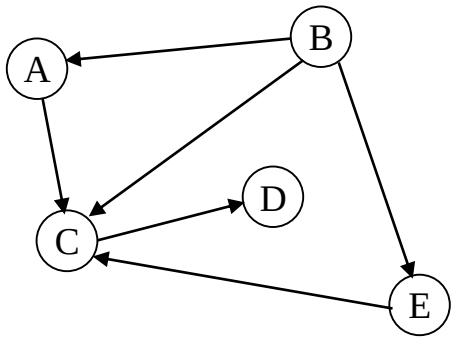
Ekspertlərin qiymətlərinin aqreqasiyasi ilə alınmış yekun ranqlaşdırma

Yekun qərar	A_1	A_2	A_3	A_4	A_5
Aqreqasiya edilmiş qərar qiyməti	0,3307	0,3226	0,3206	0,3421	0,3211
Rank	2	3	5	1	4

Cədvəl 2.1.6-dan görünür ki, təhdid A_4 (kritik infrastruktura kiberhücumlar) ən yüksək ranqa malikdir, sonra A_1 (kibercasusluq), A_2 (kiberterrorizm), A_5 (fərdi verilənlərə kiberhücumlar) və A_3 (kibercinayətkarlıq) təhdidləri gəlir. Beləliklə, üç müxtəlif kriteriya üzrə üç ekspert tərəfindən qiymətləndirilmiş beş təhdiddən ən təhlükəlisi A_4-dür.

2.2. Qarşılıqlı asılı informasiya infrastrukturlarında informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi metodu

E-dövlətin İnT-də ən çətin problemlərdən biri e-dövlətin informasiya infrastrukturları arasında qarşılıqlı asılılıqların müəyyən edilməsi və onlarla əlaqəli risklərin qiymətləndirilməsidir. Bu bölmədə e-dövlətin qarşılıqlı asılı kritik informasiya infrastrukturlarında İnT risklərinin kəmiyyət qiymətləndirilməsi üçün yeni yanaşma təklif edilir [49, s.102].



Şəkil 2.2.1. Qarşılıqlı asılı infrastrukturlar üçün risk asılılıqları qrafı

Kritiklik e-dövlətin əsas funksiyalarının təmin edilməsi, əsas e-xidmətlərin fəaliyyəti, e-xidmətlərin təhlükəsizliyi və s. baxımından müəyyən edilir. E-dövlətin Kİİ-ına misal e-hökumət veb portalı, mühüm e-xidmət sistemləri, e-imza üçün sertifikat mərkəzləri sistemi, İnternet infrastrukturu, elektron ödəniş sistemi və s. ola bilər. Fərz edilir ki, e-dövlətin Kİİ-ınn identifikasiyası və təsnifatı Elektron Dövlətin Milli Operatoru (EDMO) tərəfindən həyata keçirilir.

Şəkil 2.2.1-də qarşılıqlı asılı Kİİ üçün risklərin asılılıq qrafına misal göstərilir. Qrafın qovşaqları arasında istiqamətlənmiş tillər birinci tərtib asılılığı, yəni iki Kİİ arasındakı birbaşa informasiya asılılığını göstərir. İkinci tərtib asılılığa misal $B \rightarrow$

$A \rightarrow C$ asılılıqlar zənciri ola bilər. B infrastrukturundakı risk A-ya keçir və onun vasitəsilə C infrastrukturuna yayılır. Bu işdə birinci tərtib asılılıqlara baxılır və məqsəd bir Kİİ-da yaranan bir riskin ondan asılı olan kritik infrastrukturlarda təsirlərini qiymətləndirməkdir.

Burada risklərin kəmiyyət qiymətləndirməsinin işlənməsi üçün maliyyə institutlarında qəbul edilmiş əməliyyat risklərinin qiymətləndirilməsi metodları istifadə edilir [110, s. 15-31]. Əlbəttə, əməliyyat riskləri anlayışı İnT risklərindən bir qədər genişdir, lakin aydındır ki, InT riskləri əməliyyat risklərinin çox əhəmiyyətli hissəsidir. Buna görə də, İnT risklərinin qiymətləndirilməsi üçün əməliyyat risklərinin qiymətləndirilməsi metodlarını uyğunlaşdırılması məqsədəuyğun görünür.

Əlaqədar işlərin analizi

1. Qarşılıqlı asılı infrastrukturlarda risklərin qiymətləndirilməsi metodları

Qarşılıqlı asılı infrastrukturlarda risklərin qiymətləndirilməsi kritik infrastrukturların mürəkkəbliyi və təbiəti səbəbindən mürəkkəb məsələdir. Kritik infrastrukturlarda risklərin öyrənilməsi üçün güclü motivasiya 2003-ci ildə Şimali Amerika və Avropada elektrik təchizatı şəbəkələrində kütləvi açılma hadisələri olmuşdur [49, s.102]. Ədəbiyyatda aşkar edilmiş qarşılıqlı asılılıq modelləri analizin seçilmiş səviyyəsi ilə fərqlənir – tədqiqatçılar mikroskopik və ya makroskopik səviyyəni seçirlər. Müəlliflər [278, s.44]-də diqqəti kritik infrastruktur komponentlərində cəmləyirlər (mikroskopik səviyyədə) və bəzi infrastruktur növləri arasında xətti və tsiklik asılılıqlar üçün multi-asılılıq strukturlarının bir neçə növünü nümayiş etdirirlər.

[158, s.297]-də risklərin qiymətləndirilməsi və qarşılıqlı asılı makroiqtisadi və infrastruktur sistemlərinin idarə edilməsi üçün bir neçə analitik metodologiya nəzərdən keçirilir. Onlara dağıdıcı hadisələrin iqtisadi təsirini qiymətləndirmək, mürəkkəb sistemləri müxtəlif perspektivlərdən təsvir etmək və texnoloji prosesləri idarəetmə sistemlərinə kiberhücumlar riskini qiymətləndirmək üçün modellər daxildir. [261, s.63] elektrik şəbəkəsində baş verən qəzanın telekommunikasiya şəbəkəsindəki nəticələrini araşdırır. Müəlliflər İtaliyada bir yüksək gərginlikli elektrik

ötürmə şəbəkəsinə baxırlar və onun internet-magistralından funksional asılılıqlarını araşdırırlar. [216, s.811] heterogen nəqliyyat şəbəkələri üçün vahid risk qiymətləndirməsi platforması təqdim edir, risk qarşılıqlı asılı şəbəkələr arasında "risklərin yayılması matrisi" vasitəsilə yayılır, qarşılıqlı asılılıqların təbiəti və təhdidlərin tipləri nəzərə alınır. Qarşılıqlı asılı Kİ-larda risk qiymətləndirməsinin bəzi metodları Leontyev giriş/çıxış modelini istifadə edir, müxtəlif sektorların Kİ-larının əlyetərliyinin pozulmasına görə iqtisadi itkiləri onların qarşılıqlı asılılıqları əsasında hesablanır [91, s.243].

[283, s.128]-də infrastrukturların kritikliyini qiymətləndirmək üçün üç səviyyəli kompleks metodologiya təklif olunur: Kİ operatoru səviyyəsi, sektor səviyyəsi və milli səviyyə. Hər bir səviyyənin xüsusiyyətləri, həm də onların qarşılıqlı asılılığı müəyyən edilir. Təklif olunan metodologiyanın əsas elementi müxtəlif infrastrukturların və onların müvafiq sektorlarının qarşılıqlı asılılığının formal tərifidir. İnfrastrukturlar arasında qarşılıqlı asılılıqlar interfeys kimi çıxış edir, onların vasitəsilə təhdidlər və onların təsirləri digər infrastrukturlara ötürülür. Müasir risk qiymətləndirməsi metodologiyaları bu problemi effektiv şəkildə həll etməyə imkan vermir, buna görə bu interfeyslərin formallaşdırılması kritikliyi qiymətləndirmənin vahid metodologiyasının müəyyən edilməsi üçün əsas elementdir. Qeyd edək ki, infrastrukturun kritikliyi keyfiyyətcə qiymətləndirilir, müəlliflər risklərin qiymətləndirilməsi üçün kəmiyyət metodologiyalarının hazırlanması zərurətini vurğulayırlar. [208, s.104] bir təhlükəsizlik insidentinin bir neçə infrastrukturda potensial kaskad təsirlərinə baxır. Təklif olunan metod təkcə birinci tərtib asılılıqlara baxdıqda əhəmiyyətsiz olan, lakin bir neçə tərtib asılılıqları nəzərə aldıqda əhəmiyyətli potensial təsirə malik olan təhdidləri müəyyən etməyə imkan yaradır.

2. Əməliyyat risklərinin qiymətləndirilməsi metodları

Bazel II razılaşmasında əməliyyat riski vacibliyinə görə bazar və kredit riskləri ilə eyniləşdirilir və maliyyə institutlarından onları qarşılamaq üçün kifayət qədər kapital ehtiyatları təmin etmək üçün bu risklərin qiymətləndirilməsi məcburi tələb edilir [93, s.11]. Bu sənədə görə, əməliyyat riski "qeyri-adekvat və ya səhv daxili

proseslər, əməkdaşların və sistemlərin hərəkətləri və ya xarici hadisələr nəticəsində zərər riski" kimi müəyyən edilir. Bu tərifə görə, IT-təhlükəsizlik təhdidləri (insayderlərin hərəkətləri, icazəsiz giriş, zərərli proqram təminatı və s.) əməliyyat risklərinin ayrılmaz bir hissəsidir.

Bazel II razılaşmasında əməliyyat risklərinin qarşılanması üçün kapitalın müəyyənləşdirilməsi modellərinə 3 yanaşma təklif olunub: baza indikatorları metodu (Basic Indicator Approach, BIA), standartlaşdırılmış yanaşma (The Standardized Approach, TSA), təkmilləşdirilmiş metod (Advanced Measurement Approach, AMA) [49, s.102, 143, s.527].

Əməliyyat risklərinin kəmiyyət qiymətləndirməsi üçün istifadə edilən modellərin əksəriyyəti LDA yanaşmasına əsaslanır. LDA metodu aktuar yanaşma kimi də tanınır, çünki oxşar modellər uzun illər ərzində sığorta sahəsində oxşar məsələlərin həll üçün istifadə edilmişdir [143, s.527].

LDA-nın mahiyyəti riskin iki xarakteristikasının qiymətləndirilməsini ayırmaqdır: zərərin tezliyi (ing. loss frequency, F) və zərərin həcmi (ing. loss severity, S). Zərərin tezliyi F – müəyyən müddət ərzində əməliyyat riski hadisələrinin sayını göstərən təsadüfi kəmiyyətdir, zərərin həcmi S – hər bir ayrı-ayrı halda ziyanı təsvir edən təsadüfi kəmiyyətdir.

Bankın fəaliyyəti səkkiz istiqamətə bölünür (ing. business lines): "1) korporativ maliyyə; 2) maliyyə bazarlarında əməliyyatlar; 3) pərakəndə bank xidmətləri; 4) hüquqi şəxslərə xidmət; 5) hesablaşmalar və ödənişlər; 6) agent xidmətləri; 7) aktivlərin idarə edilməsi; 8) broker xidmətləri" [49, s.102].

Bazel Komitəsi 7 növ risk hadisəsini də standartlaşdırır: "1) daxili dələduzluq; 2) xarici dələduzluq; 3) əmək münasibətləri və əməyin təhlükəsizliyi; 4) müştərilər, bank məhsulları, biznes praktikası; 5) maddi aktivlərə zərər vurulması; 6) proseslərin idarə edilməsi; 7) sistemlərdə imtinalar"[49, s.102].

"Fəaliyyət istiqaməti/risk hadisəsinin tipi" şəklində əməliyyat riski hadisələri matris şəklində təsvir olunan 56 mümkün kombinasiya formalaşdırır. Kombinasiyaların hər biri üçün əsas problem bu göstəricilərin paylanmasını qiymətləndirməkdir [49, s.102].

Göstəricilərin hər biri üçün öz paylanması araşdırılır, çünki fərz olunur ki, rəhbərliyin qərarları bu parametrlərin hər birinə ayrı-ayrılıqda təsir edir. Paylanmanın parametrləri momentlər metodu və ya maksimum həqiqətəoxşarlıq metoduu ilə müəyyən edilir. İki paylanma əsasında ziyanın paylanması qurulur [90, s.49].

Fəaliyyət istiqamətlərinin və risk hadisələrinin 56 kombinasiyası üçün ziyanların tezliyi asılı olmayan təsadüfi kəmiyyətlərdir. Ziyanların həcmləri də təsadüfi kəmiyyətlərdir və bütün kombinasiyalarda eyni paylanır. Belə şərtlər 56 kombinasiyanın hər birini ayrı-ayrılıqda nəzərdən keçirməyə imkan verir.

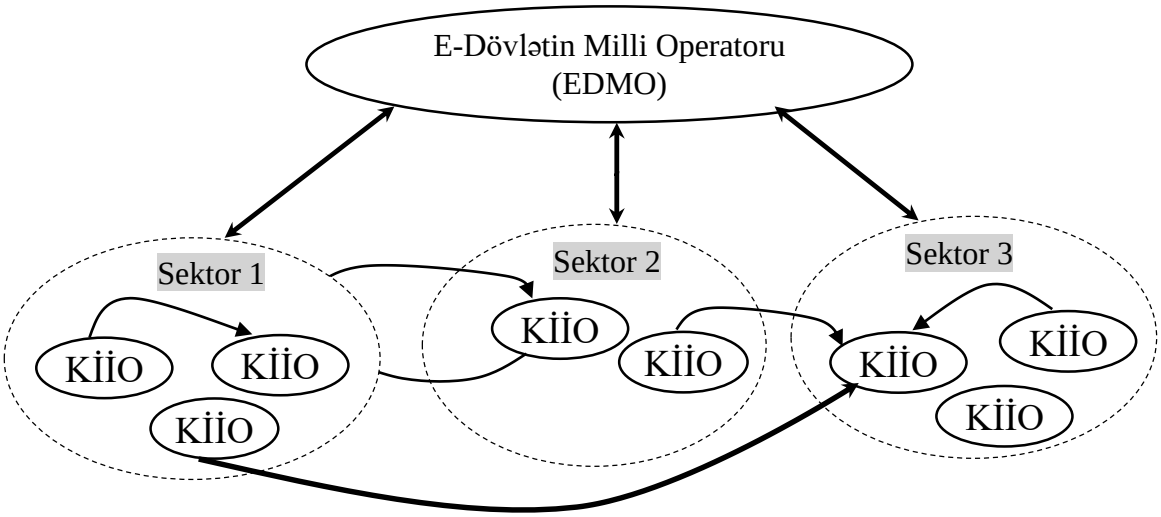
LDA yanaşmasında istifadə olunan stoxastik modellərin geniş analizi [119, s.37-60]-da verilir. Əməliyyat risklərinin qiymətləndirilməsi metodlarını İnT sahəsində tətbiq etmək cəhdləri vardır, məsələn [294, s.106, 49, s.102].

Qarşılıqlı asılı informasiya infrastrukturlarında risklərin qiymətləndirilməsi metodu

Təklif edilən yanaşmanın komponentləri aşağıda A-F bölmələrində izah edilir.

A. E-dövlətin Kİİ-da qarşılıqlı asılılıqlarının modelləşdirilməsi

Bu bölmədə e-dövlətin Kİİ-nın qarşılıqlı asılılıqlarının ikisəviyyəli iyerarxik modeli təklif edilir. 8 Kİİ və 3 sektor (məsələn, maliyyə, İKT, dövlət) nümunəsi şəkil 2.2.2-də göstərilib. Aşağı səviyyədə Kİİ-nin operatorları (KİİO) yerləşirlər. Yuxarı səviyyədə EDMO fəaliyyət göstərir.



Şəkil 2.2.2. Hipotetik Kİİ qarşılıqlı asılılıqlarının ikisəviyyəli iyerarxik modeli

Kritik informasiya infrastrukturlarının operatoru EDMO ilə sektorun Koordinatoru vasitəsilə qarşılıqlı əlaqədə olur. Koordinator KİİO ilə EDMO arasında interfeys kimi çıxış edir.

İstənilən KİİO-nun (özəl şirkət, dövlət orqanı və ya müəyyən şəxs) əsas qayğısı öz biznes əməliyyatlarını, İKT aktivlərini və sistemlərini təhlükəsizlik təhdidlərindən qorumaqdır. KİİO səviyyəsində risklərin analizi mikroskopik səviyyədə həyata keçirilir, riskləri qiymətləndirərkən həm daxili, həm də xarici təhdidlərə baxıla bilər. Lakin KİİO bütün riskləri müəyyən edə bilmir.

Həqiqətən də, hər bir KİİO yalnız özünün asılı olduğu giriş risklərini öyrənir, digər KİİO-larına və ya bütün sektora mümkün təsirləri, həmçinin bütün e-dövlət infrastrukturu üçün təsirləri və riskləri analiz etmir.

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 öz potensial risklərini qiymətləndirir.

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 təsvir 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.

B. Qarşılıqlı asılı informasiya infrastrukturlarında İnT riskinin qiymətləndirilməsi metodu

Məqsədimiz bir Kİİ-da reallaşan riskin qarşılıqlı asılı digər Kİİ-larında təsirini qiymətləndirməkdir. Bu məsələ üçün LDA yanaşmasının tətbiqi üçün əvvəlcə "fəaliyyət istiqamətlərini" və "risk hadisələrini" (RH) müəyyən etmək lazımdır. Bizim modeldə "fəaliyyət istiqamətləri" kimi seçilmiş Kİİ ilə birinci tərtib asılılıqları

olan Kİİ-larını götürmək təbiidir. Risk hadisələrinin növləri kimi isə CERT komandaları tərəfindən emal edilən İnT insidentlərinin kateqoriyalarını götürəcəyik [8]. Reallaşmış İnT riski aşkarlanan zaman CERT-komandanın informasiya bazasında insident kimi qeydiyyata alınır və insidentin kateqoriyasından asılı olaraq müəyyən prosedurlar üzrə emal olunur. Bəzi ölkələrdə aşkarlanmış bütün İnT insidentlərinin milli CERT-in verilənlər bazasında qeydiyyata alınması qanunvericiliklə tələb edilir. Buna görə CERT-lərin məlumat bazaları İnT üzrə statistik verilənlərin qiymətli mənbəyi ola bilər və bizim modeldə də İnT insidentlərinin kateqoriyalarının risk hadisələrinin tipi kimi seçilməsi məqsədəuyğundur. Qeyd edək ki, US-CERT insidentlərin 7 kateqoriyasını müəyyən edir: CAT 0 – Şəbəkə müdafiəsinin test edilməsi; CAT 1 – İcazəsiz giriş; CAT 2 – Xidmətdən imtina (Denial of Service, DoS); CAT 3 – Zərərli kod; CAT 4 – Düzgün olmayan istifadə, CAT 5 – Skanlama/Zondlama/Giriş cəhdi; CAT 6 – Təsdiqlənməmiş insidentlər.

Tutaq ki, müəyyən infrastruktur üçün j-cu tip risk hadisəsinin qiymətləndirilməsi tələb edilir. Tutaq ki, EDMO verilmiş "Kİİ/risk hadisəsi" kombinasiyası üçün asılı infrastrukturlar siyahısını müəyyən etmişdir. Onları 1, 2, … m kimi işarə edək. LDA-nın tətbiqi i = 1, 2, … n və verilmiş j üçün hər bir Kİİi-RHj kombinasiyası üçün zərər tezliyini və zərər həcmini modelləşdirmək və sonra ümumi zərərin paylanmasını hesablamaq üçün onların birləşdirilməsindən ibarətdir. Fərz edək ki, müəyyən müddət ərzində j-cu risk hadisəsinin reallaşması nəticəsində infrastrukturlara vurulan zərərlər haqqında məlumatlar EDMO-na məlumdur.

Aşağıdakı işarələri qəbul edək:

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

$$P_{ij}(n) = \sum_{k=0}^{n} p_{ij}(k). \quad (2.2.1)$$

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

$$L_{ij} = \sum_{k=1}^{N_{ij}} X_{ij}(k) = X_{ij}(1) + X_{ij}(2) + \cdots + X_{ij}(N_{ij}), \quad (2.2.2)$$

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

L_{ij} təsadüfi kəmiyyəti üçün paylanma funksiyası itkinin aqreqativ paylanması adlanır və burada G_{ij} kimi işarə olunur. Onun analitik şəkli aşağıdakı düsturla verilən mürəkkəb paylanmadır:

$$G_{ij}(x) = P(L_{ij} \le x) = \begin{cases} \sum_{n=1}^{\infty} p_{ij}(n) F_{ij}^{n\star}(x), x > 0 \\ p_{ij}(0), x = 0 \end{cases} \quad (2.2.3)$$

burada $n \star F$ paylanma funksiyasının öz-özü ilə n-qat bürünməsini bildirir.

Modeli sadələşdirmək üçün aşağıdakı fərziyyələr qəbul edilir:

Fərziyyə 1. N_{ij} tezliyi və itkilərin həcmi X_{ij} asılı olmayan təsadüfi kəmiyyətlərdir;

Fərziyyə 2. İtkilərin həcmi X_{ij} asılı olmayan və eyni paylanmış təsadüfi kəmiyyətdir.

Birinci fərziyyədən aydındır ki, itkilərin tezliyi ilə həcminə təsadüfiliyin iki asılı olmayan mənbəyi kimi baxılır. Bu 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 paylanmışdır.

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

$$T_j = \sum_{i=1}^{m} L_{ij}. \quad (2.2.4)$$

C. İtkilərin tezliyinin modelləşdirilməsi

İtkilərin tezliyini Puasson paylanması kimi modelləşdirmək standart hesab edilir. Bu yetərincə güclü fərziyyədir, o cümlədən ona görə ki, riyazi gözləmənin və dispersiyanın bərabərliyini nəzərdə tutur, lakin bu həmişə empirik şəkildə dəstəklənmir [212, s. 1-3]. 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. Bu fərziyyə [165, s.2-15]-də təxminən üç il müddətində 260 000-dən çox kompüter sistemində aşkarlanmış bütün müdaxilələr analiz edilərək yoxlanmışdı. Nəticələr göstərmişdi ki, Puasson prosesi haqqında fərziyyə qeyri-optimal ola bilər – loq-normal paylanma həm aşkar edilmiş müdaxilələrin sayı, həm də müdaxilələr arasındakı zaman müddəti üçün daha yaxşı idi. Pareto paylanması ilk müdaxilə üçün tələb edilən zamanı modelləşdirmək baxımından daha yararlıdır. Həmin məqalədə kompüter sisteminə hər uğurlu müdaxilədən sonra müdaxilə müddətinin (ing. Time To Compromise, TTC) artmasını da analiz edir. Nəticələr göstərir ki, müdaxilə üçün tələb edilən müddət müdaxilələrin sayına görə azalır.

D. İtkilərin ölçüsünün modelləşdirilməsi

Ekstremal hadisələri nəzərə almaq üçün itkilərin ölçüsü ağır quyruqlu paylanmalar ilə təsvir olunur. İtkilərin ölçüsünü təsvir etmək üçün istifadə olunan tipik ehtimal modelləri loq-normal, qamma və Veybull paylanmaları və ümumiləşdirilmiş Pareto paylanmasıdır. Son zamanlar tədqiqatçıların diqqəti daha dərin analitik analiz imkanı verən loq-normal paylamasına yönəlmişdir [119, s. 51].

E. Aqreqativ itkilərin modelləşdirilməsi

Əksər hallarda, itkilərin aqreqativ paylanması G-nin analitik təsvirini əldə etmək çətindir. Buna görə G-nin yaxınlaşması imitasiya modelləşdirməsinin köməyi ilə tapılır. İmitasiya modelləşdirməsinin ən geniş yayılmış metodu Monte-Karlo metodudur [143, s.527].

F. Ekstremal itkilərin ölçüsünün modelləşdirilməsi

Böyük itkilərin modelləşdirilməsi üçün ekstremal qiymətlər nəzəriyyəsinin (Extreme Value Theory, EVT) tətbiq edilməsi təklif edilir, onun əsasında təsadüfi kəmiyyətlərin ekstremumlarının paylanmasının asimptotik qanunauyğunluqları dayanır [114, s. 45-73]. Belə ki, 1975-ci ildə C. Pikandsın aldığı nəticəyə görə, X təsadüfi kəmiyyətinin "pik nöqtələrinin", yəni onun kifayət qədər böyük u sərhəd qiymətini keçmələrinin asimptotik paylanması müəyyən şərtlərdə ümumiləşdirilmiş Pareto paylanmasına (Generalized Pareto Distribution, GPD) yığılır:

$$\Pr(X - u < x \mid X > u) \approx GPD(\xi, \beta) = 1 - \left(1 + \xi \frac{x-u}{\beta}\right)^{-1/\xi}, \quad (2.2.5)$$

burada: ξ paylanmanın forma parametridir, "quyruğun ağırlığını" göstərir, β – miqyas parametridir.

GPD parametrlərini qiymətləndirmək üçün bir neçə metod istifadə olunur: maksimum həqiqətəoxşarlıq metodu, momentlər metodu və ehtimal çəkili momentlər metodu (ing. probability-weighted moments, PWM). Topluda verilənlərin azlığını nəzərə alaraq, GPD parametrlərini korreksiya etmək üçün müxtəlif mənbələrdən alınan məlumatların birləşdirilməsinə imkan verən Bayes yanaşması tətbiq edilə bilər [49, s.102].

GPD parametrlərinin eksperimental öyrənilməsi

A. Verilənlərin hazırlanması

Bu tədqiqatda ekstremal qiymətlərin öyrənilməsi üçün kompüter insidentlərinin emalı komandası AzScienceCERT [56, s.15] komandası tərəfindən toplanmış verilənlər istifadə edilmişdir. AzScienceCERT 2007-ci ildə qurulmuşdu və 2010-cu ildən Avropa CSIRT-lərinin Trusted Introducer xidməti (trusted-introducer.org) tərəfindən dəstəklənən verilənlər bazasında qeydiyyatdan keçmişdir.

AzScienceCERT Azərbaycan Milli Elmlər Akademiyasının AzScienceNet elm kompüter şəbəkəsinin istifadəçilərinə xidmət edir. AzScienceNet coğrafi paylanmış şəbəkədir və 5 mindən çox istifadəçiyə İnT insidentlərinin emalı üzrə müxtəlif xidmətlər təqdim edir.

AzScienceCERT İnT insidentlərinin emalı proseslərini izləmək üçün xüsusi RTIR (Request Tracker for Incident Response) proqram təminatından istifadə edir [8]. Gün ərzində AzScienceCERT bir çox mənbədən (istifadəçilər, tətbiqi proqramlar, İnT sistemləri və digər CERT-lər) İnT insidentləri haqqında onlarla məlumat alır. Daxil olan bütün insidentlər RTIR verilənlər bazasında qeydiyyata alınır. İnsidentin emalı tsiklində emalla bağlı digər zəruri məlumatlar da RTIR bazasına yazılır.

AzScienceCERT xidmətinin fəaliyyəti zamanı İnT insidentlərinin toplandığı bazada AzScienceNet çərçivəsində 8 mindən çox insident barəsində məlumat toplanmışdı. Bu insidentləri başvermə tezliyinə və təsirinə görə iki sinfə bölmək olar.

İnsidentlərin birinci sinfi nisbətən böyük tezliyə və kiçik təsirə malik insidentlərdən ibarətdir. Onlar insidentlər bazasının böyük əksəriyyətini təşkil edirlər. Bu insidentlər fərdi istifadəçilərə təsir edir, təşkilatın xidmətlərinin bütün istifadəçilərə əlyetər olmasına hər hansı təsir etmir. Gündə təxminən 5-10 belə insident baş verir.

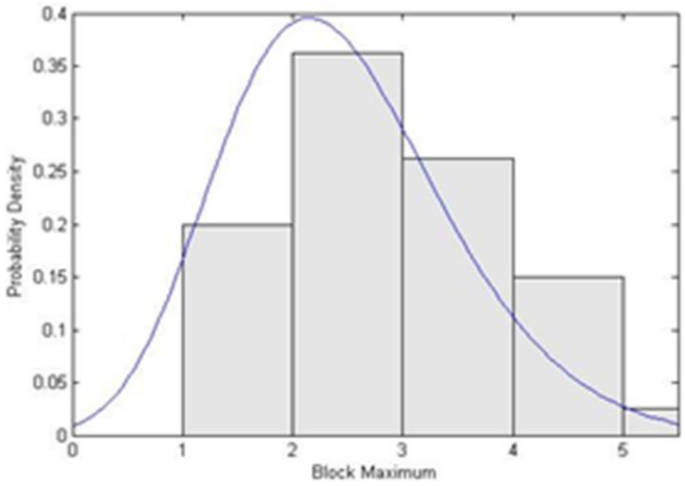
İnsidentlərin ikinci sinfi daha vacibdir, onlar kiçik tezliyə və böyük təsirə malik insidentlərdir. Bura AzScienceNet-in bəzi vacib xidmətlərini istifadəçilərin hamısına və ya istifadəçilərin altçoxluğuna göstərməsi imkanını itirdiyi insidentlər daxildir (məsələn, e-poçt serverinin dayanması). Ortalama hər iki ayda bir və ya iki belə insident olur. 2007-ci ildən 2013-cü ilə kimi AzScienceCERT tərəfindən təxminən 80 belə insident qeydə alınmışdı. Bu tədqiqat üçün 2007-2012-ci illərdə hər bir ayda baş vermiş belə insidentlərin sayı verilənlər bazasından götürülmüşdü.

B. GPD parametrlərinin qiymətləndirilməsi

GEV paylanmasının statistik xassələrini öyrənmək üçün EVIM (Extreme Value Analysis in MATLAB) proqram təminatı istifadə exdilmişdir [177, s.349].

Həqiqətəoxşarlığın maksimumu qiymətləndirməsi GEV parametrləri üçün aşağıdakı qiymətləri verir GEV $\xi = -0.145$; $\sigma = 0.940$; $\mu = 2.005$. GEV parametrləri ξ, σ və μ üçün 95% etibarlıq intervalları uyğun olaraq belədir: [-0.345, 0.779], [1.766; 0.055], [1.134, 2.244]. Bu göstərir ki, İnT insidentlərinin maksimal sayının paylanması Veybull paylanması ilə təsvir olunur.

GEV modeli üçün verilənlərin və ehtimal paylanması funksiyasının (ing. probability density function, PDF) miqyaslanmış histoqramı şəkil 2.2.3-də göstərilib. PDF-lərlə müqayisə edilə bilməsi üçün histoqram elə miqyaslanıb ki, zolaqların eni ilə hündürlüklərinin cəmi 1-ə bərabər olsun.



Şəkil 2.2.3. GEV modeli üçün verilənlərin histoqramı

Beləliklə, bu bölmədə e-dövlətin qarşılıqlı asılı informasiya infrastrukturunda İnT risklərinin qiymətləndirilməsi üçün yanaşma təklif edildi. Kəmiyyət yanaşması qurmaq üçün maliyyə institutlarında qəbul edilmiş əməliyyat risklərinin qiymətləndirilməsi metodları istifadə olunur. Gələcək tədqiqatlarda risk xarakteristikalarının asılılığını modelləşdirmək üçün kopula-funksiyaları aparatlarından istifadə edilməsi planlaşdırılır.

2.3. İnternetin milli infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri

Qeyd edək ki, son dövrlər elmi ədəbiyyatda istifadə edilən "dayanıqlıq" (ingiliscə "survavibility") anlayışının məzmunu genişdir, özündə təhlükəsizlik, qəzalara tolerantlıq, elastiklik, etibarlılıq və məhsuldarlıq konsepsiyalarını birləşdirir [80, s.106]. Dayanıqlıq dedikdə, hücumlar, insidentlər, qəzalar və digər arzu edilməyən hadisələr baş verdikdə sistemin öz missiyalarını verilmiş tələblərə uyğun surətdə fasiləsiz yerinə yetirmək qabiliyyəti başa düşülür. Dayanıqlıq etibarlılığın kateqoriyalarından biridir və etibarlılığın digər kateqoriyalarından fərqli olaraq (imtinalara dayanıqlıq, çeviklik, stabillik, adaptivlik), dayanıqlıqda müəyyənedici anlayış tam və ya qismən (məhdud) funksionallıqdır [43, s. 39].

İnternet infrastrukturunun dayanıqlığını onun yuxarıda göstərilən hər üç komponenti – kommunikasiya, ünvan və informasiya infrastrukturu üzrə aparmaq

olar, bu işdə əsasən İnternetin kommunikasiya infrastrukturunun dayanıqlığı məsələsinə baxılır. Digər iki komponentin vaciblik və aktuallığını qısaca qeyd edək.

Məlum olduğu kimi, İnternetdə ünvanlaşmanın əsası IP (İnternet Protokolu) ünvanları, AS (Autonomous System – Avtonom Sistem) nömrələri və domen adları sistemidir (Domain Name System, DNS). DNS veb tətbiqləri və e-poçt proqramları üçün xüsusilə əhəmiyyətli bir xidmətdir. Veb səhifəni açdıqda, e-poçt göndərdikdə və ya e-xidmətlərdən istifadə etdikdə İnternet resursunun yerləşdiyi yer DNS ilə müəyyən edilir. Hər hansı səbəbdən DNS sisteminin işi pozularsa, nəticədə e-xidmətlərin işinin pozulması da qaçılmaz olar. DNS iyerarxiyaya əsaslanır, bu iyerarxiyanın yuxarı səviyyəsində kök serverləri yerləşir. Ümumilikdə, A-dan M-ə işarələnmiş 13 kök serveri vardır. DNS sisteminin işinin pozulması səhv konfiqurasiyaya və ya hücumlara görə baş verə bilər. Hər bir AS-ə unikal AS nömrəsi verilir, onlar BGP marşrutlamasında (ing. Border Gateway Protocol – sərhəd şlüz protokolu) istifadə edilir. BGP-nin əsas nöqsanı onun təhlükəsizliyi təmin etmək imkanının olmamasıdır və bir sıra irimiqyaslı İnternet kəsintiləri İnternetin marşrutlama infrastrukturunun çox zəif olduğunu göstərir [104, s.100].

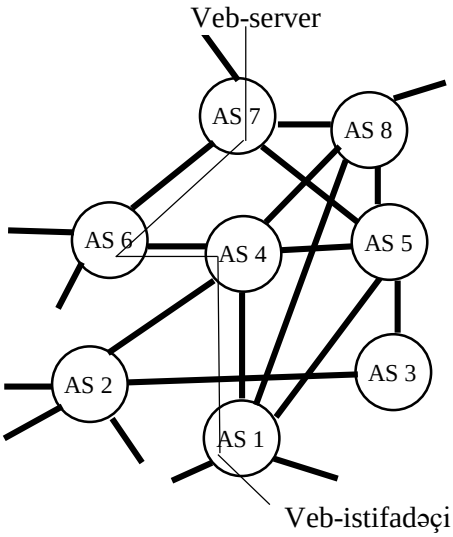
İnternetdəki bütün məlumatlar veb serverlərdə saxlanılır. Adətən, veb təhlükəsizliyi veb saytların təhlükəsizliyi ilə eyniləşdirirlər. Lakin veb təhlükəsizlik veb ekosisteminin bütün komponentlərinin (istifadəçinin kompüteri və veb brauzeri, kommmunikasiya kanalları, veb-server, veb-tətbiq, verilənlər bazası, protokollar və s.) təhlükəsizliyindən formalaşır. Bu komponentlərin hər hansı birindəki boşluqlar müxtəlif e-xidmətlərin fəaliyyətinin pozulmasına səbəb ola bilər. Buna görə veb təhlükəsizlik geniş tədqiqat sahəsidir [86, s.66].

Bu bölmədə elmi ədəbiyyatın analizi əsasında İnternetin milli infrastrukturunun dayanıqlığı ilə bağlı problemlər və onların həllinə mövcud yanaşmalar analiz edilir, İnternet infrastrukturunun dayanıqlığına yönəlmiş təhdidlər təhlil edilir, İnternetin kommunikasiya infrastrukturunun dayanıqlığının qiymətləndirilməsi üçün modellərin işlənməsi məsələsinə baxılır [25, s.39, 51, s.36].

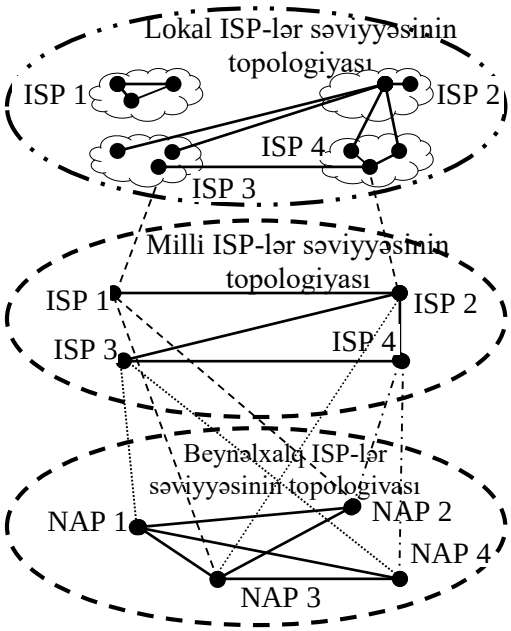
İnternetin milli infrastrukturunun çoxsəviyyəli modeli

İnternetin milli infrastrukturunun dayanıqlığının qiymətləndirilməsi modellərini işləmək üçün bu infrastrukturun topologiyasının çoxsəviyyəli modeli təklif edilir. Bu model İnternetin mövcud iyerarxik infrastrukturunu əks etdirməli və ayrı-ayrı altsistemlərin vacibliyini və təsirini nəzərə çarpdırmalıdır.

Topologiya baxımından İnternet infrastrukturunu bir neçə detallaşdırma səviyyəsində analiz etmək olar: fiziki səviyyədə, IP-marşrutizatorlar səviyyəsində, iştirak nöqtələri səviyyəsində (Point of Presense, PoP) və AS-lər səviyyəsində. Fiziki səviyyə kabellər, multipleksorlar, kross-kommutatorlar və 2-ci səviyyə sviçləri kimi şəbəkə elementlərindən ibarətdir. Marşrutlaşdırma səviyyəsi IP-səviyyədə işləyən qurğulardan ibarətdir. PoP coğrafi nöqtədə marşrutizatorlar çoxluğundan ibarətdir, PoP səviyyəsinin topologiyasına isə marşrutizatorların aqreqativ təsviri kimi baxmaq olar. AS vahid İnternet marşrutlaması siyasəti ilə bir (və ya bir neçə) operator tərəfindən idarə edilən IP-şəbəkələrin və marşrutizatorların şəbəkəsidir. AS səviyyəsində müxtəlif provayderlərin şəbəkələri bir-biri ilə trafikin qarşılıqlı mübadiləsi nöqtələrində (Internet eXchange Point, IXPs) və özəl pirinq nöqtələrində birləşirlər. Tədqiqatların əksəriyyətində əsas diqqət AS səviyyəsi topologiyasına verilir (şəkil 2.3.1).



Şəkil 2.3.1. İnternet AS topologiyasının fraqmenti



Şəkil 2.3.2. İnternetin çoxsəviyyəli topologiyası

Bu tədqiqatda biz İnternetin kommunikasiya infrastrukturunu bir-biri ilə magistral xətlər, şlüzlər və marşrutizatorlarla birləşən bir neçə IP-şəbəkədən ibarət avtonom şəbəkə kimi qəbul edirik. İnternet xidmətlərinin göstərilməsi ilə üç sinif provayderlər məşğul olurlar: beynəlxalq (Tier-1), milli və ya regional (Tier-2) və lokal (Tier-3). İlk iki sinfin qarşılıqlı əlaqəsi şəbəkə giriş nöqtələri (Network Access Point, NAP) və ya IXP nöqtələri ilə həyata keçirilir. İnternet trafikinin böyük hissəsi dayaq şəbəkəsi (ing. Internet backbone) ilə ötürülür ki, bu verilənlərin tranzitlərinin sayını azaldır.

Adi istifadəçi İnternetə girdikdə lokal İnternet xidmətləri provayderinin (Internet Service Provider, ISP) xidmətlərindən istifadə edir. İstifadəçilər ISP şəbəkəsinə PoP nöqtələrində qoşulurlar – bu nöqtələrdə müştərilərin İnternetə qoşulması üçün aparat təminatı yerləşdirilir. Lokal ISP-lər çox sayda istifadəçiyə xidmət etdiyindən onlar regional (milli) ISP-lərə yüksəksürətli xətlərlə qoşulmalıdır. Lokal ISP belə xətləri daha böyük kommunikasiya şirkətindən icarəyə götürə və ya öz xətlərini qura bilər. Regional provayder milli ISP provayderinə qoşulur. Regional (milli) ISP-lər ən azı iki başqa NAP ilə yüksəksürətli kanalla birləşməlidir. Milli provayderlərin şəbəkəsi beynəlxalq (transmilli) provayderlərin şəbəkəsinə qoşulur. Beləliklə, İnternet şəbəkəsi infrastrukturunun komponentləri ümumi iyerarxiyada birləşirlər. Kiçik və böyük şəbəkələrin birləşməsinin əsasında müqavilə razılaşmaları zənciri dayanır.

Bu işdə İnternetin milli infrastrukturunun təklif edilən çoxsəviyyəli topologiyası şəkil 2.3.2-də göstərilir. Topologiya üç səviyyədən ibarətdir: lokal provayderlər səviyyəsi, milli provayderlər səviyyəsi və beynəlxalq provayderlər səviyyəsi. Yeni «milli Tier-1 AS» tipi daxil etmək təklif olunur, bunu onların xarici AS-lər ilə müstəsna qarşılıqlı əlaqələrinin olması ilə əsaslandırmaq olar. Digər ölkələrin şəbəkəsi ilə əlaqəli olan istənilən AS-i milli Tier-1 AS qrupuna aid edirlər.

Əlaqədar işlərin icmalı

Son onillikdə elmi ədəbiyyatda kommunikasiya şəbəkələrinin dayanıqlığının kəmiyyətcə ölçülməsi və uyğun metrikaların işlənməsi məsələlərinə baxılır [273, s.705]. [161, s.1215]-də şəbəkələrdə böyük qəzaların təsirini analiz etmək üçün

müxtəlif riyazi modellər təklif edilmişdir. [222, s.367]-də telefon şəbəkəsini sıradan çıxaran irimiqyaslı statik qəzalar və bərpaetmələr baş verdikdə Markov modeli tətbiq edilməklə şəbəkənin dayanıqlığı məsələsinə baxılmışdır. [173, s.25]-də müəlliflər qəzanın yayılmasının geniş analizini və modelləşdirilməsini həyata keçirirlər, lakin onların işi modeli qəzanın yayılması ilə məhdudlaşır, şəbəkə hücumlarının yayılması zamanı şəbəkənin dayanıqlığı məsələsinə baxılmır. Şəbəkədə hücumların yayılması modeli [306, s.96]-da verilir. Adətən, yayılma Markov nəzəriyyəsi vasitəsilə modelləşdirilir.

[156, s.51]-da ABŞ kommersiya İnternet şəbəkəsinin dayanıqlığını qiymətləndirmək üçün coğrafi informasiya da nəzərə alınmaqla kommersiya İnternetinin şəbəkə topologiyası istifadə edilir. ABŞ kommersiya İnternetinin magistral sistemində qovşaq və xətlərin sıradan çıxmasının potensial təsiri imitasiya modelləşdirməsi vasitəsilə qiymətləndirilir.

Renesys şirkətinin mütəxəssisləri ölkələrin İnternetdə ayrılması risklərini qiymətləndirmişlər [118]. Qiymətləndirmə hər bir ölkə üçün xarici rabitə operatorlarına birbaşa çıxışı olan milli provayderlərin marşrutlama cədvəllərinin (ing. routing table) məlumatları əsasında aparılıb. Renesys ekspertləri ölkələri malik olduqları Tier-1 və Tier-2 provayderlərinin sayına görə bir neçə risk qrupuna ayırırlar: Məsələn, əgər ölkənin beynəlxalq çıxışda 1 və ya 2 şirkəti varsa, onda ölkənin İnternetdən ayrılması riski olduqca yüksəkdir (Azərbaycan bu qrupa aid edilir). Yaxud ölkədə 40-dan çox sərhəd operatoru varsa, onda ölkə rabitə kanallarının pozulmasına olduqca dayanıqlı hesab olunur. Bu ölkələr kateqoriyasına Kanada, ABŞ, Niderland, Rusiya və s. daxildir.

Lakin tədqiqat müəllifləri, bu risk qruplarını müəyyən edən milli provayderlərinin sayının hansı metodologiya əsasında seçildiyini, ölkələrin daha hansı xüsusiyyətlərinin nəzərə alındığını açıqlamırlar.

İnternetin imtinalara dayanıqlığının (ing. resilience) qiymətləndirilməsi üzrə tədqiqatları da qeyd etmək lazımdır [129, s.3183, 159, s.119]. Müəlliflər çox zaman "imtinalara dayanıqlıq" və "dayanıqlıq" anlayışlarını bərabərhüquqlu qəbul edirlər. Gələcək İnternetin dayanıqlığını artırmaq məqsədilə topologiyanın generasiyası

metodlarının, analitik, imitasiya və eksperimental emulyasiya yanaşmalarının kombinasiyasından istifadə etməklə şəbəkənin dayanıqlığının qiymətləndirilməsi metodologiyası [273, s.705]-də təsvir olunur.

[129, s.3183]-da AS səviyyəsində hücumlara və qəzalara qarşı İnternetin imtinalara dayanıqlığı tədqiq olunur. İnternetdən alınmış verilənlərdən istifadə etməklə müəlliflər göstərirlər ki, məqsədyönlü hücumlara qarşı İnternetin dayanıqlığı xüsusi topologiyalar üçün alınmış əvvəlki qiymətlərdən xeyli kiçikdir, təsadüfi qəzalar zamanı da onun əldə olunması xeyli aşağıdır.

Dayanıqlıq metrikaları

İnternetin milli infrastrukturunun dayanıqlığını qiymətləndirmək üçün uyğun kriteriyalar seçilməlidir. Dayanıqlığın kəmiyyət qiymətləndirilməsi üçün istifadə edilən metrikalar tətbiqlərdən asılı olaraq dəyişir və bir sıra faktorlardan asılıdır, məsələn, sistemin funksional hesab edilməsi üçün məhsuldarlığın zəruri olan minimal səviyyəsi, yaxud sistemin işləməməsinin yolverilən maksimum müddəti. 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 [84, s. 9 ANSI].

Dayanıqlıq metrikaları imtina baş verdikdən sonra hesablanmış keçid metrikalarıdır. Bölmənin bundan sonrakı qalan hissəsində *t* zamanı imtina baş verdiyi andan keçən müddəti bildirir və saatlarla ölçülür.

Dayanıqlıq göstəriciləri maraq ölçüsü də adlanan *M* məhsuldarlıq metrikasına nisbətən hesablanır [84, s. 52]. İnternet infrastrukturu sahəsində məhsuldarlıq metrikası kimi bir saatda xidmət edilən istifadəçilərin sayı götürülür. İmtinadan bilavasitə öncə *M*-in qiymətinin μ-ə bərabər olduğunu fərz edərək, dayanıqlığın davranışı *M*-in qiymətinin μ-yə qədər bərpa olunması üçün tələb edilən relaksasiya zamanı kimi atributlarla kəmiyyətcə müəyyən edilir. Bu işdə imtinadan sonra bir saatda xidmət edilməyən istifadəçilərin orta sayına fokuslanmaqla relaksasiya müddəti ilə əlaqəli metrikalar hesablanacaq.

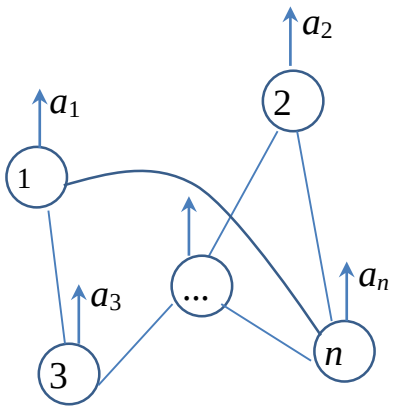
Bu bölmədə dayanıqlıqla əlaqəli metrikaların iki kateqoriyasına baxılır. Ani metrikalar – sistemin vəziyyətini *t* zaman anında göstərən keçid metrikalarıdır. Adi metrikaya misal verilmiş ISP *i*-nin *t* zaman anına bərpa olunması ehtimalı ola bilər.

Təklif edilən modellərdə kumulyativ metrikalar sistem vəziyyətlərinə mükafat faizləri mənimsətmək yolu ilə əldə edilir. Mükafat bu vəziyyətə təyin edilmiş mükafat faizinə uyğun olaraq zaman vahidlərinə görə hesablanır. Kumulyativ metrikaya misal verilmiş ISP-nin orta boşdayanma müddəti ola bilər. Bu halda kumulyativ mükafat hər bir vəziyyətdə vahid zamana görə mükafat təyin etmək yolu ilə alınmış zaman olacaq.

İnternetin milli infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri

A. Milli ISP provayderləri səviyyəsində dayanıqlığın qiymətləndirilməsi modeli

Fərz edək ki, İnternetin milli infrastrukturunda tranzit beynəlxalq trafikə xidmət edən provayderlərin sayı *n*-dir. Internet infrastrukturunun topologiyasını və qarşılıqlı asılılıqlarını təsvir etmək üçün qraflar nəzəriyyəsi istifadə edilir. Şəkil 2.3.3-də hipotetik İnternetin milli infrastrukturunun Tier-1 və Tier-2 seqmentinin şəbəkə topologiyası göstərilib. Qrafın təpələri provayderləri işarə edir, təpələrdən çıxan oxlar qlobal şəbəkəyə çıxışı göstərir. Hər bir belə çıxışa çəki verilmişdir (a_1, ..., a_n), bu çəkilər ölkədəki bütün İnternet istifadəçilərinin uyğun provayderin payına düşən nisbi sayını ifadə edir. Məsələn, $a_3 = 0.15$ onu göstərir ki, bütün İnternet istifadəçilərinin 15 %-i bu provayder vasitəsilə qlobal şəbəkəyə çıxır. $\sum_{i=1}^{n} a_i = 1$ olduğu fərz olunur.



Şəkil 2.3.3. Milli ISP provayderlərin hipotetik şəbəkəsi

Bəzi provayderlər arasında kommunikasiya əlaqələri mövcud ola bilər və onlar şəkil 2.3.3-də qrafın tilləri ilə göstərilib. Fərz edək ki, İnternetin milli kommunikasiya infrastrukturunun qraf modeli $D_{n\times n}$ insidentlik matrisi ilə verilib, əgər i və j provayderləri arasında kommuniukasiya əlaqəsi varsa, onda $d_{ij} = 1$, əks halda $d_{ij} = 0$. Qeyd edək ki, $d_{ii} = 0$ qəbul edilir.

Fərz edək ki, milli provayderlərə düşmən tərəfdən onların işini pozmaq üçün kiberhücumlar (məsələn, DDoS) həyata keçirilir, hücumların baş vermə zamanları təsadüfi hesab olunur. Qeyd edək ki, kiberhücumlar infrastrukturun bütün elementlərinə və ya onların müəyyən qrupuna eyni zamanda, koordinasiya edilmiş şəkildə həyata keçirilə bilər. Fərz edək ki, kiberhücum genişmiqyaslıdır və bütün kibermüdafiə tədbirlərinə baxmayaraq, kiberhücum uğurlu olur və provayder xidmətlərini müvəqqəti dayandırır. Uğurlu kiberhücuma məruz qalmış provayder təsadüfi müddət ərzində öz fəaliyyətini bərpa edə bilər (və ya ehtiyat sistemlə əvəzlənə bilər).

Hər bir provayderin t zaman anında vəziyyəti {0, 1} çoxluğundan qiymətlər alır. Tutaq ki, $x_i(t)$ təsadüfi kəmiyyəti t kəsilməz zaman anında i-ci provayderin vəziyyətini işarə edir. Əgər t zaman anında i-ci provayderdə uğurlu kiberhücum hadisəsi baş veribsə $x_i(t) = 0$, $(1 \le i \le n)$, əks halda $x_i(t) = 1$ qəbul olunur (yəni, provayderin normal vəziyyəti 1 ilə işarə edilir).

Onda istənilən t zaman anında İnternetin milli infrastrukturunun vəziyyətini hər bir provayderin vəziyyətləri toplusu ilə tam təsvir etmək olar:

$$X(t) = (x_1(t),\ x_2(t),\ \dots,\ x_n(t)), t \ge 0. \qquad (2.3.1)$$

Məsələn, əgər başlanğıc $t = 0$ zaman anında kiberhücum hadisəsi 1-ci provayderin fəaliyyətini dayandırıbsa, onda sistem (0, 1, ..., 1) vəziyyətində olacaq. $X(t)$ prosesini riyazi olaraq vəziyyətlər fəzası $\Omega = \{(x_1, \dots, x_n): x_1, \dots, x_n \in \{0,1\}\}$olan kəsilməz zamanlı Markov zənciri (Continuous-Time Markov Chain, CTMC) kimi modelləşdirmək olar. Ümumilikdə, Ω vəziyyətlər fəzası $N = 2n$ vəziyyətdən ibarərdir. $X(t)$ prosesi (0, 1, ..., 1) vəziyyətində başlayır və (1, 1, ..., 1) udulma vəziyyətində qurtarır, bu bütün provayderlərin işlədiyi vəziyyətdir.

İnternet infrastrukturunun dayanıqlığının kəmiyyət qiymətləndirməsini verilmiş *t* zaman anında fəaliyyət göstərən milli provayderlərin istifadəçilərin nisbi saylarının cəmi kimi qiymətləndirmək olar:

$$A = \sum_{i=1}^{n} a_i x_i(t). \quad (2.3.2)$$

Aşağıdakı ideal hala baxaq. Tutaq ki, bəzi milli səviyyə provayderləri arasında tranzit və ya pirinq xətləri mövcuddur və İnternetin milli infrastrukturunun Əlaqələndirmə Mərkəzi (ƏM) təşkil olunmuşdur. Fərz edək ki, irimiqyaslı kiberhücum və ya qəza zamanı fəaliyyətini dayandırmış Tier-2 provayderinin bütün istifadəçiləri ƏM tərəfindən provayderlər arasında mövcud olan kommunikasiya kanalları ilə digər provayderlərə dinamik olaraq yönləndirilir. Fərz edək ki, *i*-ci provayder sıradan çıxmışdır və ƏM tərəfindən onun istifadəçilərinin yönləndirildiyi provayderlərin çoxluğunu *Ji* ilə, *ai* payının müvafiq provayderlər arasında paylanması vektorunu isə $(b_{i,1}, b_{i,2}, \dots, b_{i,k})$ ilə işarə edək, burada $k = |J_i|$ və $\sum_{j \in J_i} b_{ij} \leq a_i$. Bu halda infrastrukturun dayanıqlığı aşağıdakı düsturla hesablana bilər:

$$A = \sum_{i=1}^{n} a_i x_i(t) + \sum_{i=1}^{n} \sum_{j \in J_i} (1 - x_i(t)) b_{ij} d_{ij} \ . \quad (2.3.3)$$

B. Tier-3 provayderləri üçün dayanıqlığın qiymətləndirilməsinin AI³ modeli

Aşağıda Tier-3 provayderləri səviyyəsində dayanıqlıq üçün metrika təklif edilir (onu milli ISP-lər üçün də istifadə etmək olar). Bu metrikanın işlənməsində intellektual elektrik təchizatı şəbəkələri (ing. Smart grid) üçün [92, s.241]-də verilmiş yanaşma istifadə edilmişdir.

Tutaq ki, provayderlərin sayı *C* olmaqla İnternetin milli seqmentinin topologiyası verilib. *N* – İnternetin baxılan milli seqmentinin bütün istifadəçilərinin sayıdır. Aşağıdakı işarələri qəbul edək. N_{jk} – ISP *j*-da *k*-cı imtinanın təsir etdiyi istifadəçilərin sayı, K_j – əvvəlcədən müəyyən edilmiş böyük müşahidə periodu ərzində ISP *j*-da imtinaların sayı, $j = 1, \dots, C, k = 1, \dots, K_j$. φ_{jk}– ISP *j*-da baş vermiş *k*-cı imtinanın yaratdığı kəsintinin müddətidir və saatlarla ölçülür. φ_j – ISP *j*-da olan bütün imtinalar nəticəsində kəsintilərin orta müddətidir. ψ_j – əvvəlcədən müəyyən

edilmiş həmin müşahidə periodu ərzində ISP j-da olan imtinaların orta sayıdır. Adətən, müşahidə periodu bir ilə bərabər götürülür, buna görə φ_j və ψ_j – uyğun olaraq, kəsintilərin orta illik müddəti və imtinaların sayıdır.

İnternet kəsintilərinin ortalama indeksi (Average Internet Interruption Index, AI[3]) İnternet infrastrukturunun imtinadan sonra bərpaolunma qabiliyyətinin vacib göstəricisidir:

$$AI^3 = \sum_{j=1}^{C} \sum_{k=1}^{K_j} \varphi_{jk} \frac{N_{jk}}{N}. \quad (2.3.4)$$

AI[3] indeksi İnternet provayderlərində imtinaların istifadəçilərə orta təsirini ölçür, çünki o, imtinaların müddətlərinin cəmini istifadəçilərin ümumi sayı ilə müqayisdə hesablayır.

Dayanıqlıq metrikalarının hesablanması

Dayanıqlıq metrikalarının hesablanması üçün xatırladaq ki, dayanıqlığın kəmiyyət qiyməti imtinalardan sonra keçid xarakteristikalarında fokuslanır. Tutaq ki, $\pi_{0j}(t)$ və Υ_{0j} – uyğun olaraq 0 vəziyyəti ilə əlaqəli keçid ehtimalı və mükafat faizidir. Tutaq ki, $L_j(t)$ – ISP j-da imtinadan sonra t zamanı ərzində toplanmış mükafatı xarakterizə edən təsadüfi kəmiyyətdir (məsələn, t zamanına xidmət edilməyən istifadəçilərin kumulyativ sayı). t zamanı ərzində toplanmış orta mükafat

$$\bar{L}_j(t) = \int_{y=0}^{t} \Upsilon_{0j}\, \pi_{0j}(t) \quad (2.3.5)$$

olacaq. Tutaq ki, s_{0j} – 1 vəziyyəti əldə edilənə kimi (yəni sistem tam bərpa olunana kimi) 0 vəziyyətində qalma müddətidir. Tutaq ki, L_j – sistem tam bərpa olunana kimi toplanmış mükafatı xarakterizə edən təsadüfi kəmiyyətdir. Sistemin tam bərpasına qədər toplanmış orta mükafat

$$\bar{L}_j = \lim_{t\to\infty} \bar{L}_j(t) = \Upsilon_{0j} \bar{s}_{0j} \quad (2.3.6)$$

olacaq. Qeyd edək ki, (2.3.6) –imtinadan sonra $[0, t]$ intervalında (2.3.5) ilə müəyyən edilən xidmət edilməyən istifadəçilərin orta sayıdır.

Eksperimental misallar. *Misal 1.* Tutaq ki, ölkənin İnternet infrastrukturuna üç milli provayder daxildir. Bu provayderlərin istifadəçilərin orta sayları uyğun olaraq N_1, N_2

və N_3 olsun. Tutaq ki, $N = N_1 + N_2 + N_3$. Fərz edək ki, birinci provayderə qarşı DDoS hücum baş verir və onu istifadəçilərdən təcrid edir.

Zəncirin vəziyyətlər fəzası $S = \{S_1, \dots, S_\Phi\}$ ($\Phi = 2^3 - 1 = 8$) kimi müəyyən edilir və hər bir vəziyyət (X_1, X_2, X_3) üçlüyü ilə təsvir olunur, burada $X_i \in \{0,1\}$ i-ci provayderin vəziyyətini göstərir, $i = 1, 2, 3$. Mümkün vəziyyətlər çoxluğu belədir:

S_1 = (011), S_2 = (001), S_3 = (000), S_4 = (101),

S_5 = (100), S_6 = (110), S_7 = (010), S_0 = (111).

Tutaq ki, Υ_j – j vəziyyəti ilə əlaqəli mükafat əmsalıdır, $j = 1, \dots, 8$. Milli provayderlər səviyyəsində dayanıqlığın qiymətləndirilməsinin birinci modelində istifadəçilərin sayı mükafat hesab edilir. Hər bir provayderin istifadəçilərinin sayı $N_i, i = 1, 2, 3$ nəzərə alınsa, onda hər bir vəziyyət üçün mükafat faizini asanlıqla tapmaq olar. Məsələn, yuxarıda göstərilən vəziyyətlər üçün mükafat faizləri uyğun olaraq aşağıdakı kimi olar:

$$\Upsilon_1 = \frac{N_2 + N_3}{N}, \quad \Upsilon_2 = \frac{N_3}{N}, \quad \Upsilon_3 = 0,$$
$$\Upsilon_4 = \frac{N_1 + N_3}{N}, \quad \Upsilon_5 = \frac{N_1}{N},$$
$$\Upsilon_6 = \frac{N_1 + N_2}{N}, \quad \Upsilon_7 = \frac{N_2}{N}, \quad \Upsilon_8 = 1.$$

Misal 2. Fərz edək ki, bir il ərzində j-cu provayderə qarşı iki uğurlu DDoS hücumu baş verir və DDoS hücumdan sonra orta bərpa müddəti 3 saat təşkil edir. Onda $\lambda_j = \frac{2}{365}\frac{1}{sutka} = \frac{1}{4380}\frac{1}{saat}$, $\mu_j = \frac{1}{3}\frac{1}{saat}$. Həmçinin fərz edək ki, bu provayderin istifadəçilərinin bir dəqiqədə orta sayı n_j-yə bərabərdir. 0 və 1 vəziyyətlərinə keçidin limit ehtimalları uyğun olaraq belə olacaq: $\pi_{0j} = \frac{\lambda_j}{\lambda_j + \mu_j} = 0{,}000684$ və $\pi_{1j} = \frac{\mu_j}{\lambda_j + \mu_j} = 0{,}999316$. Bütün bərpa müddəti ərzində xidmətdən imtina edilən istifadəçilərin orta sayı $\bar{L}_j = \Upsilon_{0j}\bar{s}_{0j} = 60 \cdot n_j \cdot 3 = 180 n_j$ olacaq.

Gələcək tədqiqatlarda fəaliyyəti pozulmuş milli səviyyə provayderlərinin yükünün mövcud şəbəkə topolgiyasında digər provayderlər arasında dinamik paylanması modelinin işlənməsi, Markov yanaşması çərçivəsində dayanıqlığın bir

sıra ehtimal-zaman xarakteristikalarının müəyyən edilməsi, müxtəlif kiberhücum, kibermüdafiə və bərpaetmə senarilərinin diqqətə alınması nəzərdə tutulur.

II fəsil üzrə nəticələr

- E-dövlətin İnT-nə təhdidlərin milli maraqlara yaratdıqları təhlükə səviyyələrini xarakterizə edən ekspert qiymətləndirmələri əsasında konsensus ranqlaşdırılması üçün optimallaşdırma modeli işlənmişdir [15, 34-45];
- E-dövlətin qarşılıqlı asılı informasiya infrastrukturlarında İnT risklərinin kəmiyyət qiymətləndirməsi üçün aktuar yanaşma metodu təklif edilmişdir [49, s.102-112];
- İnternetin milli infrastrukturunun irimiqyaslı kiberhücumlara və təsadüfi imtinalara qarşı dayanıqlığını qiymətləndirmək üçün modellər təklif edilmişdir [51, s.36-45].

III FƏSİL. E-DÖVLƏTİN BİOMETRİK İDENTİFİKASİYA SİSTEMİNİN TƏKMİLLƏŞDİRİLMƏSİ ÜÇÜN METODLAR

Qeyd edildiyi kimi, biometrik eyniləşdirmə sistemi e-dövlətin informasiya təhlükəsizliyi sistemində autentifikasiya və avtorizasiya altsisteminin əsasını təşkil edir və e-xidmətlərin təhlükəsizliyinin təmin edilməsində olduqca vacib rol oynayır. Lakin ölkə miqyasında biometrik eyniləşdirmə sisteminin qurulmasında qarşıya bir sıra elmi-praktiki problemlər çıxır. Bu qəbildən olan əsas problemlər mövcud biometrik sistemlərin tanıma keyfiyyətinin [50, s.24, 58, s.9-14] və təhlükəsizliyinin praktikada istifadə baxımından arzulanan səviyyədə olmaması [34, s.16], hətta eyni biometrik xarakteristika ilə işləyən müxtəlif sistemlər arasında interoperabelliyin aşağı səviyyəsi [176, s.66] və biometrik sistemlərin digər informasiya təhlükəsizliyi sistemləri, o cümlədən kriptoqrafik sistemlərlə inteqrasiyasında meydana çıxan böyük çətinliklərdir. Bu problemlərin həlli istiqamətində bu fəsildə biometrik sistemlərdə biometrik nümunənin keyfiyyəti barədə informasiyanın biometrik sistemin qərarı ilə aqreqasiyası modeli [176, s.66], dəyişilmiş barmaq izlərinin fraktal xarakteristikalar əsasında aşkarlanması metodu [47, s.11] və biometrik kriptosistemlərin sintezi üçün müxtəlif metodlardan ibarət yanaşma [185, s.1888] təqdim olunur.

3.1. Biometrik sistemlərdə informasiyanın aqreqasiyası metodu

Məlumdur ki, biometrik sistemlərdə birinci və ikinci növ statistik səhvlər olur. Bu səhvlər iki kəmiyyətlə xarakterizə olunur: 1) FRR – səhv imtinaların nisbəti (faizlə) – qanuni istifadəçi sistemə buraxılmır; 2) FAR – səhv qəbulların nisbəti (faizlə) – icazəsi olmayan istifadəçi sistemə buraxılır. Buna görə istənilən biometrik sistemdə istifadəçiləri "Biometrik sistemin doğru qərar qəbul etməsinə nə dərəcədə inanmaq olar?" sualı maraqlandırır. Biometrik sistemin qərarına inamın qiymətini ədəbiyyatda çox zaman "qərarın etibarlılığı" adlandırırlar [210, s.1-4].

Bu bölmədə barmaq izini tanıma sistemlərinin tanıma göstəricilərini yüksəltmək üçün barmaq izi təsvirlərinin keyfiyyəti haqqında informasiyanın aqreqasiyası modeli təklif edilir [176, s.66]. Qeydiyyat zamanı alınmış və verifikasiya üçün təqdim olunmuş barmaq izi təsvirlərinin keyfiyyət qiymətlərini birləşdirmək üçün Dempster-

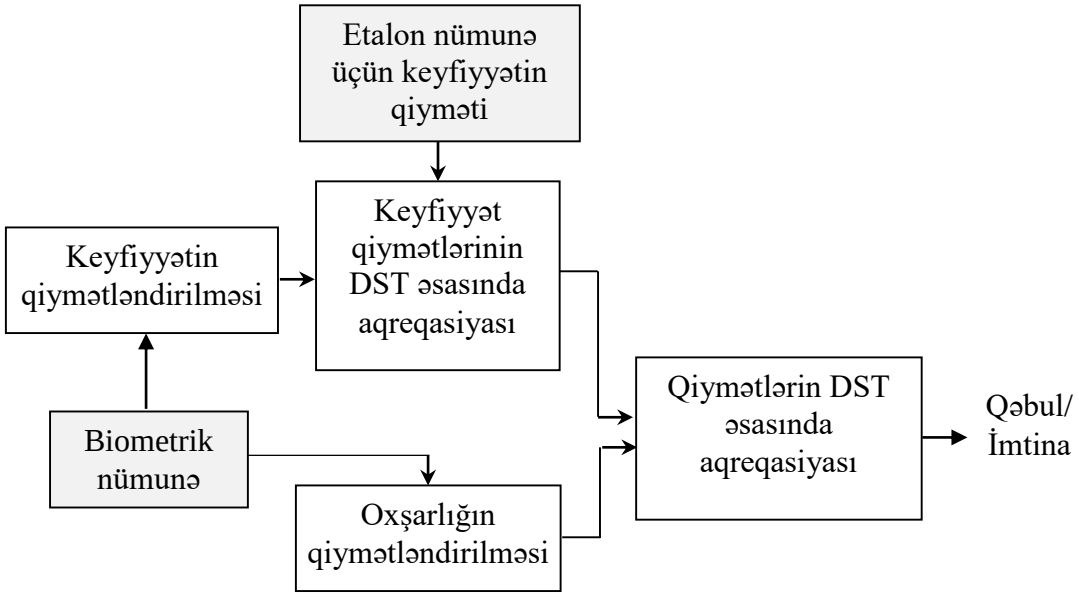
Şafer nəzəriyyəsi [100, s.37] əsasında yanaşma təklif edilir. Dempster-Şafer nəzəriyyəsi asılı olmayan sübutların aqreqasiyasının geniş öyrənilmiş və güclü metodlarından biridir, lakin biometrik sistemlərdə az istifadə edilir. Barmaq izi sensorlarının müxtəlif tiplərində barmaq izi təsvirlərinin keyfiyyət qiymətini asılı olmayan sübutlar hesab etmək olar, buna görə Dempster-Şafer nəzəriyyəsinin tətbiq edilə bilməsi şərti yerinə yetirilir.

ISO/IEC 19785-1:2006 və oxşar beynəlxalq standartların tələblərinə görə biometrik nümunənin keyfiyyət göstəriciləri biometrik şablona daxil edilir. Aşağı keyfiyyətli barmaq izi təsvirləri çox zaman nəticədə səhv və olmayan əlamətlər verir, bu isə FAR və FRR faizlərini yüksəldərək biometrik sistemin məhsuldarlığını ciddi şəkildə deqradasiya edir. NIST (National Institute of Standards and Technology) hesabatları [280, s. 3] göstərir ki, barmaq izi əsasında olan biometrik sistemlərin dəqiqliyinə digər faktorlarla yanaşı, əsasən barmaq izlərinin keyfiyyəti təsir edir. Buna görə də, biometrik sistem qərar qəbul edərkən barmaq izinin keyfiyyəti haqqında informasiyanı nəzərə almalıdır [176, s.66].

Analizlər göstərir ki, biometrik şablonların mövcud müqayisə metodları biometrik nümunələrin keyfiyyəti haqqında informasiyanı nəzərə almır. Onlar fərz edirlər ki, sadəcə, keyfiyyətə nəzarət bloku aşağı keyfiyyətli biometrik şablonları müqayisə blokuna buraxmır. Biometrik sistemlər, həmçinin təsvirin yaxşılaşdırılması metodlarından da istifadə edə – aşağı keyfiyyətli təsviri qəbul edilən səviyyəyə kimi yaxşılaşdıra bilərlər. Təbii ki, bu metodlar biometrik şablona saxta minusiyalar daxil edə və biometrik sistemin dəqiqliyinə mənfi təsir göstərə bilərlər [174, s.1-6]. Bundan başqa, biometrik sistemdə iki biometrik şablonun istifadə edilməsini nəzərə almaq və hər iki biometrik nümunənin keyfiyyətini qiymətləndirmək lazımdır.

Yuxarıda deyilənləri nəzərə alaraq, təklif edilən metodu şəkil 3.1.1-də göstərilən blok-sxem şəklində təsvir etmək olar. Fərz olunur ki, etalon şablonda qeydiyyata alınmış biometrik nümunənin keyfiyyət göstəriciləri vardır. Etalon şablonla verifikasiya üçün təqdim olunmuş biometrik giriş nümunəsinin keyfiyyət göstəriciləri verifikasiya zamanı hesablanır. Daha sonra keyfiyyət qiymətləri Dempster-Şafer nəzəriyyəsi əsasında aqreqasiya edilərək biometrik sistemin etibarlılığı müəyyən

edilir. Sonrakı addımda müqayisə qiyməti və keyfiyyət qiyməti birləşdirilərək biometrik sistemin verifikasiya haqqında son qərarı müəyyən edilir. Barmaq izi təsvirlərinin keyfiyyətinin qiymətləndirilməsi və təsvirin keyfiyyəti haqqında informasiyanın aqreqasiyası məsələlərinə növbəti paraqraflarda baxılır.



Şəkil 3.1.1. Təklif edilmiş yanaşmanın blok-sxemi

Barmaq izi təsvirlərinin keyfiyyətinin qiymətləndirilməsi. Barmaq izi təsvirlərini barmağın dərisinin (məsələn, quru, nəmli), qəbuledici sistemin erqonomikasının (məsələn, istifadəsinin, yerləşdirilməsi və düzləndirilməsinin asanlığı) müxtəlif vəziyyətlərində, sensor avadanlığının məxsusi məhdudiyyətlərində (məsələn, optik sensorlardan kölgə, tutum sensorlarından elektrik küyü) alırlar. Bu şərtlər öz növbəsində barmaq izi təsvirlərinin keyfiyyətinə təsir edir.

Barmaq izi təsvirlərinin keyfiyyətini adətən qabarıqlıqlar və çöküklər strukturunun aydınlığının, həmçinin əlamətlərin (minusiyaların və sinqulyar nöqtələrin) "çıxarıla bilərliyinin" ölçüsü kimi müəyyən edirlər [81, s.734].

Barmaq izi təsvirlərinin keyfiyyətini qiymətləndirmək üçün bir neçə yanaşma təklif edilib [81, s.734, 48, s.44]. Qabarıqlıq və çökəkliyi aydın olan blokları yaxşı keyfiyyətli blok kimi fərqləndirmək üçün bəzi işlərdə Qabor filtrləri tətbiq edilir [176, s.66]. [108, s.160]-də barmaq izi təsvirlərinin keyfiyyəti üçün iki indeks təklif edilir. Birinci indeks tezlik oblastında enerjinin paylanması entropiyasının ölçülməsinə əsaslanır. İkinci indeks bir-birini örtməyən bloklarda qradiyentlərin lokal

əlaqəliliyini qiymətləndirir. Qeyd edək ki, barmaq izi təsvirlərinin keyfiyyətinin qiymətləndirilməsi metodlarının geniş icmalı [81, s.734]-də verilir.

Dempster-Şafer nəzəriyyəsi

Dempster-Şafer nəzəriyyəsində (Dempster-Shafer Theory, DST) hər hansı predmet oblastı tam və bir-birini qarşılıqlı istisna edən hipotezlərin Θ çoxluğu ilə təsvir edilir. Θ üstlü çoxluğunu $-$ Θ çoxluğununun $\emptyset$ boş çoxluğu daxil olmaqla bütün altçoxluqları çoxluğunu 2^{Θ} ilə işarə edək.

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

$$m(\emptyset) = 1, \tag{3.1.1}$$

$$\sum_{A \in 2^{\Theta}} m(A) = 1. \tag{3.1.2}$$

$m(A)$ 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:

$$bel(A) = \sum_{B|B \subseteq A} m(B) \tag{3.1.3}$$

$pl(A)$ həqiqətəoxşarlıq funksiyası sübutların A-ya daxil olan hipotezlərlə uyuşma dərəcəsini qiymətləndirir və aşağıdakı düsturla müəyyən edilir:

$$pl(A) = \sum_{B|B \cap A = \emptyset} m(B) \tag{3.1.4}$$

Bu iki funksiya öz aralarında $pl(A) = 1 - bel(\bar{A})$ şəklində əlaqəlidir.

A fokal elementinə inamın həqiqi qiyməti aşağıdan A-nın inam qiyməti ilə, yuxarıdan isə A-nın həqiqətəoxşarlıq qiyməti ilə məhdud olur: $[bel(A), pl(A)]$.

İki çoxluqdan birləşmə aşağıdakı kimi hesablanır:

$$m_1 \oplus m_2(A) = \frac{1}{K} \sum_{B \cap C = A} m_1(B) m_2(C), \tag{3.1.5}$$

$$K = \sum_{B \cap C = \emptyset} m_1(B) m_2(C). \tag{3.1.6}$$

Təsvirin keyfiyyəti barədə informasiyanın aqreqasiyası modeli

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, $\lambda^i, i \in \{reliable, non - reliable\}$ − 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 x obrazı d metrikasına görə x^i-yə yaxındırsa, onda biz hər iki vektorun eyni sinfə mənsub olması inamına meylliyik. Əksinə, əgər $d(x, x^i)$ məsafəsi çox böyükdürsə, onda x sübutu bizi x-in sinfi mənsubiyyəti barədə tam biliksizlik vəziyyətində qoyur. Buna görə, hesab etmək olar ki, sübutun bu elementi Λ üzərində aşağıdakı münasibətlərlə müəyyən edilən $m(\cdot \mid x^i)$ kütləsi yaradır:

$$m(\{\lambda_q\} | x^i) = \alpha \phi_q(d^i), \tag{3.1.7}$$

$$m(\Lambda | x^i) = 1 - \alpha \phi_q(d^i), \tag{3.1.8}$$

$$m(A | x^i) = 0, \forall A \in 2^{\Lambda} \backslash \{\Lambda, \{\lambda_q\}\}, \tag{3.1.9}$$

burada: $d^i = d(x, x^i)$ − məsafə, λ_q − x^i $(\lambda^i = \lambda_q)$ obrazının sinfi, $\alpha, 0 < \alpha < 1$ − parametr, ϕ_q − azalan funksiyadır, $\phi_q(0) = 1$ və $\lim_{d \to \infty} \phi_q(d) = 0$ şərtlərini ödəyir. Əgər d kimi Evklid məsafəsi istifadə edilərsə, onda ϕ_q funksiyasını

$$\phi_q(d) = exp\left(-\gamma_q d^2\right) \tag{3.1.10}$$

şəklində seçmək olar, burada $\gamma_q - \lambda_q$ sinfi ilə əlaqəli müsbət parametrdir.

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:

$$m = m(\cdot\,|x^1) \oplus \ldots \oplus m(\cdot\,|x^N). \tag{3.1.11}$$

x-dən uzaqda yerləşən təlim obrazları az informasiya verir, buna görə (3.1.11) düsturunda x-in ən yaxın k qonşusuna baxmaq kifayətdir, bu halda m

$$m = m\left(\cdot\,|x^{i_1}\right) \oplus \ldots \oplus m\left(\cdot\,|x^{i_k}\right), \tag{3.1.12}$$

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

x-in k ən yaxın qonşusuna hər biri kütlənin köməyi ilə təsvir edilən k müstəqil informasiya mənbəyi kimi baxmaq olar. Qeyd edək ki, m-in hesablanmasına k sadə kütlənin birləşdirilməsi daxildir və iki sinfin sayına nəzərən xətti zamanda yerinə yetirilə bilər.

Əgər (3.1.12) düsturunda (3.1.7) və (3.1.8) nəzərə alınsa, onda istənilən $q \in \{reliable, non\text{-}reliable\}$ üçün $m()$ düsturunu

$$m\left(\{\lambda_q\}\right) =$$

$$\frac{1}{K}\left(1 - \prod_{i \in I_{k,q}} \left(1 - \alpha \cdot exp\left(-\gamma d_i^2\right)\right)\right) \prod_{r \neq q} \prod_{i \in I_{k,q}} \left(1 - \alpha \cdot exp\left(-\gamma d_i^2\right)_r\right) \tag{3.1.13}$$

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 $m\left(\{\lambda_q\}\right)$ qiymətinə uyğun λ_q sinfinə aid edilir, burada $0 < m\left(\{\lambda_q\}\right) < 1$.

Eksperimentlərin nəticələri

Barmaq izi minusiyalarının müqayisəsi üçün NBIS (NIST Biometric Image Software) [176, s.66] proqram təminatı istifadə edilmişdir. Minusiyaların çıxarılması üçün MINDTCT paketi, barmaq izlərinin müqayisəsi üçün isə barmaq izləri arasında

oxşarlıq əmsalı hesablayan BOZORTH3 paketi istifadə edilmişdir. Barmaq izlərinin keyfiyyətini qiymətləndirmək üçün NBIS paketinə daxil olan NFIQ (NIST Fingerprin Image Quality) proqram təminatı istifadə edilmişdir [280, s.16]. NFIQ tapılmış minusiyalar əsasında barmaq izlərinin keyfiyyətinə aşağıdakı qiymətlərdən birini təyin edir: 5 (pis), 4 (orta), 3 (yaxşı), 2 (çox yaxşı), 1 (əla).

Eksperimentlərdə FVC2004 müsabiqəsi üçün toplanmış DB1, DB2 və DB3 bazalarından götürülmüş barmaq izləri istifadə edilmişdi [146]. Barmaq izləri üzrə bu verilənlər bazaları üç müxtəlif sensor istifadə edilməklə toplanmışdı: DB1 − CrossMatch firmasının "V300" optik sensoru, DB2 − Digital Persona firmasının "U.are.U" optik sensoru və DB3 − Atmel firmasının "FingerChip FCD4B14CB" süpürmə optik sensoru. Bu sensorları uyğun olaraq S1, S2 və S3 kimi işarə edək. Təsvirlərin ölçüləri və sensorların ayırdediciliyi cədvəl 3.1.1-də verilib.

Cədvəl 3.1.1.
Barmaq izləri üzrə verilənlər bazalarının xarakteristikaları

Verilənlər bazası	Sensorun növü	Təsvirin ölçüləri (piksellə)	Ayırdedicilik
DB1	Optik sensor	640x480	500 dpi
DB2	Optik sensor	328x364	500 dpi
DB3	Süpürmə termo-sensor	300x480	512 dpi

Verilənlər bazasında hər bir barmağın üç müxtəlif sensorda iki həftədən az olmayan intervalla üç seans ərzində toplanmış 12 izi vardır.

Eksperimentlərdə müxtəlif barmaq izlərinə sistemdə qeydiyyata alınmış müxtəlif istifadəçilərə məxsus biometrik şablonlar kimi baxılır. Hər bir sensor üçün aşağıdakı müqayisələr aparılmışdır.

1) həqiqi barmaq izləri ilə müqayisə − barmağın hər bir izi bu barmağın qalan izləri ilə müqayisə edilir (cəmi $100 \times 12 \times 11/2 = 6\,600$ müqayisə).

2) saxta barmaq izləri ilə müqayisə − hər bir barmağın ikinci təsviri qalan digər barmaqların üç izi ilə müqayisə edilir (cəmi $100 \times 99 \times 3 = 29\,700$ müqayisə).

Təklif edilmiş model qeydiyyat və verifikasiya üçün müxtəlif sensorlardan istifadə edilməklə test edilmişdir. Keyfiyyət göstəriciləri aqreqasiya edilmədən verifikasiya nəticələri cədvəl 3.1.2-də verilib.

Təklif edilmiş aqreqasiya modelinin istifadəsi zamanı verifikasiya nəticələri cədvəl 3.1.3-də verilib. Modelin qiymətləndirilməsi üçün EER (Equal Error Rate) parametri istifadə edilir. EER biometrik sistemdə FAR və FRR əmsallarının bərabər olduğu səhv səviyyəsini göstərir.

Cədvəl 3.1.2.
Keyfiyyət göstəriciləri aqreqasiya edilmədən EER əmsalları

	Verifikasiya		
Qeydiyyat	S1	S2	S3
S1	10.23	41.81	46.55
S2	38.90	7.48	43.11
S3	45.66	45.61	8.52

Cədvəl 3.1.3.
Keyfiyyət göstəricilərinin aqreqasiyası ilə EER əmsalları

	Verifikasiya		
Qeydiyyat	S1	S2	S3
S1	5.78	20.60	29.17
S2	23.39	3.54	22.47
S3	27.43	29.25	5.02

Beləliklə, eksperimentlərin nəticələri metodun effektivliyini təsdiq edir. Qeyd edək ki, metodu digər biometrik sensorlar (məsələn, sifətin şəkli və gözün qüzehli qişası) üçün də istifadə etmək olar.

3.2. Fraktal xarakteristikalar əsasında barmaq izlərinin həqiqiliyinin aşkarlanması metodu

Süni dəyişilmiş barmaq izlərinin istifadəsi cəhdləri "biometrik obfuskasiya" kimi tanınan hücumların geniş kateqoriyasına daxildir [307, s.451]. Belə hücumlarda fərdlər öz biometrik xarakteristikalarını süni dəyişmək yolu ilə öz şəxsiyyətini biometrik sistemdən maskalamağa cəhd edirlər. Biometrik obfuskasiya hallarına barmaq izi naxışlarının dəyişilməsi, teatr linzaları vasitəsilə gözün qüzehli qişasının dəyişilməsi, plastik əməliyyatlar yolu ilə sifətin dəyişilməsi aiddir. Məlumatlar var ki,

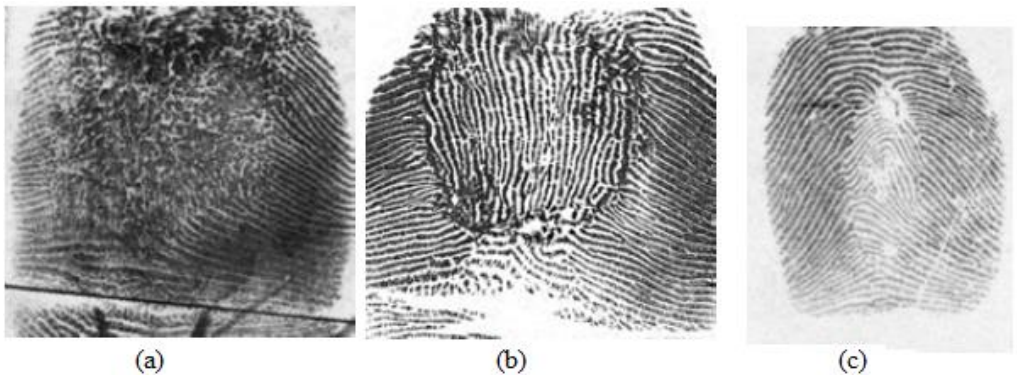
plastik əməliyyatlar sifəti tanıma sistemlərinin tanıma məhsuldarlığını əhəmiyyətli dərəcədə aşağı sala bilər, katarakt əməliyyatları isə gözün qüzehli qişasını tanıma sistemlərinin dəqiqliyini azalda bilər [47, s.11].

Barmaq izlərinin avtomatik tanınması sistemləri (Automated Fingerprint Identification System, AFIS) ən geniş yayılmış biometrik texnologiyadır, dünya biometrik sistemlər bazarının təxminən yarısını tutur [227, s. 1-3]. Bu sistemlər barmaq izlərinin unikal olması və yaşlı insanın bütün həyatı boyu dəyişmədiyi fərziyyəsinə əsaslanırlar. Süni dəyişilmiş barmaq izlərinin istifadəsi bu fərziyyələri pozur və AFIS-in təhlükəsizliyi və etibarlılığı üçün təhdid təşkil edir.

Yuxarıda qeyd edilənləri nəzərə alaraq, bu işin məqsədi fraktal xarakteristikalar əsasında süni dəyişilmiş barmaq izlərinin aşkarlanması metodunun işlənməsidir [47, s.11]. Barmaq izinə süni dəyişiklik edilməsi nəticəsində yeni struktur elementləri yaranır: çapıqlar, papilyar naxışların pozulduğu sahələr, barmaq izinin istiqamətlər meydanının kəskin dəyişməsi zonaları və s. Tədqiqat hipotezi bu müşahidəyə əsaslanır və fraktal analizin [65, s.859] mürəkkəb sistemlərin qlobal və lokal fəza strukturunu ətraflı təsvir etmək xassəsindən istifadə edir.

Süni dəyişilmiş barmaq izlərinin növləri

Süni dəyişilmiş barmaq izləri [307, s.451]-də qabarıqlar naxışında edilmiş süni dəyişikliklər əsasında üç sinfə bölünür: pozulmuş barmaq izləri, təhrif edilmiş barmaq izləri və imitasiya edilmiş barmaq izləri (şəkil 3.2.1).



Şəkil 3.2.1. Süni dəyişilmiş barmaq izi nümunələri [307]: (a) təhrif edilmiş (b) ovuc dərisindən transplantasiya (c) digər barmaq izindən "incə" transplantasiya

Barmaq izlərinə süni dəyişiklik edilməsinin ən populyar metodu sürtmə, yandırma, kəsmə, kimyəvi preparatların tətbiqi və hamar dərinin transplantasiyası vasitəsilə barmaq izi naxışlarının pozulmasıdır. Pozulmuş yerdə naxışların qabarıqlıq strukturu güclə görünür.

Təhrif edilmiş barmaq izlərini barmaqda dəri hissəsini götürərək onu fərqli vəziyyətdə köçürməklə və ya onu ovuc və ya ayaq altından dəri ilə əvəzləməklə alırlar. Təhrif edilmiş barmaq izlərində real barmaq izlərində rast gəlinməyən qeyri-adi qabarıqlıq naxışları olur.

Qabarıqlıq naxışı barmaq izində məharətlə edilmiş süni dəyişiklik prosedurundan sonra barmaq izi naxışına oxşarlığını saxlaya bilər. Məsələn, [307, s.451]-də məlumat verilir ki, sağ və sol əldə barmaqların dərisini dəyişməklə AFIS-i aldatmaq mümkün olmuşdur.

İmitasiya edilmiş barmaq izləri nəinki təsvirlərin keyfiyyətini qiymətləndirən proqram təminatının yoxlamasından keçirlər, onlar hətta barmaq izləri üzrə ekspertləri də çaşdıra bilərlər.

Şəkil 3.2.1 (c)-də süni dəyişlik edilmiş barmaq izinin istiqamətlər meydanı çox hamardır və mümkün süni dəyişikliyin yeganə sübutu nazik çapıqdır. Bu barmaq izi məharətli cərrahi prosedur nəticəsində alınmışdır və hətta cərrahi çapıq boyunca da naxışların şəkli təbiidir.

Süni dəyişilmiş barmaq izlərinin aşkarlanması metodlarının icmalı

Qeyd edildiyi kimi, süni dəyişilmiş barmaq izlərinin aşkarlanması üzrə cəmisi bir neçə iş mövcuddur. Süni dəyişilmiş barmaq izlərinin avtomatik aşkarlanması üzrə [307, s.451]-də təklif edilmiş metod iki əlamətdən istifadə edir. Birinci əlamət barmaq izlərinin istiqamətlər meydanının analizinə əsaslanır. Yaxşı keyfiyyətli barmaq izləri sinqulyar nöqtələrin ətrafı istisna olmaqla hamar istiqamətlər meydanına malikdir. Bu fakta əsaslanaraq, barmaq izlərinin istiqamətlər meydanının çox sayda modelləri işlənmişdir [95, s.905], onlar kəsilməz meydan üçün qlobal istiqamətlər meydanının və sinqulyar nöqtələrin ətrafında lokal istiqamətlər meydanının modellərini birləşdirir. Əgər istiqamətlər meydanının approksimasiyası

üçün yalnız qlobal model istifadə edilsə, onda müşahidə edilən və qlobal model üzrə hesablanmış istiqamətlər meydanları arasındakı fərq yalnız sinqulyar nöqtələrin ətrafında sıfırdan fərqli olacaq.

Süni dəyişilmiş barmaq izləri üçün modelin approksimasiya xətası həm də süni dəyişiklik edilmiş yerlərdə də müşahidə edilir, buna görə də barmaq izindən alınmış istiqamətlər meydanı ilə qlobal modellə approksimasiya edilmiş meydan arasındakı fərqi barmaq izlərinin həqiqi və ya süni dəyişilmiş izlər kimi klassifikasiya edilməsi üçün əlamətlər vektoru kimi istifadə etmək olar.

Süni dəyişilmiş barmaq izlərinin aşkarlanması üçün [256, s.45]-da istiqamətlər meydanının etibarlılığı əsasında metod təklif edilir. Barmaq izlərinin istiqamətlər meydanının etibarlılığı xəritəsi sinqulyar nöqtələrdə piklərə malikdir. Bu piklər süni dəyişilmiş barmaq izlərinin analizi üçün istifadə olunur, çünki süni dəyişiklik nəticəsində digər sinqulyar nöqtələr – kiçik amplitudlu piklər meydana çıxır.

[307]-də təklif edilmiş metodlar sinqulyar nöqtələrin tapılmasına əsaslanır, lakin bu məsələnin özü kifayət qədər mürəkkəbdir, qövs tipli barmaq izlərində isə sinqulyar nöqtələr olmur. Bundan başqa, skanerlərdən alınmış barmaq izlərində sensor səthinin kiçik olması səbəbindən delta nöqtələri olmaya bilər. [256, s.45]-da təklif edilmiş metod da sinqulyar nöqtələrə əsaslanır.

Fraktallar və fraktal ölçünün qiymətləndirilməsi metodları

Fraktallar nəzəriyyəsi və onun elmdə, texnikada və texnologiyalarda müxtəlif obyektlərə tətbiqləri son illər geniş yayılmışdır [228, s.70]. Fraktal anlayışını (latınca “fractus” – qırılmış, parçalanmış) 1960-70-ci illərdə B.Mandelbrot daxil etmişdir, fraktal həndəsəsinin yaranmasını onun “The Fractal Geometry of Nature” [229] kitabının çıxması ilə əlaqələndirirlər. Mandelbrot bu sahədə əvvəllər işləmiş digər alimlərin (Puankare, Fatu, Jülia, Kantor, Hausdorf) elmi nəticələrini vahid sistemdə birləşdirməyə nail olmuşdu.

Mandelbrot öz işlərində fraktalları aşağıdakı xassələrə malik obyektlər kimi müəyyən edərək onlara müxtəlif təriflər verirdi [228, s.70]:

- çox fraqmentar və ya qeyri-requlyar formaya malikdirlər;

– özünəoxşarlığa və özünə-affinliyə malikdirlər;
– miqyas invariantlığına malikdirlər.

Miqyas invariantlığı miqyas dəyişmələri zamanı fraktalların əsas həndəsi xassələrinin dəyişməzliyini nəzərdə tutur. Özünəoxşarlıq miqyas invariantlığının ən sadə nümunəsidir. Özünəoxşarlıq fraktalın bir miqyasdakı strukturunun başqa bir miqyasdakı strukturuna oxşar olduğunu bildirir. Qeyd edək ki, bu xassə üstlü asılılıqlara gətirib çıxarır. Özünə-affinlik özünəoxşarlığın ümumiləşdirilməsidir və miqyas invariantlığının daha mürəkkəb formasıdır. Özünə-affin oxşar obyektin hissəsi affin çevirmədən sonra bütöv obyektə oxşardır.

Fraktalı xarakterizə edən əsas parametr fraktal ölçüdür, o, miqyasın dəyişməsi zamanı statistik xarakteristikaların saxlanmasını təsvir edir. Fraktal ölçü kimi F.Hausdorf tərəfindən hələ 1918-ci ildə metrik fəzalarda kompakt çoxluqlar üçün daxil edilmiş ölçü istifadə edilir:

$$D = \lim_{\delta \to 0} \frac{N(\delta)}{1/\delta}. \qquad (3.2.1)$$

burada: $N(\delta)$ – baxılan çoxluğu örtən δ radiuslu kürələrin minimal sayıdır. Evklid fəzalarında örtmə üçün kürələrlə yanaşı xarakterik xətti ölçüləri δ olan digər elementləri də istifadə etmək olar.

Hazırda fraktal ölçünün qiymətinin hesablanması üçün bir çox metod, o cümlədən blokların sayılması metodu (box-counting method, BC-metod), Hörst metodu (R/S method – normallaşdırılmış amplitud metodu), profillərin Furye-analizi, şaquli kəsiklər metodu və s. istifadə edilir.

BC-metod daha tez-tez istifadə edilir. Bu metod çoxluğu tilinin uzunluğu δ olan d-ölçülü bloklarla örtür, onların $N(\delta)$ sayını hesablayır, loqarifmik koordinatlarda $(log(N(\delta), log(\delta))$ qrafikini qurur və meyl bucağına görə fraktal ölçünün qiymətini müəyyən edir:

$$D = -\Delta \log(N(\delta))/\log(\delta). \qquad (3.2.2)$$

BC-metodunun müxtəlif variantları mövcuddur, onlar parametrləri (məsələn, blokların sürətli sayılması alqoritmində blokun tərəfinin uzunluğu $2^k, 1 \leq k \leq K$

kimi dəyişir, burada $N = 2^K, N-$ təsvirin ölçüsüdür) və təsvirin modelləri (məsələn, nöqtələr arasında interpolyasiya olmadan və s.) ilə fərqlənirlər.

Bir çox təbii tekstur səthlərini fraktal səthlər kim qəbul etmək olar. Fraktal ölçü teksturların seqmentasiyası, formaların klassifikasiyası və bir çox sahədə qrafiki analiz üçün faydalı əlamətdir. Tədqiqatlar göstərir ki, fraktal ölçü ilə insanların səthin "qeyri-müntəzəmliyini" qiymətləndirməsi çox yaxşı korrelyasiya edir [47, s.11].

Barmaq izlərinin analizi üçün fraktal ölçünün istifadəsi imkanı [258, s.591]-də araşdırılmışdır. Biometrik identifikasiya üçün fraktal ölçünün bir qiyməti deyil, fraktal ölçü əsasında əlamətlər vektoru istifadə edilir [47, s.11]. Multifraktalların mürəkkəb tekstur şəkillərinin, o cümlədən barmaq izi şəkillərinin təsviri üçün daha uyğun olması haqqında fikirlər irəli sürülür [223, s.634].

Multifraktallar fraktalların ümumiləşdirilməsidir, onlar adi fraktallardan həndəsi xassələrin miqyas səviyyəsindən asılılığın mövcudluğu ilə fərqlənirlər. Bu asılılıq determinik və ya stoxastik ola bilər və ona gətirib çıxarır ki, multifraktalın metrik xassələri bir fraktal ölçüsü ilə deyil, fraktal ölçülərin spektri (Multifractal spectrum, MFS) ilə xarakterizə edilir. Faktiki olaraq, multifraktal yanaşması o deməkdir ki, öyrənilən obyekti hər birində özünəoxşarlıq xassələri müşahidə edilən fraqmentlərə (çoxluqlara) bölmək olar [65, s.859].

Süni dəyişilmiş barmaq izlərinin aşkarlanması metodu

Bu bölmədə süni dəyişilmiş barmaq izlərinin fraktal xarakteristikalar əsasında aşkarlanması metodu təsvir olunur. Təklif edilən metodu aşağıdakı addımlar ardıcıllığı şəklində göstərmək olar:

1. Barmaq izinin verilmiş təsviri ilkin emal edilir və normallaşdırılır [227, s. 97].

2. Fraktal xarakteristika hesablanır və onun əsasında əlamətlər vektoru formalaşdırılır.

3. Əlamətlər vektoru SVM-klassifikatorun köməyi ilə klassifikasiya edilir.

Süni dəyişilmiş barmaq izlərinin fraktal xarakteristikalar əsasında aşkarlanması üçün aşağıdakı fraktal xarakteristikalar əsasında əlamətlər vektorları istifadə etmək təklif olunur:

- modifikasiya olunmuş Katz metodu ilə hesablanmış fraktal ölçü;

– lokal miqyaslama eksponenti;

– multifraktal spektr.

Fraktal ölçü əsasında əlamətlər vektorunun hesablanması. Barmaq izlərində qabarıqlar və çöküklər lokal növbələşdikdə müstəvi sinusoidal dalğaya oxşayır. Dalğayabənzər siqnalların fraktal ölçüsünün hesablanması üçün müxtəlif alqoritmlər təklif edilib (Katz, Higuchi, Sevcik və b.) [199, s.145, 47, s.11]. Bu işdə barmaq izi şəkilləri üçün Katz metodunun variantı istifadə edilir [199, s.145].

Tutaq ki, barmaq izinin $N \times N$ ölçülü təsviri binarlaşdırılıb (təsvirin ölçüsü 256×256, dəqiqlik 500 dpi) və N sətrə və N sütuna bölünüb. Hesab etmək olar ki, hər bir sətirdə binar qiymət 1 rast gəlir (binarlaşdırılmış təsvirdə qabarığın pikseli 1 qiyməti, çöküyün pikseli isə – 0 qiyməti ilə verilir).

Hər bir sətir üçün fraktal ölçü aşağıdakı düsturla hesablanır:

$$d_n = \frac{\log_{10}(N)}{\log_{10}(M_n)}, \tag{3.2.3}$$

burada: M_n – n-ci sətirdə 1 binar qiymətinin ümumi sayıdır.

Barmaq izlərinin bütün təsviri üçün əlamətlər vektorunu belə qurmaq olar:

$$\Phi = \bigcup_{n=1}^{N} (n', d_n), \tag{3.2.4}$$

$$n' = \left[\frac{d_n - 1}{(n+1) - n}\right] \cdot n = (d_n - 1)n, \tag{3.2.5}$$

burada: n' – üfüqi miqyaslama əmsalıdır, $0 < n' < N$.

Hölder lokal eksponentləri əsasında əlamətlər vektorlarının hesablanması. Bəzi tədqiqatlar tək fraktal ölçünün təsvirin bütün tekstur xassələrini əhatə etmədiyini göstərir [223, s.634]. Gözləmək olar ki, süni dəyişilmiş barmaq izlərinin strukturunun əhəmiyyətli dəyişməsi səbəbindən blokların sayılması metodu ilə hesablanmış fraktal ölçüsü blokun ölçüsündən asılı olaraq dəyişəcək. Əgər çoxluq məhdud miqyaslama intervalında müəyyən fraktal xassəyə malikdirsə, onda bu xassəni lokal miqyaslama eksponentinin köməyi ilə qiymətləndirirlər. Qeyd edək ki, lokal miqyaslama eksponentini çox vaxt Hölder lokal ekponenti adlandırırlar, o, təsvirin lokal requlyarlığını xarakterizə edir [65, s.859].

Hölder lokal eksponentlərini hesablamaq üçün müxtəlif metodlar mövcuddur, bu işdə BC-metod istifadə edilir. D təmiz fraktal ölçüsü halında örtülmə üçün tələb edilən blokların sayı $N(\delta)$, üstlü qanuna tabe olur $N(\delta) = \delta^{-D}$, real sistemlərdə isə bu münasibət yalnız məhdud intervalda saxlanır. Əgər lokal miqyaslama eksponenti

$$D(\delta) = -\frac{\ln N(\delta)}{\ln \delta}, \qquad (3.2.6)$$

loqarifmik meyl kimi müəyyən edilsə, onda fraktallıq intervalı bu meylin təxminən saabit qaldığı miqyaslar çoxluğu olacaq.

Multifraktal əsasında əlamətlər vektorunun hesablanması. Fraktal xassəni multifraktal spektrlə (sinqulyarlıqların spektri ilə) və ya Hölder lokal eksponentlərinin ehtimal paylanması ilə daha detallı təsvir etmək olar. Multifraktal spektrlərin hesablanması üçün çox zaman veyvlet çevirmə istifadə edilir. Məlumdur ki, baxılan $\psi_{j,k}(x)$ ailəsinin bütün veyvletləri özlərinin $\psi(x)$ bazis veyvletinə oxşardır və ondan sıxılma və sürüşmənin köməyi ilə alınır. Veyvlet-analiz tədqiq olunan siqnalın analiz edən veyvletlə skalyar hasilini hesablamaqla siqnalın davranışını müxtəlif miqyaslarda öyrənir, buna görə fraktal davranışın tədqiqi üçün çox uyğun gəlir. Veyvlet-əmsallar terminlərində bu miqyas dəyişdikdə onların yüksək momentlərinin üstlü qanunla davranışını nəzərdə tutur [47, s.11].

Bu işdə ikiölçülü diskret veyvlet çevirmələr istifadə edilir (Discrete Wavelet Transform, DWT) [44, s.465]. DWT verilmiş I təsvirini bir $D_J(I)$ aşağıtezlikli komponentə və bir neçə miqyas altında yüksəktezlikli komponentlərə dekompozisiya edir: $W_{k,j}(I), k = 1,2,3; j = 1,2,\dots,J$, burada J – miqyasların sayıdır (bu işdə $J = 3$ istifadə edilir). Beləliklə, miqyasın hər bir səviyyəsində üç yüksəktezlikli komponent ($k = 1,2,3$) vardır, onlar şəklin "qırılmalarını" üfuqi, şaquli və diaqonal istiqamətlərdə təsvir edirlər. Təklif edilən metodun reallaşdırılması zamanı Dobeşi veyvletləri 'DB2' istifadə edilmişdir.

Multifraktal spektrlərin hesablanması üçün veyvletlərin $\{D_J, W_{k,j}, L_j\}$ piramidasını istifadə etmək təklif edilir [297, s.3785]: $D(I)$ – aşağıtezlikli veyvletlər, $W(I)$ – yüksəktezlikli veyvletlər və $L(I)$ – veyvlet-liderlərdir.

Veyvletlər piramidasının hər bir komponenti üçün BC-metodu ilə $\{MFS(D), MFS(W_k), MFS(L)\}$ MFS spektri hesablanır:

Veyvlet-lider daha kiçik miqyaslardakı fəza- və skeylinq-qonşuluqlarında bütün veyvlet əmsalların maksimumu kimi müəyyən edilir. Başqa sözlə, $\vec{r}_0$ pikselində $W_{k,j_0}(\vec{r}_0)$ veyvlet-əmsalı üçün müvafiq veyvlet-lider aşağıdakı şəkildə müəyyən edilir:

$$L_{j_0}(\vec{r}_0) = \max_{1\le j\le j_0} \max_{1\le k\le 3} \max_{\vec{r}\in\Omega(\vec{r}_0)} \left|W_{k,j}(\vec{r})\right|, \qquad (3.2.7)$$

burada: $\Omega(\vec{r}_0)$ – mərkəzi $\vec{r}_0$ olan kvadrat qonşuluqdur.

Veyvlet-əmsalların hər bir matrisi üçün [297, s.3785]-də verilmiş alqoritm istifadə edilməklə 26-ölçülü MFS-spektr alınır. Üç miqyas istifadə edilir (J=3) və aşağıtezlikli, yüksəktezlikli və veyvlet-liderlər daxil olmaqla 13 veyvlet-əmsalları matrisi var, nəticədə 26×13=338-ölçülü əlamətlər vektoru alınır. Bu işdə SVM üçün əlamətlərin seçilməsi alqoritmi [109, s.315] istifadə edilməklə barmaq izlərini təsvir etmək üçün 103-ölçülü əlamətlər vektoru alınmışdır.

Eksperimentlərin nəticələri. Qeyd edək ki, süni dəyişilmiş barmaq izləri üzrə əlyetər açıq təsvirlər bazalarının olmaması bu sahədəki tədqiqatçıları çətin vəziyyətdə qoyur. [256, s.45]-da eksperimentlər sintetik yaradılmış barmaq izləri bazalarında aparılmışdı. [307, s.451]-də süni dəyişilmiş barmaq izləri üzrə verilənlər bazası istifadə edilmişdir, lakin bu verilənlər bazası hələlik geniş tədqiqatçılar dairəsinə açıq deyil.

Təklif edilmiş metodun eksperimental yoxlanması üçün FVC2002-DB1 verilənlər bazasından götürülmüş barmaq izləri əsasında sintetik barmaq izləri toplusu yaradılmışdır. FVC2002-DB1 bazasında dəqiqliyi 500 dpi olan optik skanerdən alınmış 640×480 ölçülü barmaq izi şəkilləri toplanmışdır.

İki növ süni dəyişiklik imitasiya edilmişdir [256, s.45]:

1) Z-kəsik (Z şəklində kəsiklə, iki üçbucağın birləşdirilməsi və yenidən yerinə tikilməklə alınır).
2) Mərkəzi fırlanma (şəklin mərkəzində dairəvi sahənin kəsilməsi və onun fırladılması ilə alınır).

Multifraktal spektrlərin hesablanması üçün açıq kodlu proqram təminatı Fraclab və BC-metod üçün Matlab-kodları istifadə edilmişdi [47, s.11].

10-qat kross-validasiya ilə SVM-klassifikasiya üçün LIBSVM [47, s.11] proqramı radial bazis nüvə funksiyası ilə istifadə edilmişdi. LIBSVM nəticələri [0, 1] intervalına xətti miqyaslanmışdı. Verilmiş barmaq izi üçün normallaşdırılmış qiymət əvvəlcədən təyin edimiş keçid qiymətindən kiçik olduqda, təsvirin süni dəyişilmiş barmaq izi təsviri olmasının mümkünlüyü barəsində siqnal verilirdi.

Hesablama eksperimentlərinin nəticələri müxtəlif qiymətlər üçün cədvəl 3.2.1-də verilib. Klassifikasiyanın keyfiyyətini qiymətləndirmək üçün cədvəldə səhv müsbət klassifikasiya nisbətinin (False Positive Rate) verilmiş qiymətlərində düzgün müsbət klassifikasiyalarının nisbəti (True Positive Rate) [138, s.861] göstərilmişdir.

Cədvəl 3.2.1.
Süni barmaq izlərinin düzgün müsbət klassifikasiyalarının tezliyi

Əlamətlər vektorunu hesablama metodu	Səhv müsbət klassifikasiya tezliyi						
	0.1	0.2	0.3	0.5	1	2	3
Fraktal ölçü (Katz metodu)	38	42	44	50	60	76	79
Hölder lokal eksponentləri	45	57	60	64	75	85	88
Multifraktal spektr	54	65	68	73	81	90	93

Beləliklə, barmaq izlərinin kəmiyyət parametrləşdirilməsi üçün ilk dəfə multifraktal analiz istifadə edilərək müəyyənləşdirilmişdir ki, multifraktal spektrin istifadəsi süni dəyişiklik nəticəsində barmaq izində baş verən struktur dəyişikliyini effektiv əks etdirir. Eksperimentlər göstərir ki, təklif edilmiş metod süni dəyişilmiş barmaq izlərini kifayət qədər yaxşı aşkarlayır.

3.3. Barmaq izlərinin diskretləşdirilmiş tekstur deskriptorları əsasında biometrik kriptosistemin sintezi metodu

Tətbiq məqsədindən asılı olaraq, biometrik kriptosistemlərin iki növünü fərqləndirmək olar [184, s.66, 185, s.1888]: (1) açar bağlaması (Fuzzy Commitment Scheme, FCS) və (2) açar generasiyası kriptosistemləri.

Açar bağlaması kriptosistemlərində açar qeydiyyat zamanı biometrik nümunə ilə köməkçi verilənlərdə birləşdirilir. Verifikasiya zamanı yeni biometrik nümunə və

saxlanmış köməkçi verilənlər həmin açarı almaq üçün istifadə olunur. Açar bağlaması üsullarına misallar FCS [193, s.28], qeyri-səlis mücrülər [192, s.408], köməkçi verilənlər sistemləri [202, s.21] və təhlükəsiz eskizlərdir [46, s.18]. Əslində, köməkçi verilənlər sistemləri FCS sxemidir və bağlamaya əlavə olaraq, etibarlı bit seçilməsi üçün istifadəçiyə xas bəzi köməkçi verilənləri saxlayırlar.

Açar generasiyası üsulları qeydiyyat zamanı biometrik nümunədən kriptoqrafik açar alınır (zəruri olduqda köməkçi verilənlərlə). Verifikasiya zamanı yeni biometrik nümunə (və əlyetər olduqda köməkçi verilənlər) istifadə edilməklə həmin açar alınmalıdır. Qeyri-səlis ekstraktorlar [128, s.523] ən geniş istifadə edilən açar generasiyası metodudur. Barmaq izləri üçün qeyri-səlis ekstraktorun reallaşdırılmasına dair bir neçə iş nəşr edilmişdir [285, s.604, 88, s.760]. Lakin reallaşdırma nəticələri [285, s.604]-də göstərilməyib, [88, s.760]-də isə 15 % FAR və FRR göstərilir ki, bunlar praktiki tətbiqlər üçün qəbuledilməzdir.

FCS sxemləri ilk açar bağlaması kriptosistemidir. Qeyri-səlis bağlama konsepsiyası A. Juels və M. Wattenberg [193, s. 28] tərəfindən 1999-cu ildə daxil edilmişdi. O, açarı gizlətmək üçün səhvlərin korreksiyası kodu ilə kriptoqrafik heş funksiyanı birləşdirir. FCS istənilən (xətti) səhvlərin korreksiyası koduna əsaslana bilər və aşağıdakı kimi işləyir:

Fərz edək ki, səhv korreksiyası kodu və h təhlükəsiz kriptoqrafik heş-hunksiyası seçilib və giriş biometrik əlamət vektoru binar formada $x \in \{0,1\}^n$ kimi göstərilir. Qeydiyyat zamanı K kriptoqrafik açarı ECC (Error-Correcting Code) kodlaşdırıcısı ilə $c \in C$ təsadüfi kod sözünə çevrilir, burada C uzunluğu n olan kod sözləri çoxluğudur. $\delta = x - c$ sürüşməsi və $h(c)$ heş qiyməti bağlantı kimi saxlanır.

Verifikasiya zamanı, sistem x' biometrik sorğusunu qəbul edir, $\delta + x'$ hesablayır və mümkün olduqda, ən yaxın c' kod sözünə dekodlaşdırır. Əgər dekodlaşdırılmış c' kod sözünün $h(c')$ heş qiyməti saxlanmış $h(c)$ heş qiymətinə bərabərdirsə, onda nəticə uğurlu hesab edilir və məxfi c kod sözü çıxışa verilir.

FCS sxeminin tələblərindən biri biometrik əlamət vektorunun nizamlanmış binar formada olmasıdır. Bu şərt IrisCode kod üçün yerinə yetirilir, o 2048-bit uzunluqda

binar sətir şəklində təsvir edilir. [160, s.1081]-də müəlliflər IrisCode-dan 140-bit kriptoqrafik açarları 99.5% verifikasiya faizi ilə generasiya edə bilmişdilər.

Barmaq izləri üçün FCS sxeminin reallaşdırılmasında əsas maneə ondadır ki, barmaq izlərinin tanınması adətən barmaq izlərinin spesifik əlamətlərinə – minusiyalara (qabarıqlıq sonlarına və bifurkasiyalara) əsaslanır. Bu təsvir uzunluğu dəyişən nizamlanmamış çoxluqdur və minusiyalarda bir çox səhvlərlə müşaiyət olunur – fərqli sıralama, minusiyaların daxil edilməsi və ya çıxarılması, bunlar biometrik şablonların mühafizəsi üsullarının işlənməsində müxtəlif çətinliklər yaradır [174, s.1-6]. FCS sxeminin nizamlanmamış çoxluqlarla işləyə bilməməsi nöqsanını aradan qaldırmaq üçün [192, s.408] qeyri-səlis mücrü sxemini təklif edir. Qeyri-səlis mücrü yuxarıda qeyd edilən nöqsana qarşı dayanıqlıdır və buna görə barmaq izlərinin minusiyalarla təsviri üçün daha əlverişli hesab edilir.

Barmaq izləri üçün qeyri-səlis mücrü sxeminin bir neçə realizəsi məlumdur. C. Clancy və həmmüəllifləri [113, s.45] ilk dəfə qeyr-səlis mücrü sxemini barmaq izi şablonlarının mühafizəsi üçün tətbiq etmişlər. Onların sxemində yalnız minuasiya koordinatları istifad edilir. Onlar FRR-in qiymətinin 20 %-30 % aralığında olduğunu bildirmişlər. Onların realizəsinin nöqsanlarından biri ondadır ki, şablon və sorğu barmaq izlərinin əvvəlcədən nizamlanması fərz edilir. Həqiqətən də, əvvəlcədən nizamlanma tələbi barmaq izləri üçün qeyri-səlis mücrü sxeminin ən böyük nöqsanlarından biridir: müqayisə edilən iki barmaq izinin uyğun minusiya koordinatları eyni olmalıdır və buna görə də, qeyri-səlis mücrü qurulmazdan əvvəl barmaq izləri nizamlanmalıdır. Barmaq izləri üçün qeyri-səlis mücrü sxemləri üzrə yeni tədqiqatların çoxu bu əsas nöqsanın aradan qaldırılmasına yönəlib.

S. Yang və b. [305, s. 609] əvvəlcədən nizamlama məsələsinin həlli üçün istinad minusiyasından istifadə edilməsini təklif edirlər. Qeyri-səlis mücrünün qurulması və verifikasiyası zamanı istinad minusiyası bir neçə barmaq izi şəkli kombinasiya edilməklə tapılırdı. Barmaq izilərinin 100 şəkildən ibarət kiçik xüsusi bazası istifadə edilməklə qiymətləndirilmiş FRR təxminən 17% olmuşdur.

K. Nandakumar və b. [242, s.744] qeyri-səlis mücrü sxemini reallaşdırmaq üçün minusiya kooordinarlarından və istiqamət məlumatından istifadə edirlər, istiqamət

meydanından çıxarılmış köməkçi verilənlər şablon və sorğu minusiya çoxluqlarını düzləndirmək üçün istifadə olunur. Bundan əlavə, onlar kodlaşdırma və dekodlaşdırma zamanı bir neçə barmaq izi şəklindən istifadə etmişdilər. Bir sorğunu bir şablonla müqayisə etdikdə FVC2002 DB2 verilənlər bazasında qiymətləndirmə zamanı FRR = 9% və FAR = 0.01% alınmışdı.

Qeyri-səlis mücrü sxeminin bir məhdudiyyəti onun barmaq izlərinin minusiyadan başqa digər tekstur məlumatlarından səmərəli istifadə edə bilməməsidir. Müəlliflər [239, s.1-4]-da bu məhdudiyyəti qeyri-səlis mücrü qurularkən minusiya ətrafındakı qabarıqlıq tezliyi və qabarıqlıq istiqaməti məlumatlarını minusiya deskriptorlarında göstərməklə aradan qaldırmağa cəhd edirlər. FVC2002 DB2 bazasından eksperimental nəticələr göstərir ki, minusiya deskriptorları [242, s.744]-də məlumat verilənlərlə müqayisədə FAR qiymətini 0.7%-dən 0.01%-ə azaltmağa imkan verir və 95 % olan GAR (Genuine Acceptance Rate) qiymətinə təsir etmir.

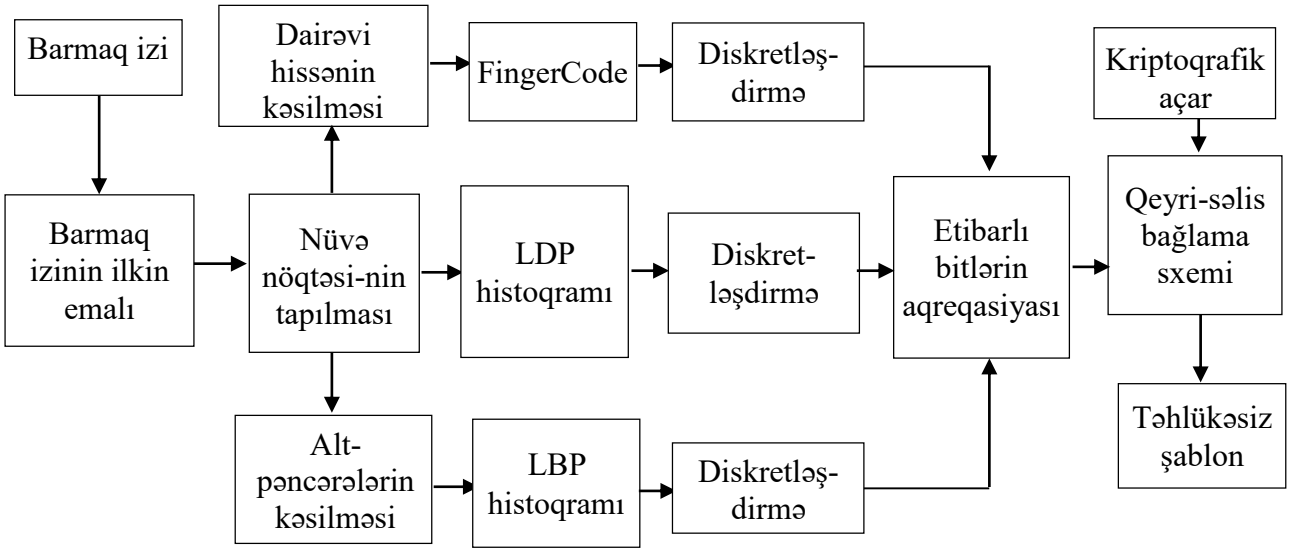
Son vaxtlar barmaq izləri üçün FCS sxemlərinin realizəsinə maraq müşahidə edilir [241, s.1-6]. Praktiki realizələr üçün FCS sxeminin əsas üstünlüyü ondadır ki, o ən sadə və çox tədqiq edilmiş biometrik kriptosistemdir və onun təhlükəsizliyi yaxşı ifadə edilmiş fərziyyələrə əsaslanır [193, s. 28]. [234, s.65]-də göstərildiyi kimi, FCS-də entropiya itkisi qeyri-səlis mücrü sxemindəkindən xeyli kiçikdir. Bundan əlavə, son dövrlər minusiya çoxluğu əsasında bir neçə sabit uzunluqlu binar təsvir təklif edilmişdir [241, s.1-6].

Təəssüf ki, bu metodlar müxtəlif problemlərdən əziyyət çəkir: onlar istiqamət/çevirmə üzərində tükədici axtarış tələb edirlər, yaxud binar təsvir olduqca uzundur, ya da kiçik sayda itmiş yaxud səhv minusiyaya qarşı dayanıqlıdırlar [185].

Biometrik kriptosistem simmetrik kriptosistemlər üçün tələb edilən minimum uzunluqda açarların (məsələn, AES (Advanced Encryption Standard) standartı üçün 128-bit) saxlanmasını və verilməsini təmin etməlidir. Lakin bu imkan yalnız IrisCode üçün nümayiş etdirilmişdir, 140-bitlik açarların FRR = 0.0047% səhv səviyyəsində saxlanmışdır [160, s.1081]. Barmaq izi əsasında FCS-lər üçün oxşar nəticələr IrisCode ilə müqayisədə xeyli aşağıdır - ən yaxşı nəticə FAR=5.4% və FRR = 5.2% səviyyəsində 76-bit açardır [286, s.436].

Təklif edilmiş biometrik kriptosistemin ümumi blok-sxemi

Barmaq izləri üçün təklif edilmiş biometrik kriptosistemin ümumi sxemi şəkil 3.3.1-də göstərilib. Sxemə barmaq izlərinin ilkin emalı; nüvə (istinad) nöqtəsinin tapılması; barmaq izi təsvirinin hissələrə (alt-pəncərələrə) bölünməsi; barmaq izinin tekstur əlamətlərinin çıxarılması; biometrik diskretləşdirmə; etibarlı bitlərin birləşdirilməsi və FCS daxildir. Sonrakı bölmələrdə bu blok-sxemin elementləri ətraflı təsvir olunur.



Şəkil 3.3.1. Təklif edilmiş biometrik kriptosistemin blok-sxemi

Barmaq izlərinin təsviri üçün üç tekstur deskriptoru istifadə edilir: Qabor filtrləri [188, s.846], lokal binar obrazı (Local Binary Pattern, LBP) [257, s. 3-47], lokal istiqamət obrazı (Local Direction Pattern, LDP) [187, s.482]. Barmaq izi tekstur deskriptorlarının binar təsviri üçün etibarlılığa əsaslanan diskretləşdirmə sxemi seçilmişdir [202, s.21].

Təəssüf ki, bir diskretləşdirilmiş barmaq izi deskriptorunun istifadəsi arzulanan məhsuldarlığa malik biometrik kriptosistem qurmağa bir çox səbəbdən imkan vermir. Bu səbəblərə tekstur deskriptorların yetərsiz dəqiqliyi və diskretləşdirmə sxemlərində diskriminativ informasiyanın itirilməsi də daxildir. Bu problemləri aradan qaldırmaq üçün diskretləşdirilmiş barmaq izi tekstur deskriptorlarının aqreqasiyası təklif edilir. Həmçinin biometrik kriptosistemlərin təhlükəsizlik analizində olan son nəticələri [274, s.34] nəzərə almaqla səhvlərin korreksiyası kodlarının seçilməsinə də baxılır. Diskretləşdirilmiş barmaq izi tekstur deskriptorlarından ən etibarlı bitlərin

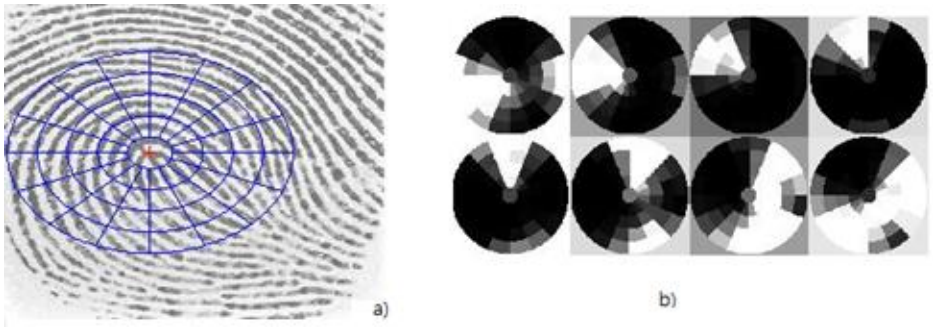
aqreqasiyası və effektiv ECC kodlarının istifadəsi praktikada tələb edilən açar uzunluğuna və biometrik tanıma göstəricilərinə malik biometrik kriptosistem qurmağa imkan verir.

Barmaq izi təsvirinin ilkin emalı, nüvə nöqtəsinin tapılması və sektorlara bölünmə

Barmaq izlərinin keyfiyyəti müxtəlifdir və barmaq izlərini tanıma sistemlərində ilk addımda barmaq izi təsvirindəki qabarıqlıq-çöküklük strukturunun keyfiyyəti yaxşılaşdırılır [227, s. 131]. Barmaq izi təsvirini yaxşılaşdırmaq üçün [227, s. 133-143]-dən məlum üsullar istifadə edilmişdir, bu üsullarda təsvir bir-birini örtən 16×16 ölçülü bloklara bölünür və bloklar tezlik və istiqamət filtrləri vasitəsilə filtrlənir, filtrlərin parametrləri Furye analizi istifadə edilməklə qiymətləndirilən lokal qabarıqlıq tezliyi və istiqamətinə əsaslanır.

Tekstura əsasında barmaq izlərinin mövcud tanınması üsullarında sürüşməyə invariantlıq əldə edilməsi üçün barmaq izlərinin düzləndirilməsi tələb edilir. FingerCode yaradılması metodu bu məqsədlə istinad nöqtəsi kimi nüvə nöqtəsini istifadə edir. Təklif edilən yanaşmada miqyaslı istiqamət meydanı əsasında nüvə nöqtəsinin lokallaşdırılması alqoritmi istifadə edilmişdir.

Nüvə nöqtəsi tapıldıqdan sonra onun ətrafında dairəvi oblast müəyyən edilir və konsentrik halqalara kəsilir, halqaların hər biri sektorlara bölünür (şəkil 3.3.2).



Şəkil 3.3.2. a) İstinad nöqtəsi (+) və sektorlara bölünmə b) müvafiq FingerCode

Barmaq izi təsvirinin ölçüsündən və miqyasdan asılı olaraq aşağıdakı parametrlər seçilmişdir:

- konsentrik halqaların sayı (B = 4);
- hər bir halqanın piksellə eni (b = 20);
- hər bir halqada sektorların sayı (k = 16);

– piksellə daxili radius (r = 12).

Barmaq izi təsvirinin deformasiyalarına invariantlığı təmin etmək üçün sektorların və alt-pəncərələrin hissələri [188, s.846]-də təsvir edilmiş prosedurlar istifadə edilməklə normallaşdırılmışdır.

FingerCode əlamətinin çıxarılması

Təklif edilmiş biometrik kriptosistemində istifadə edilən tekstura əsaslı barmaq izi əlamətləri aşağıda təsvir olunur.

Təklif edilmiş yanaşmanı eksperimental yoxlamaq üçün barmaq izinin FingerCode adlanan tekstura-əsaslı təsviri istifadə edilmişdir. İlk dəfə [188, s.846]-də daxil edilən FingerCode həqiqi qiymətlər alan sabit uzunluqlu vektordur, onu barmaq izlərinin müqayisəsi və klassifikasiyası üçün istifadə etmək olar. Müqayisə adi Evklid məsafəsi əsasında aparılır.

Qabor filtrləri tekstur təsvirdə həm lokal istiqamət, həm də tezlik informasiyasını yaxşı tutur. [188, s.846]-də göstərildiyi kimi, barmaq izi təsvirinin qlobal strukturunu tutmaq üçün filtrdə dörd istiqamət, lokal xarakteristikaları tutmaq üçünsə səkkiz istiqamət kifayət edir.

FingerCode almaq üçün sektorlardakı təsvirlər aşağıdakı cüt simmetrik Qabor filtrləri bankından istifadə edilməklə səkkiz müxtəlif istiqamətdə filtrlənir:

$$G_{\theta,f}(x,y) = exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\delta_x^2}+\frac{y'^2}{\delta_y^2}\right]\right\}\cos(2\pi f x'), \tag{3.3.1}$$

$$x' = x\cdot\sin\theta + y\cdot\cos\theta, y' = x\cdot\cos\theta - y\cdot\sin\theta,$$

burada: $\theta \in \{0°, 22.5°, 45°, 67.5°, 90°, 112.5°, 135°, 157.5°\}$, f – x-oxundan θ istiqaməti boyunca sinusoidal müstəvi dalğanın tezliyidir, δ_x və δ_y uyğun olaraq x- və y-oxları üzrə Qauss bükümünün standart meylləridir. İlkin mənbə olan [188, s.846]-də göstərildiyi kimi, 500 dpi barmaq izi təsvirləri üçün $f = 0.1$, δ_x və $\delta_y$isə hər ikisi 4.0 qəbul edilib.

Filtrlənmiş təsvirlərdə boz rəngin sektorlardakı qiymətlərinin orta mütləq meylləri hesablanır və onlardan FingerCode əlamət vektoru təşkil olunur. FingerCode vektorunun uzunluğu konsentrik halqaların sayından, hər bir halqadakı sektorların

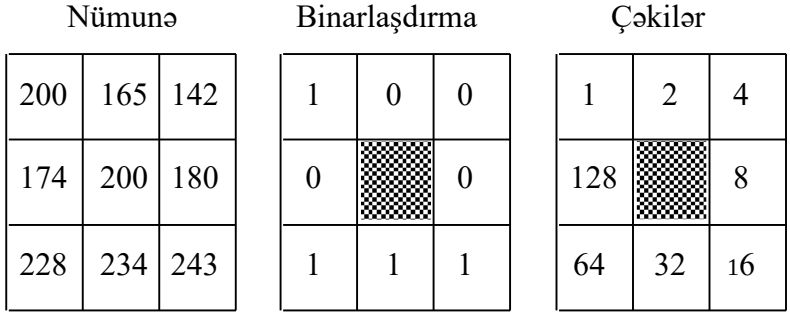
sayından və filtr bankındakı Qabor filtrlərinin sayından asılıdır. Seçilmiş parameter qiymətləri 4×16=64 sektor və FingerCode-un uzunluğu 6×48=512 idi.

LBP əlamətlərinin çıxarılması

LBP teksturların klassifikasiyası üçün güclü əlamətdir və ilk dəfə 1996-cı ildə Ojala və b. tərəfindən daxil edilmişdir [250, s.51]. LBP-nin vacib xüsusiyyətləri onun istənilən monoton boz səviyyəyə invariantlığı və hesablanmasının sadəliyidir. LBP obrazı qabarıqlıq, xətt sonluğu, künclər, ləkələr kimi mikrostrukturları aşkarlamağa imkan verir.

LBP əlamətləri daxil olmaqla teksturların klassifikasiyası, sifətin aşkarlanması, sifətin tanınması, sifət ifadəsinin tanınması, gender və yaş klassifikasiyası kimi müxtəlif tətbiqlərdə uğurla istifadə edilmişdir [185, s.1888]. [243, s3461]-də barmaq izlərinin LBP əsasında hibrid müqayisəsi sistemi təklif edilmişdir, FVC2002 bazası üçün ən yaxşı eksperimental nəticələr EER (equal error rate) qiyməti 6.2% (LBP operatoru birbaşa ağ-qara şəklə tətbiq edilib) və EER = 2.4% (LBP operatoru Qabor filtrinin çıxışına tətbiq edilib) olmuşdur. İki LBP əlamət vektoru arasındakı oxşarlıq onların Evklid məsafəsi əsasında qiymətləndirilir.

Şəkil 3.3.3 əsas LBP əməliyyatlarını illüstrasiya edir.

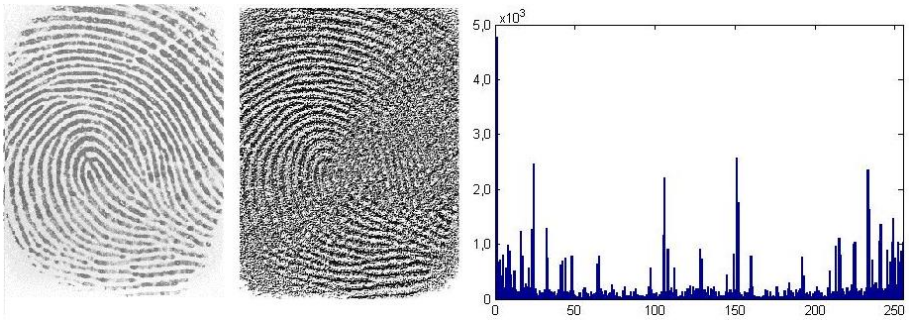


Şəkil 3.3.3. LBP kodunun hesablanması

LBP operatoru pikselin 3×3 ətrafında mərkəzi pikselin qiymətinə görə təyin olunur. Qiymətləri mərkəzi pikselin qiymətindən böyük (və ya bərabər) olan piksellərə 1 qiyməti, kiçik olan piksellərə isə 0 qiyməti verilir. Beləliklə, 8-bitlik binar LBP kodu pikselin ətrafını təsvir edir.

Hər bir pikselin LBP obrazı hesablandıqdan sonra, tekstur şəkli histoqram ilə təsvir olunur. LBP üçün histoqram səbətlərinin sayı $2^8 - 1 = 255$-dir. Şəkil 3.3.4-də barmaq izi, uyğun LBP şəkli və onun histoqramı təsvir edilir.

İlkin LBP sonradan ixtiyari dairəvi ətraf üçün təyin edilmiş və bunun üçün bir neçə genişlənməsi təklif edilmişdir (müntəzəm, dönməyə invariant, çoxmiqyaslı).

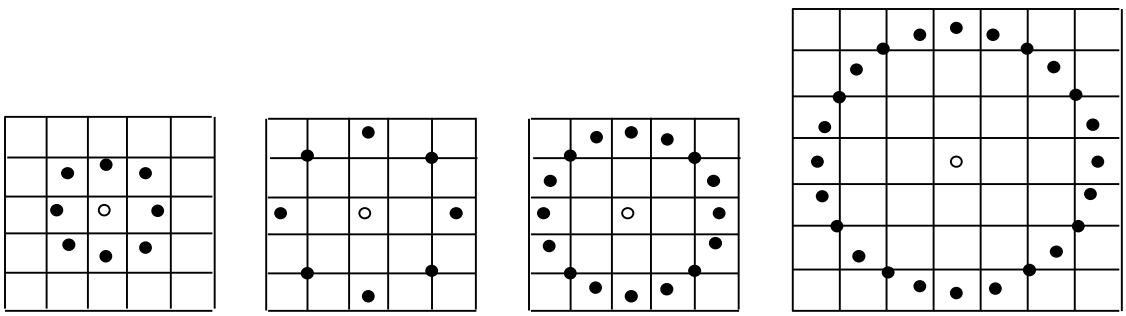


Şəkil 3.3.4. Barmaq izi, uyğun LBP təsviri və onun histoqramı

$LBP_{P,R}$ operatoru g_c-dəki teksturu R $(R > 0)$ radiuslu çevrədə bərabər məsafədə olan P sayda pikselin lokal qonşuluğunu istifadə etməklə təsvir edir. Qonşuların g_p koordinatları $(x_c + R\cos(2\pi p/P), y_c - R\sin(2\pi p/P))$ ilə verilir, burada (x_c, y_c) mərkəzi pikselin koordinatlarıdır. g_c pikselində $LBP_{P,R}$ operatorunun qiyməti belə təyin olunur:

$$LBP_{P,R}(\mathrm{g}_c) = \sum_{p=0}^{P-1} S(\mathrm{g}_p - \mathrm{g}_c) \cdot 2^p, \text{ burada } S(x) = \begin{cases} 1, \text{əgər } x \geq 0 \\ 0, \text{əks halda} \end{cases} \qquad (3.3.2)$$

burada: g_c mərkəzi pikselin qiymətidir və g_p $(p = 0, \ldots, P-1)$ ona qonşu piksellərin qiymətləridir. Qonşu piksel qəfəsin mərkəzi çərçivəsinə dəqiq düşmədikdə onun qiyməti bi-xətti interpolyasiya vasitəsilə hesablanır. Şəkil 3.3.5-də müxtəlif P və R qiymətləri üçün dairəvi simmetrik qonşular çoxluğuna nümunələr göstərilir.



P = 8, *R* = 1.0 *P* = 8, *R* = 2.0 *P* = 16, *R* = 2.0 *P* = 24, *R* = 3.0

Şəkil 3.3.5. Müxtəlif (*P*, *R*) üçün dairəvi simmetrik qonşular çoxluğu

Müntəzəm LBP obrazları [250, s.51]-da daxil edilib, tekstur şəkillərdə eksperimental olaraq müşahidə edilmişdi ki, müəyyən obrazlar (8, 1) qonşuluğu istifadə edildikdə bütün obrazların təxminən 90 %-ni və (16, 2) qonşuluğu istifadə edildikdə 70 % təşkil edir. Bu obrazlar "müntəzəm" adlanırlar və ən çoxu iki 1→0 və ya 0→1 bit keçidinə malikdirlər. Məsələn, LBP obrazı 11111111 (keçid yoxdur) və ya 01100000 (iki keçid) müntəzəmdir, 10101011 (altı keçid) obrazı isə qeyri-müntəzəmdir. 8 seçim nöqtəsi halında 58 müntəzəm obraz vardır. Qeyri-müntəzəm obrazların hamısı üçün bir histoqram səbəti təyin olunur. Deməli, müntəzəm obraz anlayışı LBP obrazların sayını 256-dan 59-a azaldır.

LBP obrazının dönməyə invariantlığı aşağıdakı tərifl ə təmin edilir:

$$LBP_{P,R}^{ri} = min\{ROR(LBP_{P,R}, i)|i = 0,1, \dots, P-1\}, \qquad (3.3.3)$$

burada: *ROR*(*x*, *i*) (ROR – rotate right) *P*-bitlik *x* ədədi üzərində saga dairəvi bit sürüşməsini *i* dəfə yerinə yetirir. Məsələn, 00011101→10001110→…→00111010.

$LBP_{P,R}^{ri}$ operatoru ilkin LBP kodunun bütün dairəvi dönmələrinə baxmaqla və onların ən kiçik qiymətini götürməklə hesablanır. $LBP_{P,R}^{ri}$ dairəvi qonşuluq üzrə istənilən monoton çevirməyə və dönməyə görə invariantdır. Ümumi halda, dönməyə invariant $LBP_{P,R}^{ri}$ obrazlarının sayını hesablamaq bir qədər çətindir. $LBP_{8,1}^{ri}$ üçün dönməyə invariant 36 mümkün obraz var. Deməli, $LBP_{8,1}^{ri}$obrazı 36-səbətli histoqramlar verəcək.

Bu işdə aşağıdakı LBP əlamətlər istifadə edilmişdir:

– $P = 8$, $R = 1$ parametrli LBP. Histoqram səbətlərinin sayı 32-dir. Bu əlamət vektoru LBP8 kimi işarə olunur. Eksperimentlərdə LBP8 əlamət vektorunun ölçüsü 32×16 = 512-dir.
– $P = 16$, $R = 2$ parametrli LBP. Histoqram səbətlərinin sayı 32-dir. Bu əlamət vektoru LBP16 kimi işarə olunur. Eksperimentlərdə LBP16 əlamət vektorunun ölçüsü 32×16 = 512-dir.
– $P = 24$, $R = 3$ pararmetrli LBP. Histoqram səbətlərinin sayı 32-dir. Bu əlamət vektoru LBP24 ilə işarə olunur. Eksperimentlərdə LBP24 əlamət vektorunun ölçüsü 32×16 = 512-dir.

– *Bircins* LBP. Histoqram səbətlərinin sayı 59-dur. Bu əlamət vektoru LBPu2 kimi işarə olunur. Eksperimentlərdə LBPu2 əlamət vektorunun ölçüsü 59×16 = 944-dir.
– Fırlanamya-invariant LBP. Histoqram səbətlərinin sayı 36-dir. Bu əlamət vektoru LBPri kimi işarə olunur. Eksperimentlərdə LBPri əlamət vektorunun ölçüsü 36×16 = 576-dir.

LDP əlamətlərinin çıxarılması

LBP və onun modifikasiyaları təsadüfi küyə və monoton olmayan işıqlanma variasiyalarına qarşı həssasdır. LDP yanaşması Kirş maskası istifadə edilməklə hesablanmış səkkiz istiqamətdə qabarıqlıq çıxışlarına əsaslanır [187, s.482]. Qabarıqlıq çıxışları intensivlik qiymətləri ilə müqayisədə daha az dəyişir və daha stabildirlər, buna görə LDP obrazlarının şəkildə boz çalar səviyyələrində təhriflər zamanı daha dayanıqlı olmaları gözlənilir.

LDP üsulunda Kirş maskası çıxışlarının yalnız k ən dominant istiqamətləri istifadə edilir. 8-bitlik LDP obrazının k ən dominant istiqamətə uyğun k bitinə 1 qiyməti mənimsədilir. Qalan (8–k) bitə isə 0 mənimsədilir. LDP obrazının generasiyası şəkil 3.3.6-da illüstarsiya edilir.

Nümunə

85	32	26
53	50	10
60	38	45

Maska indeksi	*m*7	*m*6	*m*5	*m*4	*m*3	*m*2	*m*1	*m*0
Maska qiyməti	161	97	161	537	313	97	-503	-393
Rank	6	7	5	1	4	8	2	3
Kod biti	0	0	0	1	0	0	1	1
LDP kodu	169							

Şəkil 3.3.6. LDP obrazının generasiyası [187]

Bu işdə LDP obrazı $k = 3$ dominant istiqamətə 1 mənimsədilməklə alınır, buna görə yalnız 56 mümkün qiymət (7, 11, …, 208, 224) var. Buna görə hər bir alt-pəncərə üçün 56-səbətli histoqram hesablanır. Hər bir alt-pəncərənin histoqramları

birləşdirilərək (konkatenasiya edilərək) nəticədə 56×16 = 896 komponent uzunluqda LDP əlamət vektoru alınır.

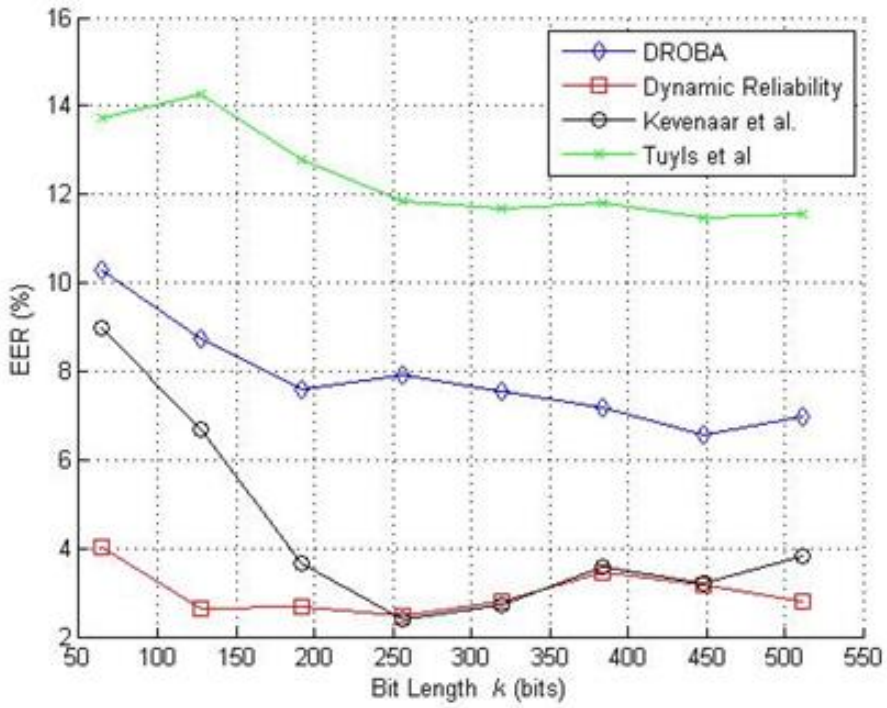
Əlamətlərin diskretləşdirilməsi

FCS sxemi biometrik əlamətlərin sabit uzunluqlu binar formada təsvir edilməsini tələb edir. Lakin bir çox biometrik sistemdə biometrik əlamətlər həqiqi qiymətli vektorlarla ifadə edilir. Buna görə də biometrik diskretləşdirmə metodlarından istifadə edilir, onlar biometrik kriptosistemlərin iş göstəricilərinə ciddi təsir göstərirlər.

Son illərdə bir sıra biometrik diskretləşdirmə metodları təklif edilmişdir [202, s.21, 286, s.436, 221, s.1960]. Mövcud biometrik diskretləşdirmə metodlarının qısa icmalını [221]-də tapmaq olar. Bu metodları bit ayırma rejiminə uyğun olaraq ilkin yanaşmada statik və dinamik sxemlərə bölmək olar. Statik diskretləşdirmə sxemlərində hər bir əlamət elementinə sabit sayda bit ayrılır [202, 286]. Dinamik diskretləşdirmə sxemlərində əlamətin statistik fərqliliyi əsasında dəyişən sayda bit ayrılır [221].

Bu işdə barmaq izi əlamətləri üçün aşağıdakı statik və dinamik biometrik diskretləşdirmə sxemləri eksperimental olaraq yoxlanmışdır: təlim bitlərinin statistikası əsasında etibarlılıq diskretləşdirilməsi sxemi [286], etibarlılıq funksiyası əsasında diskretləşdirmə sxemi [202], aşkarlama faizi optimal bit ayırma sxemi (DROBA - detection rate optimized bit allocation) və etibarlılıqdan asılı dinamik bit ayırma sxemi [221]. Qeyd edək ki, [221]-də etibarlılıqdan asılı dinamik bit ayırma sxemi yalnız sifət əlamət vektorları üçün test edilmişdi.

Biometrik diskretləşdirmə sxemlərinin dəqiqliyini müqayisə etmək üçün klassifikasiya faizinin göstəricisi kimi EER qiyməti, yəni səhv faizlərinin bərabər olduğu FAR = FRR qiymət istifadə edilir. Əldə edilmiş EER nə qədər kiçikdirsə, biometrik diskretləşdirmə sxemi bir o qədər yaxşı hesab olunur. FVC2000 DB2a bazasından FingerCode əlamət vektorları üçün bir sıra diskretləşdirmə sxemlərinin EER göstəriciləri şəkil 3.3.7-də göstərilir.

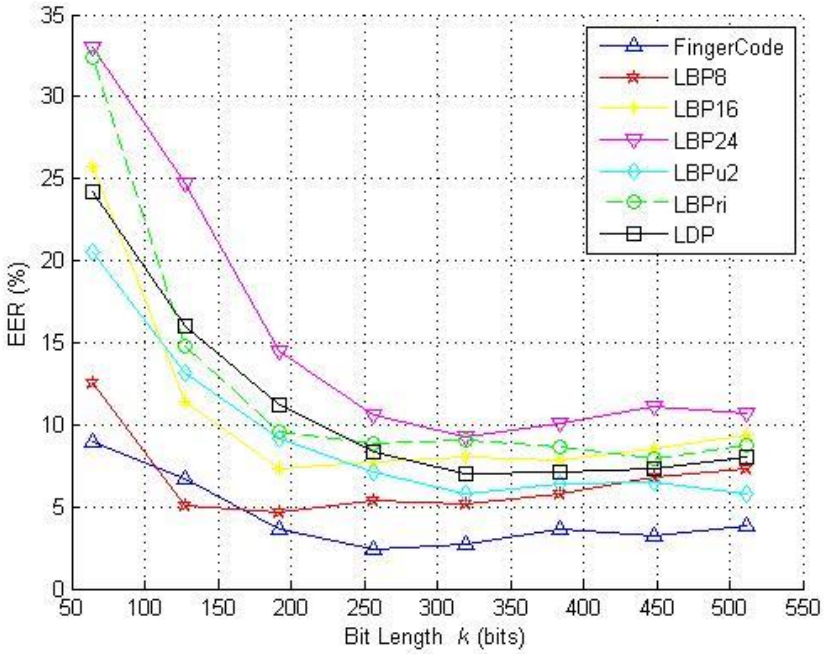


Şəkil 3.3.7. FingerCode üçün diskretləşdirmə sxemlərinin EER məhsuldarlığı

Aparılmış eksperimentlər etibarlılıq funksiyası əsasında diskretləşdirmə sxeminin və etibarlılıqdan asılı dinamik bit ayırma sxeminin barmaq izi əlamətlərinin diskretləşdirilməsi üçün daha dəqiq sxemlər olmasını göstərmişdir. Uzunluq 250–450 bit olmaqla onların hər ikisi eyni məhsuldarlıq göstəricinə malikdir, lakin birinci sxem hesablamalar baxımından daha az tələbkardır. Bu səbəbdən, biometrik kriptosistemin reallaşdırılması üçün bu işdə etibarlılıq funksiyası əsasında diskretləşdirmə sxemi seçilmişdir.

Etibarlılıq funksiyası əsasında diskretləşdirmə sxemi statik bir-bit diskretləşdirmə sxemidir, əlamət elementinin kvantlanması üçün sadə limit əsasında binarlaşdırma üsulu istifadə edilir [202]. Bütün təlim çoxluğunda əlamətin riyazi gözləməsi (medianı) limit qiyməti olaraq seçilir. Bundan sonra, çıxarılmış bitlərdən səhv funksiyası əsasında daha etibarlı komponentlər seçilir. Bu etibarlı komponentlərin yerləri və limit qiyməti köməkçi verilənlər kimi saxlanılır. Köməkçi verilənlər biometrik nümunənin diskretləşdirilməsi üçün istifadə olunur.

FVC2000 DB2a bazasından götürülmüş müxtəlif barmaq izlərinin tekstur deskriptorları üçün etibarlılıq funksiyası əsasında diskretləşdirmə sxeminin EER göstəriciləri şəkil 3.3.8-də verilmişdir.



Şəkil 3.3.8. Barmaq izi əlamətləri üçün etibarlılıq funksiyasına əsaslanan diskretləşdirmə sxemlərinin EER məhsuldarlığı

FingerCode ən yaxşı EER məhsuldarlığı nümayiş etdirir və bit uzunluğu k = 250 olduqda ən kiçik EER təxminən 2.5% olur, k-nın digər qiymətlərində 5 %-dən kiçik qalır. FingerCode üçün EER göstəriciləri digər barmaq izi tekstur deskriptorlarının göstəricilərindən təxminən 3–5% yüksək olur. Şəkil 3.3.8-dən göründüyü kimi, bit uzunluğu k > 200 olduqda, təxminən bütün barmaq izi tekstur deskriptorları 10%-dən kiçik EER nümayiş etdirir. Bit uzunluğu ilkin 64 bitdən 200 bitə kimi artdıqda barmaq izi tekstur deskriptorlarının EER göstəriciləri yaxşılaşır (azalır) və 200–250 bitdən sonra EER göstəriciləri stabilləşir; bit uzunluğu artdıqca EER göstəriciləri əhəmiyyətli dərəcədə pisləşmir.

Barmaq izlərinin diskretləşdirilmiş əlamət deskriptorlarını birləşdirmək üçün aşağıdakı sadə qayda istifadə edilir: verilmiş uzunluqda bit-sətrini almaq üçün diskretləşdirilmiş əlamətlərdən seçilmiş bitlərin nisbi sayı EER göstəricilərinə və əlyetər etibarlı bitlərin sayına uyğun olaraq müəyyən edilir. Diskretləşdirilmiş iki deskriptordan verilmiş uzunluqda bit-sətrini almaq üçün kiçik EER-ə malik olan deskriptordan daha çox bit seçilir. Bütün bitlərin sayından birləşdirilmiş birinci və ikinci deskriptorlara ayrılmış bitlərin nisbi sayını (çəkiləri) uyğun olaraq w_1 və w_2

kimi işarə edək. Birləşdirilmiş deskriptorların optimal çəkiləri hər bir deskriptor cütü üçün eksperimental olaraq müəyyən edilmişdir. Məsələn, FingerCode və LBP24 əlamətlərindən 255 bitlik bit-sətri almaq üçün optimal çəkilər $w_1 = 0.65$ (FingerCode üçün) və $w_1 = 0.35$ (LBP24 üçün) götürülmüşdü. Başqa sözlə, 255 bitlik bit-sətri diskretləşdirilmiş FingerCode-dan $round(255 \cdot 0.65) = 166$ bit və diskretləşdirilmiş LBP24-dən $round(255 \cdot 0.35) = 89$ bit konkatenasiya edilməklə alınmışdı. Eksperimentlər göstərmişdir ki, diskretləşdirilmiş barmaq izi tekstur deskriptorlarının əksəriyyətində 250-dən çox etibarlı bit olur. Əsasən bu səbəbdən, 511 bit almaq üçün birləşdirilmiş deskriptorlar üçün optimal çəkilər $w_1 = w_2 = 0.5$ götürülmüşdür.

Biometrik kriptosistemin qurulması üçün kodlaşdırma üsulunun seçilməsi

Biometrik kriptosistemlərin qurulması zamanı kritik vacib və trivial olmayan məsələlərdən biri səhv korreksiyası kodlarının və onların parametrlərinin düzgün seçilməsidir. Biometrik kriptosistemlər bəzi praktiki təhlükəsizlik hücumlarına həssasdırlar [274, 234]. Hücumların bəziləri istifadə edilən ECC ilə əlaqəlidir. Belə hücumların ən vacib növləri ECC-in "yumşaq dekodlaşdırma" və ya pozma rejimində yerinə yetirilməsi hücumu və ECC histoqram hücumudur. Bu hücumların ümumi icmalı [274]-də verilib.

FCS sxemlərinə müxtəlif təhlükəsizlik hücumları, xüsusi halda bu sahədəki tədqiqatçıların istifadə etdikləri "parçalama ilə kodlaşdırma" yanaşmasının səbəb olduğu hücumlar [274]-də müzakirə edilir. [274, s.34-39]-də vurğulanır ki, "[160]-*dəki kimi kiçik hissələr ardıcıllığından ibarət olan ECC-lərin kodun çıxış statistikasını istismar edən hücumlara qarşı daha həssas olması güman edilir*." Müəlliflər göstərirlər ki, yeganə bloklu ECC-dən istifadə edən biometrik kriptosistemlər tərifə görə bu növ hücumlara qarşı təhlükəsizdirlər və LDPC kodları onları aradan qaldırmaq üçün namizəd kimi irəli sürülür [185].

Biometrik kriptosistemlərin qurulması zamanı ECC seçilərkən aşağıdakı fikir də nəzərə alınmalıdır. Bəzi ECC-lərdə korreksiya edilə bilən bitlərin sayı səhv obrazından asılıdır. Məsələn, IrisCode səhv obrazlarının ətraflı öyrənilməsi əsasında

[160, s.1960]-də təsadüfi bit səhvlərinin korreksiyası üçün Adamar kodu seçilmişdi, Rid–Solomon kodu isə blok səviyyəsindəki səhvləri, yəni paket səhvlərini korreksiya etmək üçün istifadə edilmişdi. Barmaq izi əlamətləri üçün biometrik diskretləşdirmə sxemlərinin səhv obrazlarının dəqiq öyrənilməsinə bu iş çərçivəsində baxılmır və ECC kodları təsadüfi bit səhvlərinin korreksiyası üçün istifadə olunur.

Yuxarıdakı arqumentləri nəzərə alaraq, bu işdə biometrik kriptosistemlərin qurulması üçün BCH və LDPC kodları istifadə edilir. Bu kodların hər ikisi təsadüfi bit səhvlərini korreksiya edə bilir, bəzi müəlliflər səhvlərin korreksiyası üzrə LDPC və BCH kodlarının müqayisəsini vermişlər [203, s.392].

BCH kodları

Bose–Chaudhuri–Hocquenghem (BCH) kodları tsiklik səhv korreksiyası kodudur. Ən çox istifadə edilən BCH kodları binar əlifba ilə işləyir. Binar BCH kodlarını Hocquenghem 1959-cu ildə və ondan asılı olmadan Bose və Chaudhuri 1960-cı ildə təklif etmişdi. BCH kodları biometrik kriptosistemlər daxil olmaqla müxtəlif tətbiqlər üçün populyar seçimdir [202, 88, 286], çünki onlar məhsuldarlığına görə blokun uzunluğu bir neçə yüz bit və kod sürəti eyni olan mövcud blok kodlarının əksəriyyətindən üstündür [185].

Bu işdə dar mənada binar BCH kodları istifadə edilir [235, s. 235]. Tsiklik kodu onun bütün kod sözlərinin bölündüyü $g(x)$ törədici çoxhədlisi ilə müəyyən etmək olar. GF(2^m) üzərində uzunluğu $n = 2^m - 1$ olan, ən azı t səhvi korreksiya edə bilən dar mənada binar BCH kodunun bu törədici çoxhədlisini aşağıdakı üsulla qurmaq olar.

Tutaq ki, α GF(2^m)-nin primitiv elementdir. α^{2i-1}, $1 \le i \le t$ elementinin minimal çoxhədlisi $\phi_{2i-1}(x)$-dir. GF(2^m) üzərində uzunluğu $n = 2^m - 1$ olan, ən azı t səhvi korreksiya edə bilən dar mənada binar BCH kodunun bu törədici çoxhədlisi

$$g(x) = LCM\{\phi_1(x), \phi_3(x), \dots, \phi_{2t-1}(x)\}, \qquad (3.3.4)$$

ilə verilir, burada LCM ən kiçik ortaq bölünəni bildirir. Hər bir minimal $\phi_{2i-1}(x)$ çoxhədlisinin dərəcəsi m-dən böyük deyil, ona görə $g(x)$-in dərəcəsi də mt-dən böyük deyil. Bu o deməkdir ki, kod ən çox mt cütlük yoxlaması bitinə malikdir.

BCH kodlarının dekodlaşdırma proseduruna üç addım daxildir [235, s. 235-292]: 1) sindromun hesablanması; 2) səhv lokatoru çoxhədlisinin müəyyən edilməsi, bu çoxhədlinin kökləri səhvin olduğu yeri göstərir; 3) Chien axtarış alqoritmindən istifadə etməklə səhv lokatoru çoxhədlisinin köklərinin tapılması. Hesablanmış sindromdan səhv lokatoru çoxhədlisinin tapılması üçün müxtəlif üsullar mövcuddur və BCH kodları üçün Berlekamp–Massey alqoritmi geniş tətbiq edilir.

Binar BCH kodu adətən (n, k, t) üçlüyü ilə işarə edilir, burada $n = 2^m - 1$ (müəyyən $m \geq 3$ qiyməti üçün) blokun uzunluğu (binar biometrik şablonun uzunluğu), k məlumatın uzunluğu (məxfi açarın uzunluğu) və t səhv korreksiyası tutumudur ($n - k \leq mt$).

LDPC kodları

LDPC (Low-density parity-check – aşağı sıxlıqlı cütlük yoxlaması) səhvin korreksiyası üçün xətti kodlardır. Onların binar cütlük yoxlaması matrisində hər bir sətir və sütündа az sayda 1 var. LDPC kodlarını 1960-cı ildə Qallaqer təklif etmişdi [235, s. 634]; bir neçə onillik ərzində əsasən mürəkkəb hesablama tələblərinə görə diqqəti cəlb etməmişdi, lakin 1990-cı illərdə D. MacKay və R. Neal, həmçinin N. Wiberg tərəfindən təkrar kəşf edilmişdi. Bu kodların Şennon limitinə yaxınlaşma imkanı nümayiş etdirilmişdir [185]. Oların digər üstünlükləri sadə və effektiv kodlaşdırma metodları və onların dekodlaşdırma üçün zamana görə xətti çətinlikli alqoritmlərə malik olmasıdır.

LDPC kodunun strukturu H cütlük yoxlaması matrisi ilə tamamilə müəyyən edilir. Əgər H matrisində hər bir sütunda w_c 1və hər və bir sırada $w_r = w_c(n/m)$ sayda 1 varsa, onda belə LDPC kodları requlyar adlanır. Yuxarıdakı tərif nəzərdə tutur ki, $w_c << m$, $w_r << n$. Yaxşı LDPC kodları üçün zəruri şərt $w_c \geq 3$-dir. Bir sətirdəki və sütundakı 1-lərin sayı sabit olmadıqda bu kodlar irrequlyar LDPC kodları adlanır. Ümumi halda, qeyri-requlyar LDPC kodlarının məhsuldarlığı requlyar LDPC kodlarından üstündür [260, s.619].

H cütlük yoxlaması matrisi ilə yanaşı, LDPC kodları çox zaman ikihissəli Tanner qrafı ilə də təsvir olunur. İkihissəli qraf elə istiqamətlənməmiş qrafdır ki,

onun təpələrini iki sinfə elə ayırmaq olar ki, eyni bir sinfə aid təpələr heç bir tillə birləşməsin [64, s. 14]. Tanner qrafında təpələrin bu iki sinfi dəyişən qovşaqları (v-qovşaqlar) və yoxlama qovşaqları (c-qovşaqlar) adlanır. (Ədəbiyyatda dəyişən qovşaqlarına simvol və ya bit qovşaqları, yoxlama qovşaqlarına isə funksiya qovşaqları da deyilir.) LDPC kodunun Tanner qrafı birbaşa qurulur: əgər H matrisində h_{ji} elementi 1-dirsə, onda j yoxlama qovşağı i simvol qovşağına birləşir.

LDPC kodlarında kodlaşdırma alqoritmi $x = uG$ ilə ifadə oluna bilər, burada G generator matrisidir, u məlumat bitləridir və x isə nəticədə alınan kod sözüdür. Bütün kod sözləri $xH^T = 0$ bərabərliyini ödəməlidir. Kodlaşdırma o faktdan istifadə edir ki, xətti blok kodunun istənilən generator matrisi sistematik formada göstərilə bilər. G generator matrisi və H cütlük yoxlama matrisi arasında $GH^T = 0$ münasibəti var. G-nin qurulması üsullarından biri Qauss yoxetmə üsulu ilə H matrisini $H = [P^{\mathrm{T}}\ I]$ şəklinə gətirməkdir, burada H matrisi $m \times n$, P isə $m \times (n - m)$ ölçülüdür. Sonra G generator matrisi $G = [I\ \ P^{\mathrm{T}}]$ kimi formalaşdırıla bilər, burada G-nin ölçüləri $(n-m) \times n$-dir.

BCH kodlarından fərqli olaraq LDPC kodları ümumi halda ehtimallı dekodlaşdırma strategiyasından istifadə edir. LDPC kodları dekodlaşdırma üçün MPA (Message-Passing Algorithm) alqoritmlərindən istifadə edir (məlumat 1 və ya 0 ötürülməsi ehtimalıdır) [185]. Alqoritmin bütün iterasiyalarında məlumatlar simvol qovşaqlarından yoxlama qovşaqlarına və yoxlama qovşaqlarından geriyə – simvol qovşaqlarına ötürülür. Müxtəlif MPA alqoritmləri ötürülən məlumatların tipindən və ya qovşaqlarda yerinə yetirilən əməliyyatlardan asılı olaraq adlandırılır (BPA – belief propagation algorithm, SPA – sum-product algorithm və s.).

LDPC kodunun məhsuldarlığı Tanner qrafındakı ən qısa tsikllərin uzunluğundan (kodun əhatəsindən) asılıdır. MPA alqoritmlərində posterior ehtimalların asılı olmaması fərz edilir. Qısa tsikllər MPA məhsuldarlığına ziyan vurur, çünki asılı olmama fərziyyəsini pozurlar. İkihissəli qrafda ən qısa mümkün tsiklin uzunluğu 4-dür. Bu uzunluqda tsiklin olmamasını cütlük yoxlama matrisinin bütün sətirlərinin (və ya sütunlarının) skalyar hasili ilə müəyyən etmək mümkündür. Əgər matrisin sütunlarının (və ya sətirlərinin) cüt-cüt hasilləri 1-dən böyük deyilsə, onda bu,

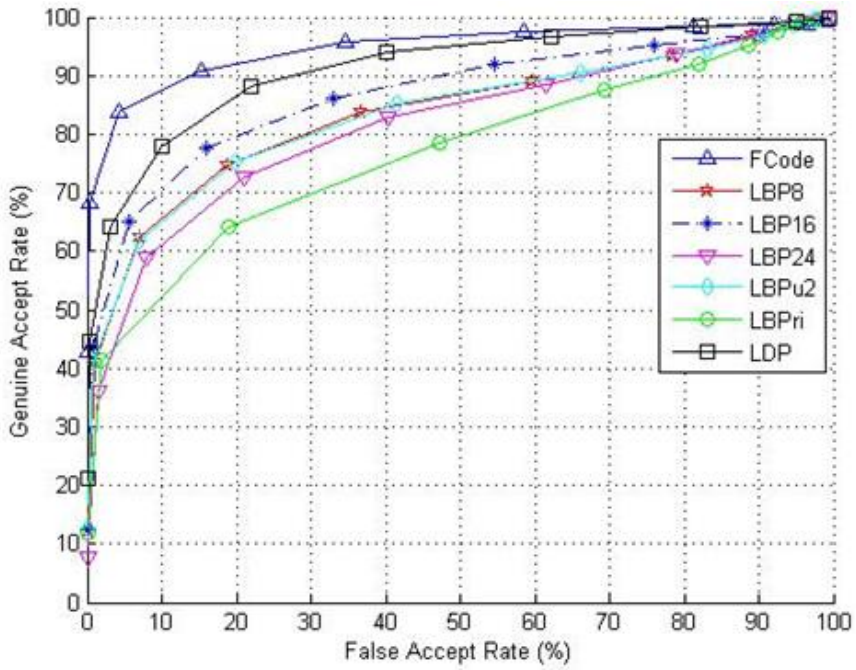
uzunluğu 4-ə bərabər olan tsiklin olmadığını göstərir. Uzunluğu 4 olan bütün tsikllər yox edilsə də, uzunluğu 6-ya bərabər olan tsikllər qala bilər. LDPC kodlarının cütlük yoxlama matrislərində minimal uzunluqlu tsikllərin axtarılmasına və aradan qaldırılması alqoritmlərinə həsr edilmiş bir çox tədqiqat vardır [127, s.1-16].

Ədəbiyyatda LDPC kodunun cütlük yoxlama matrisinin qurulmasına həsr olunmuş çox sayda üsul mövcuddur. Qurulma metodlarına görə LDPC kodlarını təsadüfi kodlara və strukturlu kodlara ayırmaq olar. Təsadüfi LDPC kodları onların Tanner qraflarının müəyyən struktur xassələrinin, məsələn, qrafın əhatəsi və qovşaqların dərəcə paylanmaları əsasında qurulur [260, s.619]. Strukturlu LDPC kodları müəyyən cəbri və ya kombinator prinsiplər əsasında qurulur [289, s.1156].

Bu işdə LDPC kodlarının cütlük yoxlama matrisinin qurulması üçün Hu və b. [170, s.386] tərəfindən daxil edilmiş PEG (Progressive Edge-Growth) alqoritmi istifadə edilmişdir. PEG alqoritmi simvol qovşaqları və yoxlama qovşaqları arasında tilləri ardıcıl olaraq müəyyən edir. PEG alqoritmi ilə ixtiyari parametrli requlyar və qeyri-requlyar LDPC kodları qurmaq olar. Simvol qovşaqlarının sayı n, yoxlama qovşaqlarının sayı m və simvol qovşaqlarının dərəcə paylanması verildikdə PEG alqoritmi Tanner qrafını ardıcıl şəkildə elə qurmağa imkan verir ki, növbəti tili əlavə etdikdə mümkün ən böyük lokal əhatə əldə edilsin [170, s.386]. Yaxşı qeyri-requlyar dərəcə paylanmasını sıxlıq evolyusiyası metodu ilə əldə etmək olar [185, s.1888].

Eksperimentlərin nəticələri və müzakirələr. Təklif edilmiş yanaşmanın iş göstəricilərini test etmək üçün FVC 2000 DB2a barmaq izləri bazası istifadə edilmişdir [145]. FVC 2000 DB2a bazasında 100 müxtəlif barmağın hər birinin 8 təsviri var; təsvirlərin ölçüləri 256×364 pikseldir, ayırdetmə 8-bit dəqiqliyi ilə 500 dpi-dir. Təhlükəsiz biometrik şablonun yaradılması üçün hər bir barmağın ilk 5 təsviri və verifikasiya üçün sonrakı 3 barmaq izi istifadə edilir.

Barmaq izi tekstur deskriptorları əsasında nəticələrin müqayisəsi. Müqayisə üçün Evklid məsafəsi istifadə edilməklə barmaq izlərinin tekstur deskriptorları əsasında barmaq izlərini tanıma sistemi realizə edilmişdir, onun nəticələri şəkil 3.3.9-da göstərilmişdir.



Şəkil 3.3.9. Barmaq izi tekstur əlamətlərinin FVC2000 DB2a bazasında məhsuldarlığı

Qeyd edək ki, [188, s.846]-də dönməyə invariantlığın təmin edilməsi üçün barmaq izinin qeydiyyat zamanı onun təsvirinin 11.25° addımı ilə bütün dönmələrinə uyğun gələn 10 FingerCode şablonu yaradılmış və verilənlər bazalarında saxlanmışdır. Yekun müqayisə qiyməti kimi təqdim olunmuş barmaq izinin FingerCode şablonunun saxlanmış 10 şablonla müqayisəsindən alınmış qiymətlərin minimumu götürülür [188, s.846]. Bu işdə yalnız bir şablon istifadə edilmişdir və FingerCode üçün nəticələr də bir şablona uyğun gəlir.

Barmaq izi tekstur deskriptorları FingerCode, LBP8, LBP16, LBP24, LBPu2, LBPri və LDP üçün EER göstəricisi FVC2000 DB2a bazasında uyğun olaraq 10.96%, 22.79%, 19.54%, 24.6%, 22.88%, 29.56% və 15.95%-dir.

BCH kodları ilə qurulmuş biometrik kriptosistemlərin məhsuldarlığı

Burada BCH kodları istifadə edilməklə qurulmuş biometrik kriptosistemin FVC2000 DB2a barmaq izləri bazasında test edilməsi nəticələri göstərilmişdir.

BCH kodları bütün (n, k, t) üçlükləri üçün mövcud deyil, buna görə $n = 255$ və $n = 511$ blok uzunluğu üçün mümkün BCH kodların siyahısından seçilmişdir. Cədvəl 3.3.1-də müqayisə üçün uyğun kodlar və bit səhvlərinin faizi göstərilmişdir.

Qeyd edək ki, $n = 255$ blok uzunluğunda seçilmiş parametrlərlə BCH kodlarının korreksiya etdiyi bitlərin maksimal sayı binar vektorun 8.6 % və 17.6 % arasındadır.

Blok uzunluğu $n = 511$ olduqda seçilmiş parametrlərlə BCH kodlarının ən yaxşı bit səhvləri faizi 21.6 % və 36.5 %. arasındadır.

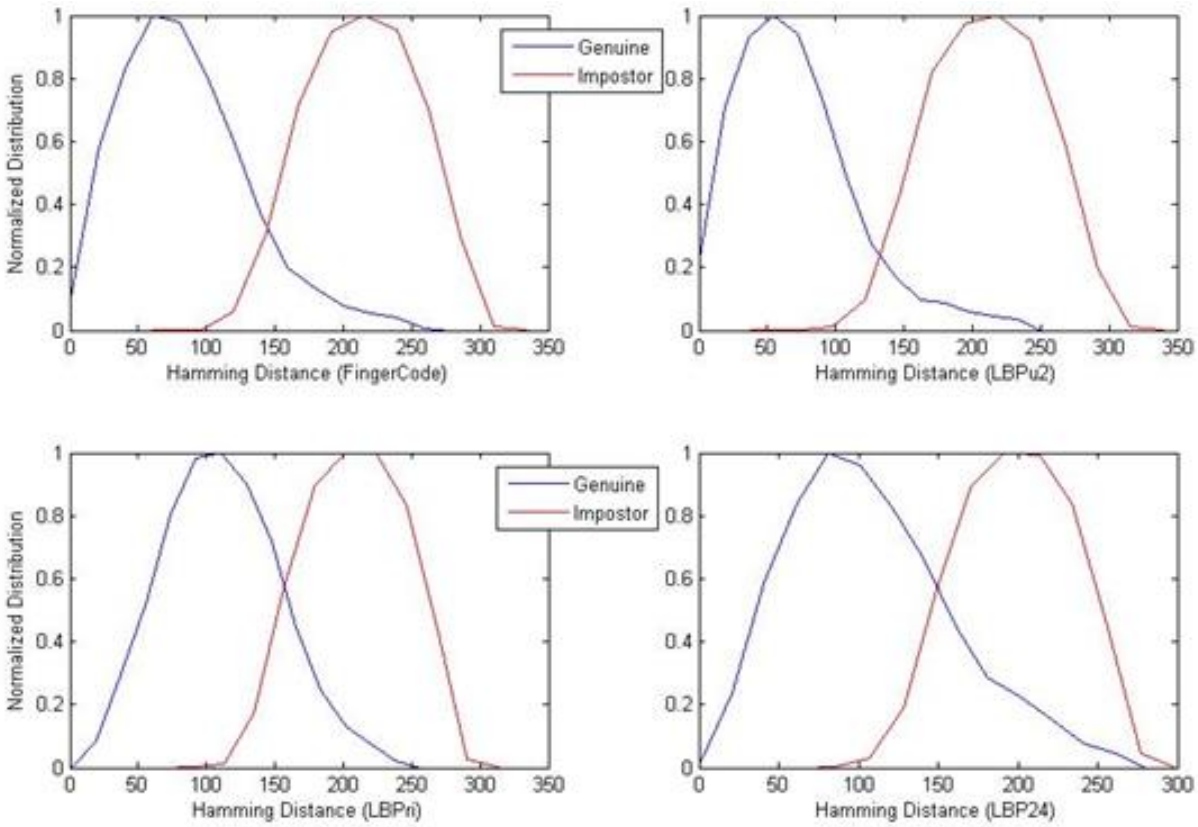
Cədvəl 3.3.1.
BCH kod parametrlərinin seçilməsi

n	k	t	Kod sürəti (k/n)	Bit-səhvi nisbəti (t/n)	n	k	t	Kod sürəti (k/n)	Bit-səhvi sürəti (t/n)
255	107	22	0.419	0.086	511	130	55	0.254	0.216
255	91	25	0.357	0.098	511	103	61	0.202	0.239
255	71	29	0.278	0.114	511	85	63	0.166	0.247
255	63	30	0.247	0.118	511	76	85	0.149	0.333
255	47	42	0.184	0.165	511	67	87	0.131	0.341
255	37	45	0.145	0.176	511	49	93	0.096	0.365

Qeyd edək ki, hər bir istifadəçinin bir neçə təlim nümunəsi olduğundan və qeyri-səlis bağlama əməliyyatı müxtəlif təhlükəsiz C_i şablonları verdiyindən, bu şablonlar bütün C_i-lərin ədədi ortası götürülməklə bir istinad şablonunda birləşdirilir.

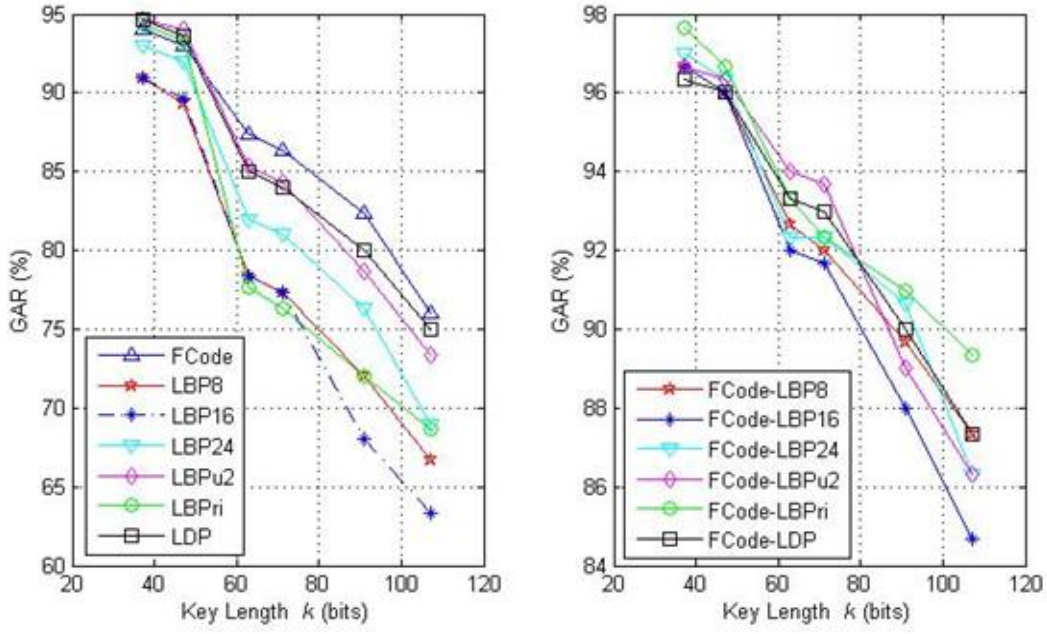
Eksperimentlərdə 300 yüz həqiqi və 29,700 saxta istifadəçi müqayisəsi aparılmışdı. Qurulmuş biometrik kriptosistemin dəqiqliyi GAR (burada GAR = 1 – FRR) və FAR ilə qiymətləndirilmişdir. Eksperimentlərdə FAR qiyməti 0-a bərabər olmuşdur. Bunu belə izah etmək olar. ECC-in səhv korreksiyası potensialı verifikasiya limiti kimi çıxış edir. Səhvlərin korreksiyası potensialının artırılması verifikasiya limitinin artmasına ekvivalentdir. Deməli, səhvlərin korreksiyası potensialını artırmaqla FRR-i azaltmaq olar. Lakin bunun nəticəsində FAR da artır.

Diskretləşdirilmiş barmaq izi tekstur deskriptorları əsasında həqiqi və saxta istifadəçi müqayisələri üçüm Hemminq məsafələrinin paylanması əyriləri şəkil 3.3.10-da göstərilib. Bu məsafə paylanması əyrilərindən görünür ki, həqiqi və saxta istifadəçilərə aid məsafələr yalnız Hemminq məsafəsi 100-dən böyük olduqda bir-biri ilə örtüşür. Seçilmiş BCH kodlarının səhv korreksiyası potensialı (t parametri) 100-dən kiçikdir (cədvəl 3.3.1). Deməli, saxta istifadəçinin açar generasiyası cəhdlərinin heç biri uğurlu olmayacaq, bunun nəticəsində FAR = 0 olacaq. Qeyd edək ki, həqiqi və saxta istifadəçi müqayisələri üçün Hemminq məsafələrinin paylanması digər barmaq izi əlamətləri üçün də oxşar formadadır (şəkil 3.3.10).



Şəkil 3.3.10. Diskretləşdirilmiş barmaq izi tekstur deskriptorları üçün Hemminq məsafələrinin paylanması

Şəkil 3.3.11 barmaq izi əlamətlərinin birləşdirilməsi olmadan və birləşdirilməsi halında blok uzunluğu $n = 255$ olan BCH kodları istifadə edildikdə GAR göstəricisinin açarın uzunluğundan asılılığı göstərilir.



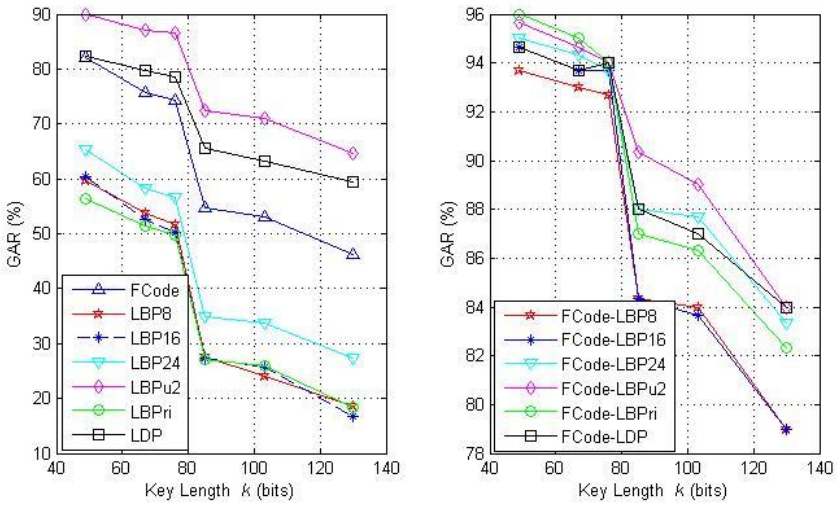
a) birləşdirmə olmadan fusion (b) birləşdirmə ilə

Şəkil 3.3.11. Təklif edilmiş biometrik kriptosistemin blok uzunluğu $n = 255$ olan BCH kodları üçün GAR məhsuldarlığı

Şablon mühafizəsi olmayan biometrik sistemlərin EER göstəricilərindən gözlənildiyi kimi (şəkil 3.3.11), ən yaxşı göstəricilər FingerCode və LDP əlamətləri ilə qurulmuş FCS sxemlərinə məxsusdur. LBP-əsaslı barmaq izi əlamətləri arasında ən yaxşı göstəricilər LBPu2 və LBP24 ilə alınır. BCH(255,47,42) kodu bit səhvlərinin təxminən 16.5 %-ni korreksiya edə bilər, nəticədə seçilmiş əlamətlərin əksəriyyəti GAR>90 % olmaqla uzunluğu k = 47 olan açar generasiya etməyə qabildir. Parametri n = 255 olan BCH kodunun səhv korreksiyası potensialı aşağıdır. Açarın uzunluğu artdıqca, səhv korreksiyası potensialı azalır və nəticədə GAR sürətlə aşağı düşür.

İki barmaq izi əlamətlərindən etibarlı bitlərin birləşdirilməsi n = 255 parametrli BCH kodları üçün açarın uzunluğunu qəbul edilən GAR qiymətində xeyli artırmağa imkan verir. Məsələn, diskretləşdirilmiş əlamətlərin birləşdirilməsi GAR = 90–92% qiymətində birləşdirilən əlamətlərin bütün kombinasiyalarında 80 bit uzunluqda açarların generasiyasına imkan verir. FingerCode-LBPu2, FingerCode-LDP və FingerCode-LBPri kombinasiyaları digər əlamət kombinasiyaları ilə müqayisədə yüksək göstəricilərə malik olur.

Şəkil 3.3.12-də tək və birləşdirilmiş barmaq izi əlamətləri istifadə edildikdə n = 511 parametrli BCH kodu üçün GAR göstəricisinin açar uzunluğundan asılılığı göstərilir.



(a) birləşdirmə olmadan (b) birləşdirmə ilə

Şəkil 3.3.12. Təklif edilmiş biometrik kriptosistemin blok uzunluğu n = 511 olan BCH kodları üçün GAR məhsuldarlığı

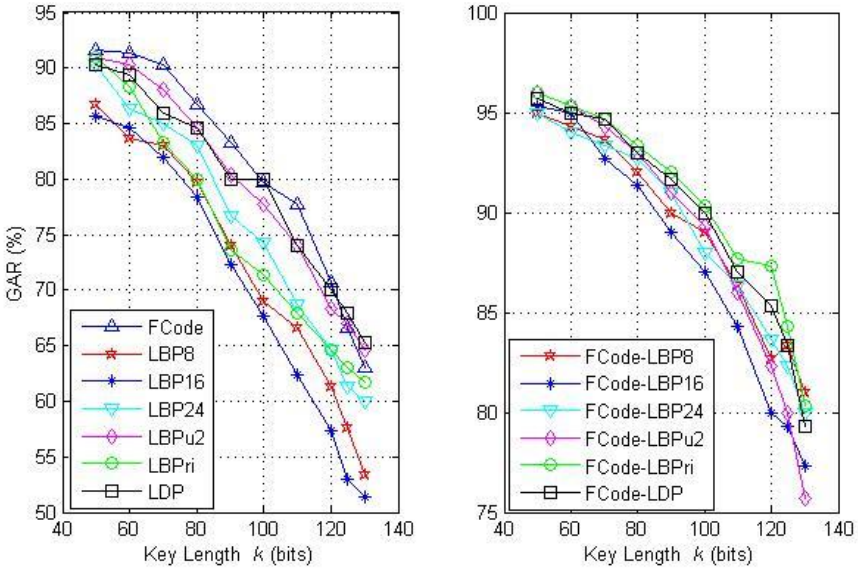
Bu kodun səhv korreksiyası potensialı yüksəkdir – ən pis halda 21 %-dən çoxdur (Cədvəl 3.3.1). Tək barmaq izi əlamətləri arasında LBPu2 əlamətində ən yüksək göstəricilər alınır, çünki bu əlamət daha dayanıqlıdır və barmaq izi təsvirlərinin mikro-tekstur elementlərini daha dəqiq əks etdirir.

İki barmaq izi əlamətinin birləşdirilməsi əlamətlərin bütün cüt kombinasiyaları üçün GAR = 92–94 % səviyyəsində 80 bit uzunluğunda açarlar almağa imkan verir. FingerCode-LBPu2, FingerCode-LBP24 və FingerCode-LBPri kombinasiyaları 50–80 bit açar uzunluğunda digər əlamət kombinasiyaları ilə müqayisədə daha yüksək göstəricilərə malik olur. FingerCode-LBPu2 kombinasiyası da GAR ≈ 89% ilə 100 bit uzunluqda açarların generasiyasına imkan verir.

LDPC kodları ilə qurulmuş biometrik kriptosistemlərin məhsuldarlığı. Tutaq ki, LDPC(n, k) blok uzunluğu n və məlumat bit uzunluğu k olan LDPC kodunu təsvir edir. Blok uzunluğu $n = 255$ və $n = 511$ olan LDPC üçün də eksperimentlər aparılmışdır. Blok uzunluğu $n = 255$ olduqda k parametri 5 və ya 10 addımı ilə 50-dən 120-yə qədər dəyişən LDPC kodu seçilmişdi. $n = 511$ olduqda isə k parametri 5 və ya 10 addımı ilə 60-dan 140-a kimi dəyişən LDPC kodu seçilmişdi. Seçilmiş parametrlər əsasında kod sürəti 0.13–0.27 diapazonunda dəyişir. Eksperimentlər üçün qeyri-requlyar cütlük yoxlaması matrisləri PEG alqoritminin istifadəsi ilə generasiya edilmişdir (www.telecom.tuc.gr/~alex/software/peg.zip).

Şəkil 3.3.13-də tək və birləşdirilmiş barmaq izi əlamətləri istifadə edilməklə reallaşdırılmış FCS sxeminin GAR göstəricisini $n = 255$ parametrli LDPC kodu üçün göstərilib. LDPC kodunun səhv korreksiyası potensialı blok uzunluğu eyni olan BCH kodundan yüksəkdir. Tək əlamət halında blok uzunluğu $n = 255$ olan LDPC kodunun GAR göstəricisi blok uzunluğu eyni olan BCH kodunun GAR göstəricisinə oxşardır, bu zaman FingerCode, LDP və LBPu2 əlamətləri yüksək göstəricilərə malik olur.

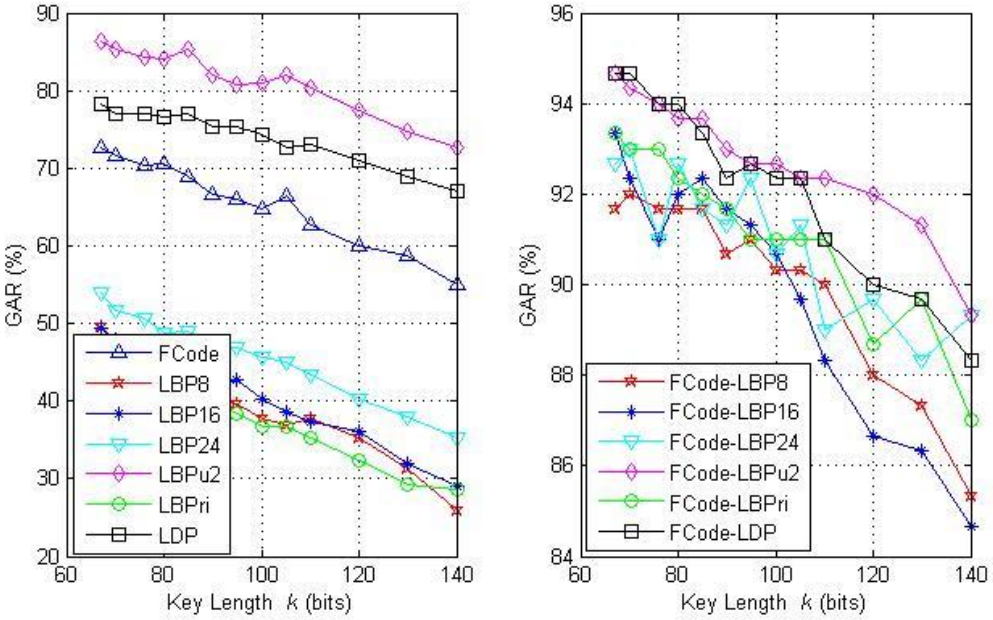
Barmaq izi tekstur əlamətləri istifadə edildikdə blok uzunluğu $n = 511$ olan LDPC kodu üçün FCS sxeminin GAR göstəriciləri şəkil 3.3.14-də göstərilir.



(a) birləşdirmə olmadan (b) birləşdirmə ilə

Şəkil 3.3.13. Təklif edilmiş biometrik kriptosistemin blok uzunluğu n = 255 olan LDPC kodları üçün GAR məhsuldarlığı

Seçilmiş LDPC kodları üçün LBPu2 istisna olmaqla, LBP əlamətləri aşağı GAR göstəricilərinə malik olur. FingerCode-LBPu2 kombinasiyası isə ən yüksək GAR göstəricisinə malik olur. Bu kombinasiya GAR ≈92% səviyyəsində 120 bit açarların yaradılmasına imkan verir. Bu barmaq izi əsasında reallaşdırılmış FCS sxemləri üçün məlum olan ən yaxşı nəticədir.



(a) birləşdirmə olmadan (b) birləşdirmə ilə

Şəkil 3.3.14. Təklif edilmiş biometrik kriptosistemin blok uzunluğu n = 511 olan LDPC kodları üçün GAR məhsuldarlığı

Digər biometrik kriptosistemlərlə məhsuldarlığın müqayisəsi

Barmaq izlərinin tekstur əsasında təsvirləri üçün məlum olan ən yaxşı biometrik kriptosistem [286, s.436]-da təklif edilmişdi. Cədvəl 3.3.2 təklif edilmiş biometrik kriptosistemin məhsuldarlığını [286]-dakı kriptosistemin məhsuldarlığı ilə müqayisə edir.

Cədvəl 3.3.2
Təklif edilmiş kriptosistemin məhsuldarlığının oxşar sistemlə müqayisəsi

BCH(n, k, t)	[286, şəkil 5]		FCode-LBPu2		FCode-LDP		LBPu2-LDP	
	GAR (%)	FAR (%)	GAR (%)	FAR (%)	GAR (%)	FAR (%)	GAR (%)	FAR (%)
(511, 85, 63)	90.1	2.5	90.4	0.0	87.3	0.0	88.0	0.0
(511, 76, 85)	94.6	5.2	95.3	0.0	94.7	0.0	94.1	0.0
(511, 67, 87)	94.8	5.5	95.7	0.0	95.0	0.0	94.7	0.0

Cədvəl 3.3.3 təklif edilmiş biometrik kriptosistemin məhsuldarlığını ədəbiyyatda rast gəlinən digər biometrik kriptosistemlərlə müqayisə edir. Təklif edilmiş biometrik kriptosistem IrisCode əsasında olan kriptosistem istisna olmaqla, digər sistemlərdən açarın uzunluğu, FRR və FAR baxımından üstündür [160, s.1081].

Cədvəl 3.3.3
Təklif edilmiş sistemin digər biometrik kriptosistemlərlə müqayisəsi

Metod	Biometrik əlamət	Açarın uzunluğu (bitlər)	GAR (%)	FAR (%)
Hao et al. [160]	Qüzehli qişa	140	99.53	0.0
Zhou et al. [312]	Sifət	107	99.6	12.0
Maiorana [225]	Əl imzası	29	93.05	6.95
Nandakumar et al.[242]	Barmaq izi	40	99.98	17.5
Arakala et al. [88]	Barmaq izi	34	85.0	15.0
Li et al. [218]	Barmaq izi	50	95.15	0.0
Tuyls et al. [286]	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

Cədvəl 3.3.3-də açarının uzunluğu $k = 76$ olan təklif edilmiş biometrik kriptosistem FingerCode və LBPu2, yaxud FingerCode və LBPri diskretləşdirilmiş barmaq izi tekstur deskriptorlarının birləşdirilməsi əsasında qurulmuşdur və səhvlərin korreksiyası üçün BCH(511, 76, 85) kodu istifadə edilmişdir. Açarının uzunluğu $k = 100$, 120 və 140 olan təklif edilmiş biometrik kriptosistem FingerCode və LBPu2 diskretləşdirilmiş barmaq izi tekstur deskriptorları əsasında LDPC(511, 100),

LDPC(511, 120) və LDPC(511, 140) kodları istifadə edilməklə qurulmuşdur. Qeyd edək ki, FingerCode və LDP diskretləşdirilmiş barmaq izi tekstur deskriptorları da açarının uzunluğu $k = 100$ olan və eyni GAR göstəricisinə malik kriptosistem qurmağa imkan verir (şəkil 3.3.13 b).

III fəsil üzrə nəticələr

- Biometrik sistemlərdə qeydiyyata alınmış və verifikasiyaya təqdim edilmiş biometrik nümunələrin keyfiyyət məlumatlarnın Dempster-Şafer nəzəriyyəsi əsasında aqreqasiyası modeli təklif edilmişdir [176, s.66-74];
- Dəyişdirilmiş barmaq izlərinin aşkarlanması üçün fraktal xarakteristikalar əsasında metod işlənmişdir [47, s.11-16];
- Barmaq izlərinin diskretləşdirilmiş tekstur deskriptorları və səhvlərin korreksiyası kodları əsasında biometrik kriptosistem təklif edilmişdir [185, s.1888-1901].

IV FƏSİL. E-DÖVLƏT MÜHİTİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİNİN İDARƏ EDİLMƏSİ METODLARI

E-dövlətdə İnT insidentlərinin erkən mərhələdə aşkarlanması və onların qısa müddətdə minimal xərclərlə aradan qaldırılması İnT-nin idarə edilməsinin çox vacib aspektidir. Xidmətdən imtina hücumları (Denial of Service, DoS) tez-tez təsadüf edilən İnT insidentlərindən biridir və geniş tədqiq olunmasına baxmayaraq, onun erkən və dəqiq aşkarlanması hələ də problem olaraq qalır [183, s.1-17]. Böyük informasiya sistemlərində hər gün mütəxəssislər tərəfindən qısa zamanda araşdırılması və adekvat cavablandırılması tələb edilən onlarla, bəzən yüzlərlə İnT insidenti qeydə alınır [284]. İnsan resurslarının məhdudluğu və insidentlərin emalı müddətlərinə qoyulan ciddi tələblər insidentlərə bir sıra meyarlar əsasında emal ardıcıllığını müəyyən edən prioritetlərin təyin edilməsini tələb edir [178, s.183]. Yuxarıda qeyd edilən səbəblərdən İnT insidentlərinin real zamanda emalı üzrə işlərin CERT-qrupları arasında optimal paylanması da aktual məsələdir və bu fəsildə insidentlərin emalı proseslərinin çoxmeyarlı optimallaşdırılması üçün də yanaşma təklif edilir [21, s.80].

4.1. Dərin təlim əsasında DDoS hücumların aşkarlanması metodu

DoS hücumları qanuni istifadəçilərin sistemə, şəbəkəyə, tətbiqi proqrama və ya verilənlərə girişinin qarşısını almağa yönəlir. Paylanmış DoS hücumları (DDoS) xidmətdən imtina hücumlarının xüsusi növüdür, İnternet infrastrukturu obyektlərini (marşrutlayıcılar və DNS serverləri daxil olmaqla), buraxma zolağını və serverləri (HTTP və digər xidmətləri) hədəfə alır.

Hazırda DoS hücumları istənilən şəbəkə xidmətinə qarşı reallaşdırmaq olar və bunun üçün xüsusi biliklər tələb edilmir. Belə ki, bu hücumun reallaşdırılmasını münasib qiymətə sifariş etmək və ya bədniyyətlilər tərəfindən hazırlanmış xüsusi alətlərdən istifadə etmək olar. DoS hücumların iqtisadi (rəqiblə mübarizə), siyasi, terrorizm və kibercinayətkarlıq motivləri vardır. DDoS hücumlarını ölkələrə, siyasi partiyalara və sosial hərəkatlara qarşı siyasi məqsədlər üçün istifadə edilməsi faktları vardır [21, s.80]. Kasperski Lab-ın Q3 2017 hesabatına görə, 2017-cü ilin üçüncü

rübündə 98 ölkədə resurslara DDoS hücumları edilib [198]. Hakerlər DDoS hücumları nəhəng sürətə çatdırmaq üçün xüsusi texnologiya və paylanmış infrastrukturdan (botnetlərdən) istifadə edirlər. Bu hətta bir ölkənin bütün informasiya infrastrukturunu İnternetdən təcrid edilməsinə imkan verir.

Bu bölmədə DDoS hücumların real zamanda dəqiq aşkarlanması üçün dərin neyron şəbəkələrinə əsaslanan yanaşma işlənir [183, s.1-17]. Bu məqsədə çatmaq üçün stoxastik neyronlar şəbəkəsinin enerji modelinə əsaslanan öz-özünə öyrənən Məhdud Bolsman Maşını (Restricted Boltzman Machine, RBM) istifadə olunur.

Dərin neyron şəbəkələri - əlaqədar işlərin icmalı

Deep Learning-ə aid edilən çox sayda metodlar var, [124, s.1-29] onları üç qrupa bölür: generativ, diskriminativ və hibrid. Generativ metodlara avtoenkoderləri, rekurrent neyron şəbəkələrini (ing. recurrent neural networks, RNN) və Bolsman maşınlarını (ing. Boltzman Machine, BM) aid edilir.

Avtoenkoderlər – bir gizli layı olan neyron şəbəkəsidir, verilənləri gizli lay vasitəsilə çevirir və çıxış layında onları təkrar almağa çalışır. Avtoenkoderin gizli layında neyronların sayı girişdəkindən az olur. Avtoenkoderlər əlamətlərin çıxarılması və ya ön-treninq üsulu kimi çox faydalıdır. Çoxlaylı şəbəkənin öyrədilməsi üçün avtoenkoderlər stekindən (ing. Stacked Autoencoder, SAE) istifadə edilir. Şəbəkənin hər bir layı əvvəlcə ön-treninq prosedurunu keçərək müstəqil öyrənir. Seçilmiş modeldən asılı olaraq, hər bir lay RBM və ya CNN (Convolutional Neural Network) ola bilər.

BM simmetrik birləşdirilmiş stoxastik binar qovşaqların şəbəkəsidir. Qovşaqlar görünən və gizli vəziyyətləri təsvir etməklə iki qrupa bölünür (gizli Markov modelləri ilə analogiya). Görünən və gizli neyronların vəziyyətləri ehtimal aktivləşdirmə funksiyalarına uyğun olaraq dəyişir.

RBM gizli layının neyronları arasında əlaqələr olmayan BM-dir. Belə xüsusi ikihissəli qraf strukturu sayəsində gizli lay neyronlarının ehtimallarını aşkar şəkildə tapmaq mümkün olur. Əgər gizli layda kafi sayda neyron istifadə edilərsə, RBM istənilən diskret paylanmanı generasiya (təsvir) edə bilər.

RBM dərin inam şəbəkələrinin (ing. Deep Belief Network, DBN) qurulması üçün əsas struktur vahididir. DBN – aşağı layları siqmoid inam şəbəkəsi, yuxarı layı isə RBM olan çoxlaylı şəbəkədir.

Dərin BM (ing. Deep BM, DBM) bəzən ön-treninq mərhələsində avtoenkoder əvəzinə istifadə edilir. RBM-dən əsas fərqi çoxlaylı arxitekturasıdır.

Hibrid arxitektura generativ və diskriminativ arxitekturaları birləşdirir. Hibrid arxitekturaya misal kimi Deep Neural Network (DNN) göstərilə bilər. [124, s.1-29]-ə görə DNN tam əlaqəli gizli layların kaskadıdır və çox zaman ön-treninq mərhələsi kimi RBM stekini istifadə edir.

DDoS hücumların aşkarlanması metodları

İlk irimiqyaslı DDoS hücumları 2000-ci ilin fevralın əvvəlində Yahoo!, eBay, CNN kimi böyük şirkətlərə edilmişdi və həmin vaxtdan DDoS hücumlara qarşı mübarizə mexanizmlərinin işlənməsi praktiklərin və elmi tədqiqatçıların diqqət mərkəzindədir. Həmin vaxtdan bu mövzuda olduqca çox sayda tədqiqat aparılmışdır və DDoS hücumların aşkarlanması üçün təklif edilmiş metodları ilkin yanaşmada, statistik, biliyə (siqnaturaya) əsaslanan, soft kompütinq və maşın təlimi metodlarına bölmək olar [101, s.537, 149, s.125].

Statistik analizin standart metodları və biliyə əsaslanan metodlar əvvəllər məlum olmayan hücumları aşkarlamağa imkan vermir, buna görə bu problemin həll mexanizmi kimi maşın təlimi metodları geniş tətbiq edilir.

Dərin təlim metodları DDoS hücumların aşkarlanması üçün hələlik az tətbiq edilmişdir. [266, s.293]-da hücumların aşkarlanması üçün RBM üzərində qurulmuş DBN (əlamətlərin seçilməsi) və SVM (Support Vector Machine, klassifikasiya üçün) əsasında hibrid üsul təklif edilmişdir. Qeyd edək ki, bu yanaşmada NSL-KDD verilənlər bazasındakı 41 əlamətdən yalnız 5 əlamət istifadə edilmişdir.

[105, s.1-58]-də seyrək avtoenkoder və soft-max reqressiya tipli öz-özünə öyrənmə dərin təlim üsulu tətbiq olunaraq şəbəkə hücumlarının aşkarlanması üsulu təklif edilmişdir.

[219, s.205]-də avtoenkoder və DBN əsasında zərərli proqramların aşkarlanması üsulu təklif olunur. Eksperimentlərin nəticəsi göstərir ki, burada təklif olunan hibrid

metodun aşkarlama dəqiqliyi tək DBN üsulunun nəticəsindən daha üstündür. [224, s.1-23]-də sensor şəbəkələrində müdaxilələrin aşkarlanması üçün spektral klasterləşmə və DNN-in birləşməsi əsasında hibrid yanaşma təklif olunur. Əvvəlcə şəbəkənin əlamətləri klasterlərə bölünür, sonra bu klasterlərə DNN tətbiq olunmaqla daha yaxşı əlamətlər alınır.

Çoxlaylı DBN əsasında DDoS hücumların aşkarlanması üsulu [147, s.247]-də təklif olunur. DBN çox sayda RBM-dən ibarətdir, öyrənmə prosesində RBM əvvəlcədən öyrədilir. Sonra RBM-in öyrədilmiş əlamətləri DBN stekindəki növbəti layın RBM-ni öyrətmək üçün giriş verilənlər kimi istifadə olunur.

[139, s.13]-da yarı-supervizorlu yanaşma əsasında şəbəkə anomaliyasının aşkarlanması üçün diskriminativ RBM aləti istifadə olunur. Burada klassifikator verilənlərin normal profilinə uyğun olaraq öyrədilir, normal profildən böyük kənarlaşma anomaliya kimi modelləşdirilir.

[281, s.258]-də dərin öyrənmənin tətbiqi ilə SDN (Software Defined Networking) mühitində axın əsasında anomaliyanı aşkarlama yanaşması təklif olunur. NSL-KDD verilənlərinin bütün əlamətləri üzrə test etdikdə dərin öyrənmə üsulu J48, Naive Bayes (NB), NB ağacı, Random Forest, Random Tree, Multi-Layer Perceptron, SVM kimi metodlarla müqayisədə çox aşağı nəticə verir, lakin 6 əlamət ilə test edildikdə, Accuracy üzrə 75,75 %-ə bərabər yüksək nəticə əldə edliir.

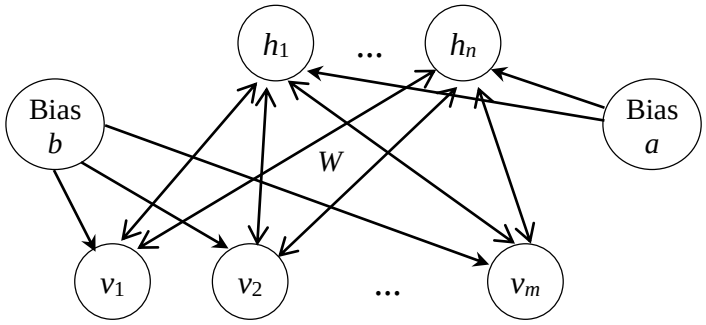
Dərin öyrənmə [304, s.361]-də tətbiq səviyyəsində DDoS hücumların aşkarlanmasında istifadə edilir, əlamətlərin çıxarılması üçün avtoenkoder steki tətbiq olunur. Tətbiq səviyyəsində DDoS hücumları TCP- və IP-səviyyəsindəki DDoS hücumlarına nisbətən aşkarlamaq daha çətindir, çünki onlarda qanuni şəbəkə kompüterlərindən qanuni HTTP sorğuları istifadə edilir.

Məhdud Boltzman Maşını

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 [214, s.536].

Burada bir layın neyronları yalnız digər layın neyronları ilə əlaqələndiyi üçün şəbəkə məhdud adlandırılmışdır. Laylar arasındakı əlaqələr simmetrikdir və ikiistiqamətlidir, bu informasiyanın hər iki istiqamətdə ötürülməsinə imkan verir.

RBM qrafik olaraq şəkil 4.1.1-də təsvir olunur.



Şəkil 4.1.1. Məhdud Bolsman maşını

Şəkil 4.1.1-də m görünən $v_1, \dots, v_m$ layındakı neyronların, n isə gizli $h_1, \dots, h_n$ layındakı neyronların sayıdır. a və b sürüşmə (ing. bias) vektorları, W çəki matrisidir.

RBM enerji tipli modeldir, görünən dəyişənlərlə ehtimal paylanmasını modelləşdirmək üçün gizli dəyişənlər layından istifadə edir [214, s.536]. Görünən elementlər birinci layı təşkil edir və müşahidənin komponentlərinə uyğun gəlir, məsələn, giriş nümunəsinin hər bir əlaməti üçün bir görünən element götürülür. Gizli elementlər müşahidənin komponentləri arasındakı asılılığı, məsələn, əlamətlər arasındakı asılılığı modelləşdirir. Enerji əsaslı model nəzərdə tutur ki, v və h dəyişənləri üzrə ehtimal paylanması entropiya funksiyası ilə müəyyən olunur. Bu funksiya vektor şəklində (4.1.1) və genişləndirilmiş şəkildə (4.1.2) düsturu vasitəsi ilə təyin olunur [214, s.536]:

$$E(v,h) = -h^T W v - a^T v - b^T h \tag{4.1.1}$$

$$E(v,h) = -\sum_{i,j=1}^{m,n} v_i h_j w_{ij} - \sum_{i=1}^{m} a_i v_i - \sum_{j=1}^{n} b_j h_j \tag{4.1.2}$$

Entropiya funksiyasından istifadə etməklə şəbəkənin hər bir neyron cütü üçün bir ehtimal təyin etmək mümkündür. Bu ehtimallardan biri görünən lay, digəri isə gizli lay üçün aşağıdakı ehtimal paylanma verməklə təyin olunur [214, s.536]:

$$p(v,h) = \frac{e^{-E(v,h)}}{\sum_{v,h} e^{-E(v,h)}} \tag{4.1.3}$$

v görünən layın vektorunun ehtimalı gizli layın vektorunun bütün paylanmalarının cəmi şəklində verilir [214, s.536]:

$$p(v) = \frac{\sum_h e^{-E(v,h)}}{\sum_{v,h} e^{-E(v,h)}} \tag{4.1.4}$$

RBM-də eyni layın qonşu neyronları arasında əlaqələr olmadığı üçün burada hadisələr bir-birindən asılı deyil. Bu vəziyyət şərti ehtimalların hesablanmasını asanlaşdırır [214, s.536]:

$$p(h|v) = \prod_j p\big(h_j|v\big), \tag{4.1.5}$$

$$p(v|h) = \prod_i p(v_i|h). \tag{4.1.6}$$

Yuxarıda təsvir edilmiş RBM binar verilənləri olan məsələlərin həlli üçün yaradılmışdır. (4.1.5) və (4.1.6) düsturlarının binar verilənlərin ehtimal paylanması üçün ümumiləşdirilmiş forması aşağıdakı kimidir [214, s.536]:

$$p\big(h_j = 1|v\big) = sigm\big(b_j + \sum_{i=1}^{m} v_i w_{ij}\big), \tag{4.1.7}$$

$$p(v_i = 1|h) = sigm\big(a_i + \sum_{j=1}^{n} h_j w_{ij}\big), \tag{4.1.8}$$

burada: $sigm(x)$ siqmoid funksiyadır.

RBM-in yalnız binar verilənlərə tətbiqi müəyyən problemin həllində onun imkanlarını məhdudlaşdırır. Məsələnin həlli dəqiqliyini artırmaq üçün RBM-in kəsilməz verilənlərə tətbiqinə imkan verən formasından istifadə edirlər. Bu tip RBM-lərdən ən məşhuru Qauss tipli RBM-dir, onun görünən layının ehtimal paylanması Qauss paylanması ilə əvəz edilir. Bu variant Qauss-Bernulli RBM-i adlanır [163, s.504]. Qauss-Bernulli RBM-in ehtimal paylanmaları aşağıdakı kimi təyin olunur:

$$p\big(h_j = 1|v\big) = sigm\left(b_j + \frac{1}{\sigma^2}\sum_{i=1}^{m} v_i w_{ij}\right), \tag{4.1.9}$$

$$p(v_i = 1|h) = N\big(a_i + \sum_{j=1}^{n} h_j w_{ij}, \sigma^2\big). \tag{4.1.10}$$

RBM-in öyrədilməsi. RBM-in öyrədilməsi aşağıda verilmiş mənfi loq-həqiqətəoxşarlığı minimallaşdırmaqdan ibarətdir:

$$\Delta w_{ij} = e\frac{\partial \log p(V)}{\partial w_{ij}} = e\langle v_i h_j\rangle_d - \langle v_i h_j\rangle_m \tag{4.1.11}$$

burada: e öyrənmə sürəti, $\langle\cdot\rangle_d$ və $\langle\cdot\rangle_m$ uyğun olaraq, verilənlərin və modelin riyazi gözləmə qiymətləridir.

Binar verilənlər üçün riyazi gözləmə (4.1.7) və (4.1.8) düsturları ilə, kəsilməz verilənlər üçün isə (4.1.9) və (4.1.10) düsturları ilə tapılır.

Eksperimentlər və müzakirələr

Eksperimentlər üçün üç dərin təlim: Bernulli-Bernulli RBM, Qauss-Bernulli RBM, DBN və üç ənənəvi maşın təlimi arxitekturası SVM (radial basis), SVM (epsilon-SVR) və Decision tree reallaşdırılıb.

DoS hücumların aşkarlanması üçün 7 laydan, 100 gizli neyrondan və 38 görünən neyrondan ibarət RBM istifadə edilmiş və eksperimentlər 5 sinifdən (probe, U2R (User to Root), R2L (Remote to Local), DoS (Denial-of-Service) və normal) ibarət NSL-KDD verilənlər bazasında aparılmışdır.

Laylarda neyronların sayı uyğun olaraq 100, 100, 100, 100, 100, 100, 100 götürülmüşdür. Bazanın verilənləri sütun üzrə [0, 1] intervalı arasında normallaşdırılmışdır. Şəbəkəni öyrətmək üçün 5 epoxa (ing. epochs) istifadə edilmişdir. İstifadə olunan100 gizli neyron üçün çəkilər təsadüfi seçilmişdir. NSL-KDD-Train verilənlərinin 20 faizi şəbəkənin öyrədilməsi üçün, NSL-KDD-Test verilənlərinin 20 faizi şəbəkəni test etmək üçün istifadə edilmişdir. Belə ki, train verilənləri 25194, test verilənləri isə 4508 sətirdən ibarətdir. Eksperimentlər bazanın 38 əlaməti üzərində aparılıb. Modelin aktivləşdirmə funksiyası siqmoiddir.

Eksperimentlərin nəticələrini qiymətləndirmək üçün Accuracy, F-measure, g-mean, Precision, Recall, Sensitivity, Specifisity, TN (True Negative), TP (True Positive), Orta qiymət (ing. Average value) indeksləri istifadə edilmişdir. Cədvəl 4.1.1-də RBM-in nəticələrinin klassik klassifikasiya alqoritmləri ilə müxtəlif metrikalar üzrə müqayisəli analizi təsvir edilmişdir. Cədvəl 4.1.1-dən göründüyü kimi, RBM alqoritminin nəticələri digər alqoritmlərlə müqayisədə daha üstündür. Belə ki, SVM (radial basis) alqoritminin Accuracy göstəricisi 0.7161, SVM (epsilon-SVR) 0.7269, Decision tree 0.6744, RBM alqoritmində isə 0.7323 olmuşdur. Buradan görünür ki, RBM alqoritminin DoS hücumları aşkarlama effektivliyi digər alqoritmlərlə müqayisədə daha üstündür.

Cədvəl 4.1.1.

Metodların effektivliyinin qiymətləndirilməsi

	Accuracy	F-measure	g-mean	Precision	Recall	Sensitivity	Specificity	TN	TP	Orta qiymət
SVM Radial basis	0.7161	0.7400	0.7173	0.6096	0.9416	0.9416	0.5464	0.5464	0.9416	0.7445
SVM (epsilon-SVR)	0.7269	0.7550	0.7251	0.6139	0.9804	0.9804	0.5363	0.5363	0.9804	0.6998
Decision tree	0.6744	0.7190	0.6620	0.5710	0.9705	0.9705	0.4516	0.4516	0.9705	0.7157
RBM	0.7323	0.7530	0.7348	0.6233	0.9509	0.9509	0.5678	0.5678	0.9509	0.7591

Tədqiqatlarda təklif olunan üsulların nəticələrinin əhəmiyyətini qiymətləndirmək üçün statistik testlər aparılmışdır [183, s.1-17]. RBM alqoritmi NSL-KDD bazası üzərində 22 dəfə işə salınmışdır. Üsulun effektivliyi Accuracy, F-measure, g-mean, Precision, Recall, Sensitivity, Specifisity, TN və TP metrikaları əsasında qiymətləndirilmişdir və nəticələr cədvəl 4.1.2, cədvəl 4.1.3 və cədvəl 4.1.4-də verilmişdir.

Cədvəl 4.1.2.

Qauss-Bernulli RBM

İcra sayı	**Accuracy**	**F-measure**	**g-mean**	**Precision**	**Recall**	**Sensitivity**	**Specificity**	**TN**	**TP**	**Orta qiymət**
1	0.7214	0.7478	0.7210	0.6115	0.9623	0.9623	0.5402	0.5402	0.9623	0.7521
3	0.7169	0.7432	0.7169	0.6086	0.9540	0.9540	0.5387	0.5387	0.9540	0.7472
5	0.7229	0.7480	0.7233	0.6135	0.9581	0.9581	0.5461	0.5461	0.9581	0.7527
7	0.7243	0.7481	0.7253	0.6153	0.9540	0.9540	0.5515	0.5515	0.9540	0.7531
9	0.7214	0.7469	0.7216	0.6122	0.9576	0.9576	0.5437	0.5437	0.9576	0.7514
11	0.6939	0.7260	0.6909	0.5895	0.9474	0.9474	0.5052	0.5052	0.9447	0.7278
13	0.6932	0.7260	0.6898	0.5887	0.9468	0.9468	0.5025	0.5025	0.9468	0.8070
15	0.6894	0.7294	0.6803	0.5826	0.9752	0.9752	0.4745	0.4745	0.9752	0.7285
17	0.6901	0.7229	0.6868	0.5866	0.9416	0.9416	0.5010	0.5010	0.9416	0.7237
19	0.7010	0.7333	0.6975	0.5941	0.9576	0.9576	0.5080	0.5080	0.9576	0.7350
21	0.7298	0.7545	0.7302	0.6184	0.9674	0.9674	0.5511	0.5511	0.9674	0.7597
22	**0.7323**	**0.7530**	**0.7348**	**0.6233**	**0.9509**	**0.9509**	**0.5678**	**0.5678**	**0.9509**	**0.7591**

Cədvəl 4.1.3.

Bernulli-Bernulli RBM

İcra sayı	Accuracy	F-measure	G-mean	Precision	Recall	Sensitivity	Specificity	TN	TP	Orta qiymət
1	0.6726	0.7220	0.6552	0.5680	0.9907	0.9907	0.4333	0.4333	0.9907	0.7174
3	0.6610	0.7146	0.6403	0.5595	0.9886	0.9886	0.4147	0.4147	0.9886	0.7078
5	0.6577	0.7105	0.6384	0.5577	0.9783	0.9783	0.4166	0.4166	0.9783	0.7036
6	**0.6828**	**0.7282**	**0.6687**	**0.5759**	**0.9902**	**0.9902**	**0.4516**	**0.4516**	**0.9902**	**0.7255**
7	0.6797	0.7265	0.6644	0.5734	0.9912	0.9912	0.4454	0.4454	0.9912	0.7232
9	0.6488	0.7046	0.6271	0.5514	0.9757	0.9757	0.4030	0.4030	0.9757	0.6961
11	0.6528	0.7068	0.6328	0.5544	0.9747	0.9747	0.4108	0.4108	0.9747	0.6992
13	0.6424	0.7006	0.6185	0.5468	0.9747	0.9747	0.3925	0.3925	0.9747	0.6908
15	0.6431	0.7013	0.6190	0.5472	0.9762	0.9762	0.3925	0.3925	0.9762	0.6916
17	0.6639	0.7175	0.6427	0.5613	0.9943	0.9943	0.4155	0.4155	0.9943	0.7110
19	0.6555	0.7101	0.6342	0.5558	0.9829	0.9829	0.4092	0.4092	0.9829	0.7025
21	0.6520	0.7101	0.6266	0.5526	0.9933	0.9933	0.3953	0.3953	0.9933	0.7013

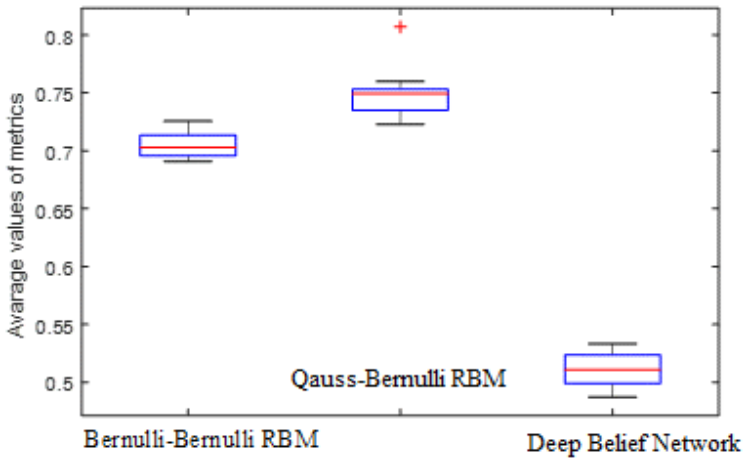
Cədvəl 4.1.4.

Deep Belief Network (DBN)

İcra sayı	Accuracy	F-measure	g-mean	Precision	Recall	Sensitivity	Specificity	TN	TP	Orta qiymət
1	0.4772	0.5552	0.4482	0.4373	0.7602	0.7602	0.2643	0.2643	0.7602	0.5252
3	0.4734	0.5566	0.4390	0.4358	0.7700	0.7700	0.2503	0.2503	0.7700	0.5239
5	0.4343	0.5273	0.3913	0.4111	0.7349	0.7349	0.2083	0.2083	0.7349	0.4873
7	0.4579	0.5403	0.4256	0.4247	0.7421	0.7421	0.2441	0.2441	0.7421	0.5070
9	0.4443	0.5393	0.3976	0.4186	0.7576	0.7576	0.2087	0.2087	0.7576	0.4989
11	0.4729	0.5629	0.4301	0.4370	0.7907	0.7907	0.2340	0.2340	0.7907	0.5270
13	0.4785	0.5511	0.4549	0.4370	0.7457	0.7457	0.2775	0.2775	0.7457	0.5237
15	0.4610	0.5329	0.4389	0.4242	0.7163	0.7163	0.2689	0.2689	0.7163	0.5049
17	0.4627	0.5461	0.4290	0.4284	0.7530	0.7530	0.2445	0.2445	0.7530	0.5127
19	0.4798	0.5677	0.4390	0.4413	0.7959	0.7959	0.2421	0.2421	0.7959	0.5333
21	**0.4809**	**0.5603**	**0.4503**	**0.4402**	**0.7705**	**0.7705**	**0.2631**	**0.2631**	**0.7705**	**0.5299**
22	0.4610	0.5417	0.4303	0.4265	0.7421	0.7421	0.2455	0.2495	0.7421	0.5090

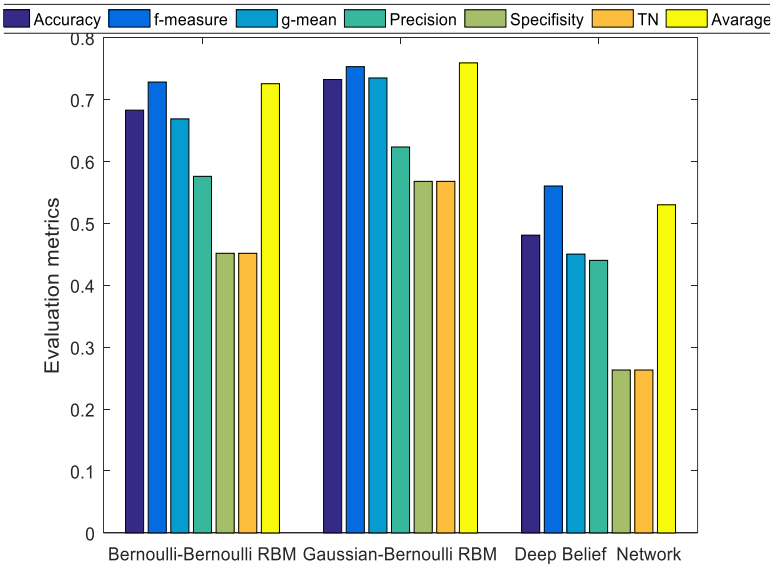
Bernulli-Bernulli RBM, Qauss-Bernulli RBM, Deep Belief Network alqoritmlərinin dayanıqlığını yoxlamaq üçün proqram Matlab mühitində NSL-KDD bazası üzərində 22 dəfə işə salınmışdır və müxtəlif metrikalar üzrə alınmış nəticələrin

orta qiymətləri əsasında boxplot təsvir yaradılmışdır. DoS hücumların aşkarlanması üçün dərin təlim metodlarının müxtəlif metrikaların orta qiymətlərinin boks-plot təsviri şəkil 4.1.2-də verilmişdir.



Şəkil 4.1.2. DoS hücumların aşkarlanması üçün dərin təlim metodlarının müxtəlif metrikalar üzrə orta qiymətlərinin təsviri

Şəkil 4.1.2-dən göründüyü kimi, burada Qauss-Bernulli tipli RBM digər metodlardan üstündür və bu metodun boks-plot təsviri çox sıx olduğu üçün bu metodda kənaraçıxma olduqca azdır. Nəticələrin daha yaxşı nümayiş etdirilməsi üçün şəkil 4.1.3-də metodların müqayisəsi vizual diaqramı verilmişdir. Qeyd edək ki, metodların fərqini daha aydın görmək üçün Recall, Sensitivity və TP rate metrikaları təsvirdən çıxarılmışdır.



Şəkil 4.1.3. Metodların NSL-KDD verilənləri üzərində müqayisəsi

Hər bir alqoritmin 22 dəfə işə salınması nəticəsində alınmış ən pis, orta və ən yaxşı halların qiymətləri cədvəl 4.1.5-də verilmişdir.

Cədvəl 4.1.5.
Dərin təlim metodlarının Accuracy metrikasına görə nəticələri

Metod	Ən pis	Orta	Ən yaxşı
Bernulli-Bernulli RBM	0.6422	0.7255	0.6828
Qauss-Bernulli RBM	0.6894	0.7591	0.7323
Deep Belief Network	0.4343	0.5299	0.4809

Cədvəl 4.1.5-dən göründüyü kimi, Qauss-Bernulli RBM metodunun ən pis halda aldığı qiymət digər metodların ən yaxşı halda aldığı qiymətlərdən daha yaxşıdır.

Dərin neyron şəbəkələri çox böyük sayda parametrləri olan modellərdir və bu parametrlər təlim zamanı tənzimlənməlidir. Bu tip modellərin öyrədilməsi zamanı çox böyük həcmdə verilənlər istifadə olunmalıdır. Lakin burada istifadə olunan NSL-KDD bazası kiçik ölçüyə malikdir. Dərin təlim modelinin böyük iterasiya qiymətləri ilə kiçik ölçülü bazalar üzərində öyrədilməsi şəbəkənin həddindən artıq öyrədilməsi (ing. overfitting) ilə nəticələnir [172, s.5854] və bu modelin effektivliyinin azalmasına səbəb olur. Təqdim olunan işdə bu problemin həlli üçün iterasiyaların sayı az götürülmüşdür.

Qauss-Bernulli tipli RBM-i müxtəlif sayda epoxalarla öyrətdikdə hücumların aşkarlanması dəqiqliyi Cədvəl 4.1.6-da təsvir edilir.

Cədvəl 4.1.6.
Qauss-Bernulli tipli RBM-in effektivliyinin epoxaların sayından asılılığı

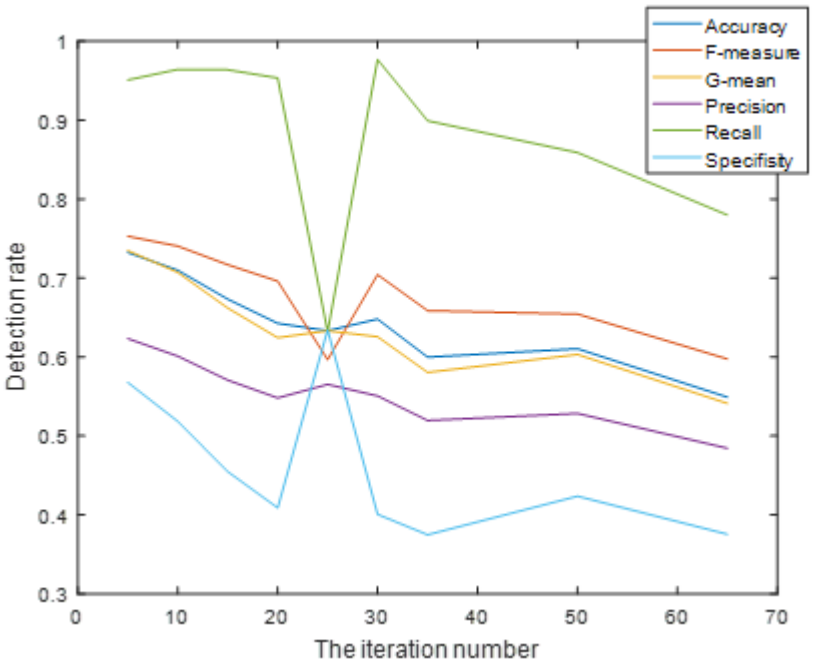
Epoxa sayı	Accuracy	F-measure	g-mean	Precision	Recall	Sensitivity	Specificity	TN rate	TP rate
5	0.7323	0.7530	0.7348	0.6233	0.9509	0.9509	0.5678	0.5678	0.9509
10	0.7098	0.7405	0.7071	0.6010	0.9643	0.9643	0.5185	0.5185	0.9643
15	0.6732	0.7169	0.6620	0.5707	0.9638	0.9638	0.4547	0.4547	0.9638
20	0.6426	0.6961	0.6244	0.5481	0.9535	0.9535	0.4089	0.4089	0.9535
25	0.6333	0.5967	0.6332	0.5652	0.6320	0.6320	0.6343	0.6343	0.6320
30	0.6480	0.7043	0.6256	0.5507	0.9767	0.9767	0.4007	0.4007	0.9767
35	0.5998	0.6586	0.5804	0.5196	0.8992	0.8992	0.3747	0.3747	0.8992
50	0.6105	0.6543	0.6032	0.5285	0.8589	0.8589	0.4236	0.4236	0.8592
65	0.5490	0.5975	0.5411	0.4843	0.7798	0.7798	0.3754	0.3754	0.7798

Cədvəl 4.1.6-nın göstərdiyi kimi, epoxaların sayı artıqca RBM-in DoS hücumu aşkarlaması dəqiqliyi tədricən azalır. Lakin epoxaların sayı 2-dən 5-ə kimi artdıqda RBM-in DoS hücumu aşkarlaması dəqiqliyi tədricən artır (Cədvəl 4.1.7). Lakin 5-dən başlayaraq 65-ə kimi artırdıqda alqoritmin aşkarlama dəqiqliyi get-gedə aşağı düşür. Bu şəkil 4.1.4-də vizual təsvir edilmişdir.

Cədvəl 4.1.7.
Qauss-Bernulli RBM-in öyrənməsinin epoxaların sayından asılılığı

Epoxa sayı	Accuracy	F-measure	g-mean	Precision	Recall	Sensitivity	Specificity	TN	TP
2	0.6939	0.7326	0.6855	0.5860	0.9767	0.9767	0.4812	0.4812	0.9767
3	0.7025	0.7379	0.6964	0.5933	0.9757	0.9757	0.4971	0.4971	0.9757
4	0.7212	0.7445	0.7226	0.6136	0.9463	0.9463	0.5519	0.5519	0.9463
5	0.7323	0.7530	0.7348	0.6233	0.9509	0.9509	0.5678	0.5678	0.9509

Test verilənlərindəki hücumlar dörd kateqoriyaya bölünür: Probe (məsələn, IP sweep, vulnerability scanning), DoS (məsələn, mail bomb, UDP storm), U2R (məsələn, buffer overflow attacks, root kits) və R2L (məsələn, password guessing, soxulcan hücumu).



Şəkil 4.1.4. Epoxaların sayı 5-dən 65-ə artdıqda RBM-in dəqiqlik dinamikası

Bazada U2R və R2L verilənlərinin sayı probe və DoS verilənlərinin sayından az olduğu üçün alqoritmin hücumları aşkarlama effektivliyində hər zaman azalma

müşahidə olunur. Bu vəziyyət alqoritmin U2R və R2L hücumlarını emal edə bilməməsi ilə əlaqələndirilir. Buna görə də tədqiqatçılar hücum növlərini ayrı-ayrı siniflərə görə öyrənməyə çalışırlar.

Aşağıda Probe, DoS, U2R, R2L və normal siniflərdəki nöqtələrin sayı və Qauss-Bernulli RBM metodunun iterasiyaların müxtəlif saylarında bu nöqtələri aşkarlama vəziyyəti verilmişdir (Cədvəl 4.1.8).

Cədvəl 4.1.8.
RBM DoS hücum aşkarlamasının epoxalar əsasında statistikası

Siniflər		**Real nöqtələrin sayı**	**Proqnoz edilən nöqtələrin sayı**						
			5 epoxa	10 epoxa	15 epoxa	20 epoxa	25 epoxa	30 epoxa	35 epoxa
Normal	1	1935	2908	2780	2885	3009	1356	3227	2874
DoS	2	1526	1077	1555	844	895	1323	918	1027
U2R	3	46	0	0	0	0	0	0	0
R2L	4	513	0	0	429	520	1638	228	594
Probe	5	488	523	173	350	84	191	135	13
Cəmi		4508	4508	4508	4508	4508	4508	4508	4508

Qauss-Bernulli RBM metodunda iterasiyaların sayını artırdıqca R2L sinfindən nöqtələr aşkarlanır, lakin bu zaman metodun aşkarlama dəqiqliyi aşağı düşür. Bu onunla əlaqədardır ki, burada yalnış aşkarlanmaya çox yol verilir. Aparılan eksperimentlərdə Probe, DoS və normal nöqtələr yüksək dəqiqliklə aşkarlanır, lakin digər U2R və R2L hücumları müqayisədə daha pis nəticələr verir. Qeyd edək ki, U2R və R2L sinifləri verilənlərin arasında daha az təsadüf edilir, buna görə aşkarlanma dəqiqliyinin aşağı olması gözləniləndir.

4.2. İnformasiya təhlükəsizliyi insidentlərinin çoxmeyarlı dinamik prioritetləşdirilməsi metodu

Proqram təminatının mürəkkəbliyinin artması, kompüter şəbəkələrinin qarşılıqlı əlaqələrinin və qarşılıqlı asılılıqlarının güclənməsi ilə İnT boşluqlarının sayı sürətlə artır və bədniyyətlilər bu situasiyadan yararlanmaq fürsətini əldən qaçırmırlar. Nəticədə İnT insidentləri qaçılmaz olur və təşkilatların əksəriyyəti İnT insidentlərinin qarşısının alınması, erkən aşkarlanması və cavablandırılması problemləri ilə

qarşılaşırlar [8, s.51]. Hələ ilk İnT insidentinin emalı təcrübəsi göstərdi ki, belə insidentlərin cavablandırılması üçün xüsusi komandaların yaradılması zəruridir [298, s. 9-58]. Adətən, bu komandaları CERT-komandaları adlandırırlar.

CERT-in əsas problemlərindən biri artan iş yükünü məhdud insan resursları ilə balanslaşdırmaqdır [8, s.51]. Hər bir insidentin vaxtında aradan qaldırılması üçün müəyyən insan resursları və texniki vasitələr tələb edilir. Müasir informasiya sistemlərində hər gün onlarla, bəzən yüzlərlə İnT insidenti baş verir. CERT-in resursları məhdud olduğundan bir neçə İnT insidentinin eyni vaxtda emalı tələb edildikdə insidentlərin prioritetlərini müəyyən etmək və məhdud CERT resurslarını bu insidentlər arasında bölüşdürmək məsələsi qarşıya çıxır. Hər bir insidentə prioritet mənimsədilir və insidentin emalı ona uyğun aparılır. Prioritet insidentin emal növbəsini və reaksiya vaxtının standart normasını təyin edir [284, s.42].

Böyük sistemlərdə gün ərzində aşkarlanmış yüzlərlə İnT insidentinin vacibliyinin və təcililiyinin insan tərəfindən müəyyən edilməsi çətindir, çox vaxt tələb edir və səhvlərə meyillidir. Buna görə insidentlərin avtomatlaşdırılmış emalı üsulları, o cümlədən insidentlərin prioritetləşdirilməsi metodları tələb edilir [178, s.183].

Əlaqədar işlərin icmalı. Müxtəlif CERT komandaları insidentləri prioritetləşdirmək üçün çeşidli yanaşmalar istifadə edirlər. Lakin insidentlərə prioritet təyin edilməsinin ən yaxşı üsulu haqqında konsensus yoxdur. Müəlliflərin bir çoxu insidentləri prioritetləşdirmək üçün Kateqoriya 1, 2, 3 və ya Yüksək, Orta, Aşağı kimi sadə ranqlaşdırmadan istifadə edirlər.

Bəzi hallarda prioritet şkalası kimi digər faktorlarla müqayisədə kritiklik səviyyəsinin tərsi istifadə edilir. Maraqlı tərəflərin çox olduğu şəraitdə insidentlər bir istifadəçi qrupuna deyil, bir neçə qrupa təsir edə bilər. Əgər nisbi prioritetlər hamı tərəfindən başa düşülməzsə, onda cəhd edilən cavab hərəkətləri bu fəaliyyətin yekun uğuruna ciddi mənfi təsir edə bilər [178, s.183].

İnsidentlərin idarə edilməsinə ITIL yanaşmasında [189, s. 278-283] prioritet insidentin təcililiyi (insidentin nə qədər tez aradan qaldırılması tələb edilir) və

insidentin təsir səviyyəsi əsasında müəyyən edilir. ITIL metodikasında bu elementlərdən insidentin prioritet səviyyəsini hesablamaq üçün cədvəl 4.2.1-dən istifadə edilir.

ITIL metodunda prioritet 1-dən 5-ə tam qiymətlər alır; ən yüksək prioritet 1-dir. Prioritet qiymətləri Critical, High, Moderate, Low və Planning kimi interpretasiya edilir və insidentin emalı müddətləri uyğun olaraq 1 saat, 8 saat, 24 saat, 48 saat və "plan üzrə" olaraq müəyyən edilir.

Cədvəl 4.2.1.
Prioritetin təyin edilməsi üçün ITIL metodu

	Təsir			
Təcililik		Yüksək	Orta	Aşağı
	Yüksək	1	2	3
	Orta	2	3	4
	Aşağı	3	4	5

İnsidentlərin prioritetləşdirilməsi üçün riskin qiymətləndirilməsinə və AHP metoduna əsaslanan RIM modeli (Risk Index Model) [87, s.25]-da təklif edilir. Modeldə insidentlərin risk indeksini hesablamaq üçün qərar qəbuletmə faktorları olaraq kritiklik, "təmirə" yararlılıq, əvəzlənə bilmə və asılılıq indikatorları istifadə edilir.

İnsidentlər relevant faktorlar əsasında prioritetləşdirilməlidir. Ənənəvi prioritetləşdirmə metodları daha çox insidentin təsiri və təciliyi ilə maraqlanır, maliyyə itkilərini və riskləri nəzərə almırlar. [292, s.536]-də təklif edilən yanaşmada insidentlər biznes itkilərinin cəmi və risklər minimallaşdırılmaqla prioritetləşdirilir.

İnsidentlərin prioritetləşdirilməsi metodlarının yuxarıda göstərilən nöqsanları ilə yanaşı, qeyd edilməlidir ki, mövcud metodlar müxtəlif qərar qəbuletmə faktorlarına vacibliklərı əsasında çəki verilməsi məsələsinə baxmırlar. Faktorlar üçün müxtəlif çəkilərin istifadə edilməsi qərar qəbul edən şəxslərin insidentlərin prioritetləşdirilməsinə fərqli münasibətlərini, seçimlərini göstərməyə imkan verir.

İnsidentlərin prioritetləşdirilməsinə çoxkriteriyalı qərar qəbulu məsələsi kimi baxmaq və çoxkriteriyalı qərar qəbulu metodu kimi AHP-dən insident faktorlarının

vaciblik çəkilərini tapmaq üçün istifadə etmək olar. AHP metodu bir çox qərar qəbuletmə sahələrində uğurla tətbiq edilib [264, s.9]. AHP methodu cüt-cüt müqayisələr vasitəsilə müxtəlif çəkilər verməyə imkan verir və prioritet şkalasını almaq üçün ekspertlərin rəyinə arxalanır.

Klassik AHP yanaşmasında məqsədə nəzərən hər bir faktor üçün cüt-cüt müqayisələr 9-ballıq şkala istifadə edilməklə yerinə yetirilir. Cüt-cüt müqayisə nisbətləri adi həqiqi ədədlərlə ifadə edilir. İnsident faktorlarında həmişə qeyri-müəyyənlik olur, buna görə insident faktorlarının təsviri, adətən, linqvistik və qeyri-səlisdir [310, s.338]. Bundan başqa, məlumdur ki, keyfiyyət atributlarının insan tərəfindən qiymətləndirilməsi həmişə subyektiv və qeyri-dəqiqdir. Buna görə, klassik AHP-nin insident faktorlarının atributlarını adekvat əks etdirməsi və bu faktorların vaciblik çəkilərini dəqiq müəyyən etməsi çətindir. Bu baxımdan qeyri-səlis AHP metodunun qərar qəbuletmə proseslərini daha dəqiq təsvir etdiyini nəzərə alaraq, burada insident prioritetlərinin təyin edilməsi üçün qeyri-səlis AHP yanaşması istifadə edilir.

Qeyri-səlis ədədlər. Praktiki tətbiqlərdə çox zaman üçbucaq qeyri-səlis ədədlərlə işləməyə üstünlük verirlər, bunun səbəbi hesablamaların sadəliyi və onların qeyri-səlis mühitdə informasiyanın təsviri və işlənməsi üçün yararlı olmalarıdır [102, s. 1-9].

Qeyri-səlis M ədədinin $\mu_M(x): R \to [0,1]$ mənsubiyyət funksiyası aşağıdakı şəkildə olarsa, ona üçbucaqşəkilli qeyri-səlis ədəd (ÜQƏ) deyilir [102, s. 22]:

$$\mu_M(x) = \begin{cases} (x-l)/(m-l), l \le x \le m, \\ (u-x)/(u-m), m \le x \le u, \\ 0, \text{əks halda.} \end{cases} \quad (4.2.1$$

burada: $l \le m \le u$ – həqiqi ədədlərdir. ÜQƏ (l, m, u) üçlüyü ilə göstərilir.

ÜQƏ-lər üzərində müxtəlif əməllər müəyyən edilir. Əgər $M_1 = (l_1, m_1, u_1)$ və $M_2 = (l_2, m_2, u_2)$ iki müsbət ÜQƏ olarsa, onda [102, s. 22-23]:

$$\begin{aligned} &\text{Toplama: } M_1 \oplus M_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2); \\ &\text{Vurma: } M_1 \otimes M_2 = (l_1 l_2, m_1 m_2, u_1 u_2); \end{aligned} \quad (4.2.2)$$

Tərs qiymət: $M_1^{-1} \approx (1/u_1\,, 1/m_1\,, 1/l_1)$.

İnsidentlərin prioritetləşdirilməsi faktorlarının iyerarxiyası

Tipik qeyri-səlis AHP qərar qəbulu problemi aşağıdakılardan ibarətdir: (1) M_i (i = 1, 2,…, m) alternativlər çoxluğu, (2) C_j (j = 1, 2, …, n) qiymətləndirmə kriteriyaları çoxluğu, (3) r_{ij} hər bir kriteriya cütünün nisbi vacibliyini təsvir edən linqvistik mühakimə və (4) $w = (w_1, w_2, ..., w_n)$ çəki vektoru.

Təklif edilən modelin ilk addımı bütün vacib kriteriyaları və onların qərar qəbuletmə problemi ilə onların münasibətini iyerarxiya formasında müəyyən etməkdir. Bu iyerarxiya müxtəlif səviyyələrdə strukturlaşdırılır: yuxarıdan (yəni məqsəddən) orta səviyyələr vasitəsilə (sonrakı səviyyələrin asılı olduğu kriteriyalar və altkriteriyalar) ən aşağı səviyyəyə (yəni alternativlərə).

Prioritet insidentin müxtəlif faktorları nəzərə alınmaqla müəyyən edilir. AHP metodunu İnT insidentlərinin prioritetləşdirilməsi üçün tətbiq etmək üçün insidentin prioritetləşdirilməsi faktorlarının strukturlaşdırılmış iyerarxiyasını qurmaq lazımdır.

İnsidentin prioriteti insident atributlarına, sistem atributlarına, təşkilatın atributlarına, boşluqların atributlarına və servis xidməti razılaşmalarına əsaslanmalıdır. İnsidentlərin faktorlarını identifikasiya etmək üçün bu sahədəki ədəbiyyatın qısa icmalı aparılmışdır. NIST insidentləri aşağıdakı faktorların əsasında prioritetləşdirməyi tövsiyə edir [112, s.50]:

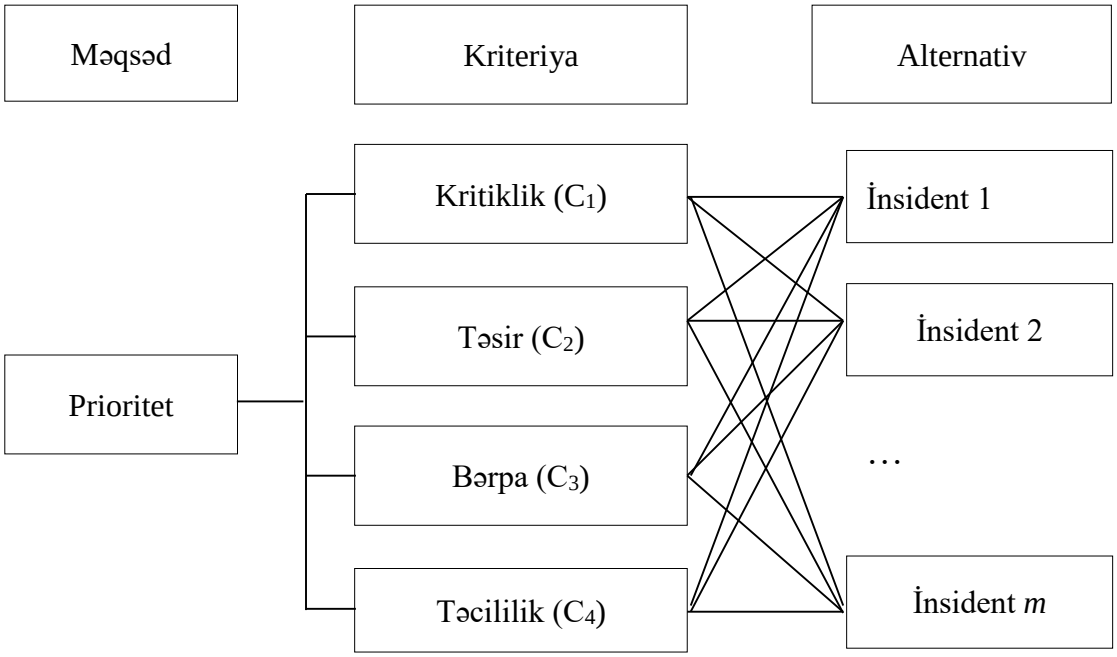
- insidentin funksional təsiri (məsələn, biznes funksiyalara cari və ehtimal edilən gələcək mənfi təsiri);
- insidentin informasiya təsiri (məsələn, təşkilatın informasiyasının konfidensiallığına, tamlığına və əlyetərliyinə təsiri);
- insidentin nəticələrinin aradan qaldırılması (məsələn, insidentin nəticələrini aradan qaldırmaq üçün tələb edilən müddət və resursların növü).

İnsidentlərin prioritetləşdirilməsi üçün [21, s.80]-də aşağıdakı kriteriyalar təklif edilir:

- insidentin emalında tələb edilən resurslar;
- istifadəçilərə təsiri;

– insidentin növü;
– ziyanın növü və miqyası;
– hücumun mənbəyi və ya hədəfi.

Yuxarıda sadalanmış kriteriyalar əsasında biz insidentin prioritetləşdirilməsi faktorların aşağıdakı iyerarxik strukturunu təklif edirik (şəkil 4.2.1).



Şəkil 4.2.1. İnsidentlərin prioritetləşdirilməsi faktorlarının iyerarxiyası

Kritiklik: insidentə cəlb olunmuş informasiya aktivlərinin kritikliyi ilə müəyyən olunur (məsələn, tətbiqi proqramlar və infrastruktur).

Təsir: servisin normal səviyyəsindən (xidmət səviyyəsi müqaviləsindəki parametrlərdən – Service Level Agreement, SLA) uzaqlaşma dərəcəsi; insidentin təsir etdiyi istifadəçilərin sayı və biznes proseslərin sayı ilə ifadə olunur;

Bərpa: insident sonrası bərpa üçün tələb edilən insan və texniki resursları təsvir edir.

Təcililik: istifadəçi və ya biznes proses üçün insidentin cavablandırılmasında yolverilən gecikmə.

Qeyd edilməlidir ki, insidentin prioriteti dinamik ola bilər – əgər şərait dəyişirsə və ya insident SLA-da nəzərdə tutulmuş müddətdə aradan qaldırılmayıbsa, onda situasiyanı əks etdirmək üçün prioritet dəyişməlidir.

İyerarxiya müəyyən edildikdən sonra cüt-cüt müqayisə yerinə yetirilir. İyerarxiyanın eyni səviyyəsində yerləşən bütün kriteriyalar əvvəlik (yuxarı)

səviyyənin hər bir kriteriyası ilə müqayisə edilir. Cüt-cüt müqayisə linqvistik termlər istifadə edilməklə aparılır. Qeyri-səlis müqayisə matrisinin qurulması üçün 0-9 şkalasında beş linqvistik term – "Ən az Vaciblik", "Az Vaciblik", "Orta Vaciblik", "Yüksək Vaciblik" və "Fövqəladə Vaciblik" istifadə edilir. Bu beş linqvistik dəyişən cədvəl 4.2.2-da göstərildiyi kimi qeyri-səlis ədədlərlə təsvir olunur.

Cədvəl 4.2.2.
Qeyri-səlis Vaciblik şkalası

Linqvistik dəyişən	**İzahı**	**Qeyri-səlis ədəd**
Ən az Vaciblik	Kriteriya digərindən əhəmiyyətli geridə qalır	(1, 1, 1)
Az Vaciblik	Kriteriya digərindən bir az geridədir	(2, 3, 4)
Bərabər Vaciblik	İki kriteriyanın obyektə töhfəsi bərabərdir	(4, 5, 6)
Yüksək Vaciblik	Kriteriya digərindən bir az üstündür	(6, 7, 8)
Fövqəladə Vaciblik	Kriteriya digərindən əhəmiyyətli üstündür	(9, 9, 9)
	İki qonşu mühakimə arasında aralıq qiymətlər	(1, 2, 3), (3, 4, 5), (5, 6, 7) və (7, 8, 9)

Fərz edək ki, hər bir ekspert (D_p) cüt-cüt müqayisəni (4.2.3)-də göstərildiyi kimi fərdi yerinə yetirir:

$$D_p = \begin{bmatrix} b_{11}^p & b_{12}^p & \cdots & b_{1m}^p \\ b_{21}^p & b_{22}^p & \cdots & b_{2m}^p \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1}^p & b_{m2}^p & \cdots & b_{mm}^p \end{bmatrix} \tag{4.2.3}$$

Sonra ekspertlərin qiymətləri (4.2.4) düsturu ilə birləşdirilərək yekun cüt-cüt müqayisə matrisi qurulur. Bu yolla cüt-cüt müqayisə qiymətləri qeyri-səlis üçbucaq ədədlərə çevrilir:

$$l_{ij} = \min_p b_{ij}^p \,;\; m_{ij} = \frac{\sum_{p=1}^{t} b_{ij}^p}{p} ;\; u_{ij} = \max_p b_{ij}^p,$$
$$p = 1,2,\dots,t;\; i = 1,2,\dots,m;\; j = 1,2,\dots m, \tag{4.2.4}$$
$$\tilde{b}_{ij} = \left(l_{ij}, m_{ij}, u_{ij}\right), i = 1,2,\dots,m;\; j = 1,2,\dots m.$$

Qeyri-səlis analitik iyerarxiya prosesi

Ədəbiyyatda bir çox qeyri-səlis AHP metoduna təsadüf olunur. Bu işdə genişlənmiş qeyri-səlis AHP istifadə edilir [106, s.649].

Tutaq ki, $X = \{x_1, x_2, ..., x_m\}$ obyektlər çoxluğu və $G = \{g_1, g_2, ..., g_n\}$ məqsədlər çoxluğudur. Chang genişlənmə analizinə uyğun olaraq [106, s.649], hər bir obyekt götürülür və hər bir g_i məqsədi üçün genişlənmə analizi yerinə yetirilir. Deməli, m hər bir obyekt üçün aşağıdakı kimi işarə olunan genişlənmə analizi qiymətləri alına bilər:

$$M_{g_i}^1, M_{g_i}^2, \dots, M_{g_i}^m, i = 1, \dots, n, \tag{4.2.5}$$

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

Addım 1. i-ci obyektə nəzərən qeyri-səlis sintetik ölçü aşağıdakı kimi təyin olunur:

$$S_i = \sum_{j=1}^{m} M_{g_i}^j \otimes \left[\sum_{i=1}^{n} \sum_{j=1}^{m} M_{g_i}^j\right]^{-1}. \tag{4.2.6}$$

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:

$$(M_2 \geq M_1) = \begin{cases} 1, \text{əgər } m_2 \geq m_1 \\ 0, \text{əgər } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, \text{əks halda} \end{cases} \tag{4.2.7}$$

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:

$$\begin{gathered} V(M \geq M_1, M_2, \dots, M_k) = \\ = V[(M \geq M_1) \; and \; (M \geq M_2) \dots and \; (M \geq M_k)] = \\ = \min V(M \geq M_i), i = 1,2, \dots, k. \end{gathered} \tag{4.2.8}$$

Fərz edək ki,

$$d(A_i) = \min V(S_i \geq S_k), k = 1,2, \dots, n; k \neq i. \tag{4.2.9}$$

Onda çəki vektoru

$$W' = (d'(A_1), d'(A_2), \dots, d'(A_n))^T, \tag{4.2.10}$$

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

Addım 4. Normallaşdırılmış çəki vektorları hesablanır:

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T, \qquad (4.2.11)$$

burada: W qeyri-səlis olmayan (həqiqi) ədədlərin vektorudur.

Eksperimental tədqiqat və müzakirə. Fərz edək ki, dörd kriteriya üçün üç ekspertin cüt-cüt müqayisələri aşağıdakı kimidir:

$$D_1 = \begin{array}{c} \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & C_4 \end{array} \\ \begin{bmatrix} 1 & 3 & 5 & 1/3 \\ 1/3 & 1 & 5 & 1 \\ 1/5 & 1/5 & 1 & 3 \\ 3 & 1 & 1/3 & 1 \end{bmatrix} \end{array}, \quad D_2 = \begin{array}{c} \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & C_4 \end{array} \\ \begin{bmatrix} 1 & 5 & 5 & 3 \\ 1/5 & 1 & 5 & 3 \\ 1/5 & 1/5 & 1 & 3 \\ 1/3 & 1/3 & 1/3 & 1 \end{bmatrix} \end{array}, \quad D_3 = \begin{array}{c} \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & C_4 \end{array} \\ \begin{bmatrix} 1 & 3 & 1/3 & 5 \\ 1/3 & 1 & 7 & 3 \\ 3 & 1/7 & 1 & 7 \\ 1/5 & 1/3 & 1/7 & 1 \end{bmatrix} \end{array}$$

(4.2.4) düsturu ilə cədvəl 4.2.3-də göstərilən cüt-cüt müqayisə matrisi qurulur.

Cədvəl 4.2.3.
Məqsədə nəzərən qeyri-səlis qiymətləndirmə matrisi

	C_1	C_2	C_3	C_4
C_1	(1, 1, 1)	(3, 3.67, 5)	(0.33, 3.44, 5)	(0.33, 2.78, 5)
C_2	(0.2, 0.29, 0.33)	(1, 1, 1)	(5, 5.67, 7)	(3, 3.67, 7)
C_3	(0.2, 1.33, 3)	(0.14, 0.18, 0.2)	(1, 1, 1)	(3, 4.33, 7)
C_4	(0.2, 1.18, 3)	(0.33, 0.55, 1)	(0.14,0.27,0.33)	(1, 1, 1)

Cədvəl 4.2.3-dən genişlənmə analizinə uyğun olaraq əsas məqsədə nəzərən qiymət (4.2.5) düsturu ilə hesablanır:

$$S_{C_1} = (4.66, 10.89, 16.0) \otimes \left(\frac{1}{47.86}, \frac{1}{31.36}, \frac{1}{19.87}\right) = (0.097, 0.347, 0.805).$$

$$S_{C_2} = (9.2, 10.63, 15.33) \otimes \left(\frac{1}{47.86}, \frac{1}{31.36}, \frac{1}{19.87}\right) = (0.19, 0.34, 0.77).$$

$$S_{C_3} = (4.34, 6.84, 11.2) \otimes \left(\frac{1}{47.86}, \frac{1}{31.36}, \frac{1}{19.87}\right) = (0.091, 0.218, 0.564).$$

$$S_{C_4} = (1.67, 3.0, 5.33) \otimes \left(\frac{1}{47.86}, \frac{1}{31.36}, \frac{1}{19.87}\right) = (0.035, 0.096, 0.268).$$

Bu qeyri-səlis qiymətlər (4.2.6) düsturu istifadə edilməklə müqayisə olunur və aşağıdakı qiymətlər alınır:

$V(S_{C_1} \geq S_{C_2}) = 1;$ $V(S_{C_1} \geq S_{C_3}) = 1;$ $V(S_{C_1} \geq S_{C_4}) = 1.$
$V(S_{C_2} \geq S_{C_1}) = 0.99;$ $V(S_{C_2} \geq S_{C_3}) = 1;$ $V(S_{C_2} \geq S_{C_4}) = 1.$
$V(S_{C_3} \geq S_{C_1}) = 0.784;$ $V(S_{C_3} \geq S_{C_2}) = 0.754;$ $V(S_{C_3} \geq S_{C_4}) = 1.$

$V\left(S_{C_4} \geq S_{C_1}\right) = 0.404;\ \ V\left(S_{C_4} \geq S_{C_2}\right) = 0.241;\ \ V\left(S_{C_4} \geq S_{C_3}\right) = 0.59.$

Sonra (4.2.8) istifadə edilməklə prioritet çəkiləri hesablanır:

$d(C_1) = \min\left(1.0,\ 1.0,\ 1.0\right) = 1.0;$

$d(C_2) = \min\left(0.99,\ 1.0,\ 1.0\right) = 0.99;$

$d(C_3) = \min(0.784,\ 0.754,\ 1) = 0.754;$

$d(C_4) = \min(0.404,\ 0.241,\ 0.59) = 0.241.$

Prioritet çəkiləri $W = (1.0,\ 0.99,\ 0.754,\ 0.241)$ vektorunu əmələ gətirir. Bu qiymətlərin normallaşdırılmasından sonra əsas məqsədə nəzərən prioritet çəkisi $(0.335,\ 0.332,\ 0.252,\ 0.081)$ kimi hesablanır.

Növbəti mərhələdə insidentlərin prioritet çəkilərinin hesablanması nümayiş etdiriləcək. Fərz edək ki, aşağıdakı üç insident eyni vaxtda aşkarlanıb:

- *İnsident* 1 – "güclü" virus və e-poçt spamı nəticəsində VIP statuslu bir neçə istifadəçi təsirə məruz qalıb;
- *İnsident* 2 – təşkilatın veb-saytı difeys (ing. deface) edilib;
- *İnsident* 3 – hakinq nəticəsində xarici İnternet marşrutlayıcısı imtina edir.

Bu üç insidentin ekspertlər tərəfindən cüt-cüt müqayisəsi nəticəsində cədvəl 4.2.4-4.2.7-də qiymətləndirmə matrisləri formalaşdırılır. Sonra hər bir kriteriya üçün insidentlərin prioritet çəkiləri hesablanır, nəticələr cədvəl 4.2.8-də göstərilib.

Cədvəl 4.2.4.

C_1 kriteriyasına görə qeyri səlis qiymətləndirmə matrisi

Kriteriya C_1	İnsident 1	İnsident 2	İnsident 3
İnsident 1	(1, 1, 1)	(0.2, 0.29, 0.33)	(0.33, 0.56, 1)
İnsident 2	(3, 3.67, 5)	(1, 1, 1)	(0.2, 2.06, 3)
İnsident 3	(1, 2.33, 3)	(1, 1, 1)	(0.33, 1.67, 5)

Cədvəl 4.2.5.

C_2 kriteriyasına görə qeyri-səlis qiymətləndirmə matrisi

Kriteriya C_2	İnsident 1	İnsident 2	İnsident 3
İnsident 1	(1, 1, 1)	(0.2, 0.24, 0.33)	(0.14, 0.27, 0.33)
İnsident 2	(3, 4.33, 5)	(1, 1, 1)	(3, 3.67, 5)
İnsident 3	(3, 4.33, 7)	(0.2, 0.29, 0.33)	(1, 1, 1)

Cədvəl 4.2.6.
C_3 kriteriyasına görə qeyri-səlis qiymətləndirmə matrisi

Kriteriya C_3	İnsident 1	İnsident 2	İnsident 3
İnsident 1	(1, 1, 1)	(3, 3.67, 5)	(0.33, 2.78, 5)
İnsident 2	(0.2, 0.29, 0.33)	(1, 1, 1)	(0.2, 0.47, 1)
İnsident 3	(0.2, 1.18, 3)	(1, 3.67, 5)	(1, 1, 1)

Cədvəl 4.2.7.
C_4 kriteriyasına görə qeyri-səlis qiymətləndirmə matrisi

Kriteriya C_4	İnsident 1	İnsident 2	İnsident 3
İnsident 1	(1, 1, 1)	(0.33, 2,78, 5)	(3, 3, 3)
İnsident 2	(0.2, 1.18, 3)	(1, 1, 1)	(0.33, 2.78, 5)
İnsident 3	(0.33, 0.33, 0.33)	(0.2, 1.18, 3)	(1, 1, 1)

Cədvəl 4.2.8.
İnsidentlərin kriteriyalar üzrə prioritet çəkiləri

	Kriteriya C_1	Kriteriya C_2	Kriteriya C_3	Kriteriya C_4	İnsidentin prioritet çəkisi
Çəki	0.335	0.332	0.252	0.081	
İnsidentlər					
İnsident 1	0.03	0.0	0.47	0.41	0.162
İnsident 2	0.52	0.62	0.10	0.36	0.434
İnsident 3	0.45	0.38	0.43	0.23	0.404

Cədvəl 4.2.8-ə uyğun olaraq *Kritiklik*, *Təsir*, *Bərpa* və *Təcililik* kriteriyalarının çəki vektorları uyğun olaraq aşağıdakı kimi hesablanır:

(0.03, 0.52, 0.45); (0.0, 0.62, 0.38); (0.47, 0.10, 0.43) və (0.41, 0.36, 0.23).

Beləliklə, təklif edilmiş metod ilə insidentlərin prioritet sırası belədir: *İnsident* 2> *İnsident* 3 > *İnsident* 1.

İnT insidentlərinin prioritetlərinin müəyyən edilməsi onların cavablandırılması prosesində çox vacib qərar mərhələsidir. Prioritet müəyyən edildikdən sonra insident emal prosesini gözləyən insidentlərin növbəsinə daxil edilir və insidentlərin emalı üzrə əməliyyatların optimal planlaşdırılması həyata keçirilir.

4.3. İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərinin optimal planlaşdırılması metodu

Fərz olunur ki, CERT xidmətləri göstərən provayderə bir neçə İnT insidentini emal etmək sifarişi daxil olub. İnsidentlər müxtəlif təşkilatlardan (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. Qeyd edək ki, CERT-qrupu bir nəfərdən də ibarət ola bilər. Aşağıdakı məhdudiyyətlər nəzərə alına bilər:

- İnsidentin emalı (cavablandırılması) bir neçə prosedurdan ibarətdir;
- Prosedurların yerinə yetirilməsi ardıcıllığı var, bəzi prosedurlara yalnız ondan əvvəl gələn bütün prosedurlar emal edil dikdən sonra başlamaq olar;
- Hər bir proseduru yalnız bir CERT-qrupu yerinə yetirə bilər;
- CERT-qrupu eyni vaxtda bir neçə emal prosedurunu yerinə yetirə bilməz;
- Bir insidentin emalı üzrə bəzi prosedurları eyni vaxtda yerinə yetirmək olar;
- CERT- qrupu bir insidentin emalından digərinin emalına keçdikdə müəyyən xərclər tələb edilə bilər (bir coğrafi məkandan digərinə yerdəyişmə);
- İnsidentin emalının son müddətinə məhdudiyyət qoyula bilər.
- Hər bir CERT-qrupu istənilən insident prosedurunu yerinə yetirə bilər.

Qeyd edək ki, CERT praktikasında geniş isifadə olunan aşağıdakı prosedurları fərqləndirmək olar: insident barədə sübutların toplanması və emalı; insidentin lokallaşdırılması; insidentin aradan qaldırılması; insidentdən sonra bərpa və insident barədə hesabatın hazırlanması.

Məsələnin həlli üçün optimallaşdırma modeli

Tutaq ki, $J_1, J_2, \ldots, J_n$ insidentlər çoxluğu $R_1, R_2, \ldots, R_m$ 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: $O_{1j} \rightarrow O_{2j} \rightarrow$

$\cdots \rightarrow O_{n_i,j}, i = 1, \ldots, n$. 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 proseduru yalnız bir CERT-qrupu emal edə bilər. Əgər j-cu prosedur CERT-qrupu R_k tərəfindən yerinə yetirilirsə, onun emal müddəti t_{jk}-dır. R_k CERT-qrupu $[s_k^v, l_k^v], v = 1, \ldots, V_k$ kəsişməyən zaman intervalları ərzində əlyetər (boş) olur, burada $l_k^v \leq s_k^{v+1}, v = 1, \ldots, V_k - 1$. Bundan əlavə, R_k-in toplam iş vaxtı aşağıdan H_k^- və yuxarıdan isə H_k^+ ilə məhdudlaşdırmaq olar, burada $H_k^- \leq H_k^+ (k = 1, \ldots, m)$.

Cədvəl 4.3.1-də illüstrasiya üçün 3 insident üçün prosedurlar siyahısı və 4 CERT-qrupu üçün prosedurların emal müddətləri təqdim olunur.

Cədvəl 4.3.1.

Üç insident və dörd CERT-qrupu üçün prosedurların emal müddətləri

İnsidentlər	Prosedurlar	Prosedurların emal müddətləri			
		R_1	R_2	R_3	R_4
J_1	O_{11}	1	3	4	1
	O_{12}	3	8	2	1
	O_{13}	3	5	4	7
J_2	O_{21}	4	1	1	4
	O_{22}	2	3	9	3
	O_{23}	9	1	2	2
J_3	O_{31}	8	6	2	5
	O_{32}	4	5	8	1

Cədvəldən göründüyü kimi, məsələn, J_1 insidentinin cavablandırılması O_{11}, O_{12} və O_{13} prosedurlarının ardıcıl yerinə yetirilməsini tələb edir. Cədvəlin sətir və sütunlarının kəsişməsində duran ədədlər uyğun prosedurun müvafiq CERT-qrupu

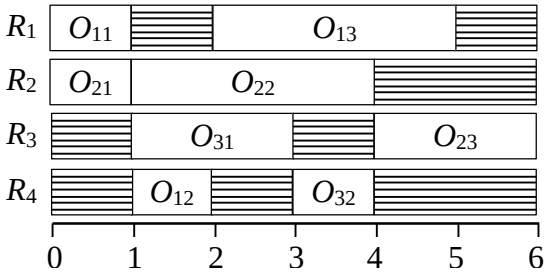
(R_1, R_2, R_3 və R_4) tərəfindən yerinə yetirilməsi müddətini seçilmiş zaman vahidləri ilə (məsələn, saatla) göstərir.

Prosedurlar ardıcıllığı əsasında onların CERT-qruplarına minimal emal müddəti meyarı üzrə təyin edilməsi planı aşağıdakı kimi ola bilər:

S={(O_{11}, R_1), (O_{12}, R_4), (O_{13}, R_1), (O_{21}, R_2), (O_{22}, R_2), (O_{23}, R_1), (O_{31}, R_3), (O_{32}, R_4)} = {(O_{11}, R_1: 0-1), (O_{12}, R_4: 1-2), (O_{13}, R_1: 2-5), (O_{21}, R_2: 0-1), (O_{22}, R_2: 1-4), (O_{23}, R_3: 4-6), (O_{31}, R_3: 1-3), (O_{32}, R_4: 3-4)}.

Plana görə, məsələn, O_{11} proseduru R_1 CERT-qrupu tərəfindən [0; 1] zaman intervalında, O_{12} proseduru R_4 CERT-qrupu tərəfindən [1; 2] zaman intervalında, O_{13} proseduru isə R_1 CERT-qrupu tərəfindən [2; 5] zaman intervalında icra edilməlidir. Beləliklə, J_1 insidentinin emalına iki CERT qrupu cəlb edilir: O_{11} və O_{13} prosedurları R_1 CERT-qrupu, O_{12} proseduru isə R_4 CERT-qrupu tərəfindən yerinə yetiriləcək.

Adətən belə tipli planları vizuallaşdırmaq üçün Qantt diaqramı istifadə edilir. Yuxarıda verilmiş plana uyğun Qantt diaqramı şəkil 4.3.1-də göstərilib.



Şəkil 4.3.1. Üç insident və dörd CERT-qrupu üçün emal planının diaqramı

Diaqramdan göründüyü kimi, R_1 qrupu [1; 2] və [5; 6], R_2 qrupu [4; 6], R_3 qrupu [0; 1] və [3; 4], R_4 qrupu [0; 1], [2; 3] və [4; 6] zaman intervallarında boş olurlar.

İnsidentlərin emalının ümumi müddətini tapaq. Tutaq ki, t_{ij}^F ilə O_{ij} prosedurunun başa çatma anı işarə edilib. Yuxarıdakı plan üçün şəkil 4.3.1-dən uyğun t_{ij}^F anlarını tapmaq və onların arasından maksimumu seçməklə ümumi emal müddətini müəyyən etmək olar. Beləliklə, insidentlərin emalının ümumi müddəti 6 zaman periodu olacaq:

$$t = max\{t_{11}^F, t_{12}^F, t_{13}^F, t_{21}^F, t_{22}^F, t_{23}^F, t_{31}^F, t_{32}^F\} = max\{1,\ 2,\ 5,\ 1,\ 4,\ 6,\ 3,\ 4\} = 6.$$

Yuxarıda və həmçinin yeni daxil edilmiş işarələri aşağıdakı kimi sistemləşdirək:

n – insidentlərin sayı;

m – CERT-qrupların sayı;

ni – 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 indeksidir, i, h = 1, 2, ..., n;

k – CERT-qruplarının indeksidir, burada k = 1, 2, ..., m;

j, g – cavadlandırma prosedurlarının indeksidir, burada 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 (kritiklik dərəcəsi və ya gecikməyə görə cərimə əmsalı);

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

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

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

$$W_k = \sum_{i=1}^{n} \sum_{j=1}^{n_j} p_{ijk} x_{ijk}, \quad (4.3.1)$$

i-ci insidentin cavablandırılmasının gecikmə müddəti T_i belə müəyyən olunur:

$$T_i = max\left(t_{i,n_i}^{F} - d_i, 0\right), \quad (4.3.2)$$

Adətən, insidentlərin emalını planlaşdıran zaman bir deyil, bir neçə kriteriya nəzərə alınmalıdır. 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, bu işdə 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:

$$min\, F_1 = \max_{1\le i\le n}\left\{\max_{1\le j\le n_i}\{t_{ij}^F\}\right\}, \tag{4.3.3}$$

$$\min F_2 = \max_{1\le i\le n}\{w_i T_i\}, \tag{4.3.4}$$

$$min\, F_3 = \max_{1\le k\le m}\{W_k\}. \tag{4.3.5}$$

Modeldə aşağıdakı məhdudiyyətlər vardır:

$$t_{ij}^F - t_{i,j-1}^F \ge p_{ijk}x_{ijk}, j = 2, \dots, n_i, \forall i, k \tag{4.3.6}$$

$$\begin{aligned}&\left[(t_{hg}^F - t_{ij}^F - t_{hgk})x_{hgk}x_{ijk} \ge 0\right]\\ &\vee\left[(t_{ij}^F - t_{hg}^F - t_{ijk})x_{hgk}x_{ijk} \ge 0\right], \forall (i,j),(h,g),k\end{aligned} \tag{4.3.7}$$

$$\sum_{k=1}^{m} x_{ijk} = 1, \forall i, j. \tag{4.3.8}$$

(4.3.6) şərti prosedurların ardıcıllığına olan məhdudiyyətləri təmin edir. (4.3.7) şərti hər bir CERT-qrupun ixtiyari zaman anında yalnız bir proseduru emal edə bildiyini ifadə edir. (4.3.8) şərti hər bir prosedurun emalı üçün bir CERT-qrupunun seçilə bildiyini göstərir.

Bu işdə çoxkriteriyalı optimallaşdırma məsələsinin həlli üçün mövcud yanaşmalardan ən sadə yanaşma götürülmüşdür. Belə ki, ümumi məqsəd funksiyası hər birinə eyni çəki verməklə yuxarıda ifadə edilmiş məqsəd funksiyalarının çəkili cəmi kimi müəyyən edilir:

$$F = \frac{1}{3}F_1 + \frac{1}{3}F_2 + \frac{1}{3}F_3. \tag{4.3.9}$$

Optimallaşdırma məsələsi üçün həll alqoritmi

Bu bölmədə qoyulmuş məsələnin həlli üçün 1997-ci ildə R. Storn və K. Price tərəfindən təklif edilmiş diferensial evolyusiya (DE) alqoritmi tətbiq olunur [275].

Həllin vektorlarla təsviri

Qoyulmuş optiamallaşdırma məsələsində iki altməsələ var: prosedurların CERT-qruplara təyinatı məsələsi və prosedurların ardıcıllığı məsələsi. Ona görə məsələnin həllini iki vektorla göstərmək məqsədəuyğun olardı [21, s.80]. Vektorlardan biri prosedurların permutasiyasını göstərir, digər vektor isə prosedurların CERT-qruplara təyinatını təsvir edir. Hər iki vektor N-ölçülüdür, burada N – prosedurların ümumi sayıdır. Təklif olunmuş bu təsvir metodu həllin ardıcıllıq şərtlərini ödəməsini təmin edir. Qeyd edək ki, bu iki vektoru bir vektorda birləşdirmək də olar.

Prosedurların permutasiyası vektoru. Permutasiya prosedurların ardıcıllığını göstərmək üçün istifadə olunur. Eyni insidentə aid olan prosedurlar vektorda eyni ədədlə işarə olunur. Prosedurların bu təsvir metodu şəkil 4.3.2-də illüstrasiya edilir. Məsələn, vektorun birinci elementi olan 3 ədədi insident 3-ə uyğundur, həm də

O_{31}	O_{11}	O_{21}	O_{12}	O_{32}	O_{22}	O_{23}	O_{13}
3	1	2	1	3	2	2	1

Şəkil 4.3.2. Prosedurların permutasiyası vektoru

insident 3-ə ilk dəfə rast gəlinir, buna görə insident 3-ün 1-ci proseduruna, yəni O_{31}-ə uyğun gəlir. Oxşar qaydada, vektorun beşinci elementi olan 3 ədədi insident 3-ün ikinci rastgəlməsidir, buna görə insident 3-ün 2-ci prosedurunu, yəni O_{32}-ni işarə edir.

CERT-qrupların təyinatı vektoru. Bu vektorun elementi uyğun prosedur üçün təyin edilmiş CERT-qrupunu işarə edir. Təyinatlar vektoru şəkil 4.3.3-də illüstrasiya edilir. Məsələn, vektorun birinci elementindən yuxarıda yazılan O_{11} onu bildirir ki, insident 1-in 1-ci proseduru CERT-qrup 1 tərəfindən yerinə yetiriləcək. Oxşar olaraq, O_{12} və O_{13} işarə edir ki, insident 1-in 2-ci proseduru CERT-qrup 4 tərəfindən, 3-cü proseduru isə yenə CERT-qrup 1 tərəfindən icra olunacaq.

O_{11}	O_{12}	O_{13}	O_{21}	O_{22}	O_{23}	O_{31}	O_{32}
1	4	1	2	2	3	3	4

Şəkil 4.3.3. CERT-qrupların təyinatı vektoru

İlkin populyasiyanın generasiyası

İlkin populyasiya alqoritmin məhsuldarlığına böyük təsir göstərir. Təklif edilən alqoritmin yaxşılaşdırılması üçün ilkin populyasiya Kacem və həmmüəlliflərinin

yanaşmasından istifadə edilir [194, s.1-13]. Bu yanaşmada ilkin populyasiya AssignmentRule1 və AssigmentRule2 ilə generasiya olunur. AssignmentRule1 emal müddətinin minimallaşdırmasına fokuslanır, prosedurların və CERT-qrupların ardıcıllığını müəyyən edir. AssigmentRule2 populyasiyanın müxtəlifliyini təmin edir.

İstifadə edilən alqoritmdə prosedurların və CERT-qrupların ardıcıllığı təsadüfi generasiya edilir. Təyinatlar müəyyən ediləndən sonra CERT-qruplarında prosedurların ardıcıllığı nizamlanır. Buna üç müxtəlif metodun köməyi ilə nail olurlar: təsadüfi (insident təsadüfi seçilir), əksəriyyəti qalmış iş və əksəriyyəti qalmış prosedurlar seçilir. Təklif edilmiş alqoritmdə ilkin populyasiya fərdlərinin 40 %-i AssignmentRule1, 60 %-i AssignmentRule2 istifadə edilməklə generasiya edilir, prosedurların ardıcıllığı növbə ilə yuxarıdakı üç dispetçer qaydası ilə tənzimlənir.

Diskret diferensial evolyusiya alqoritmi

DE alqoritminin konsepsiyası genetik alqoritmlərin də daxil olduğu geniş evolyusiya alqoritmlərindən götürülüb. Mutasiya, çarpazlaşma və seçmə kimi bir neçə mexanizm mövcud həlləri yenidən kombinasiya etməklə yeni həllər almaq və optimal həll və ya ən azı, məsələnin şərtlərini ödəyən həllərin tapılmasında istifadə edilir. DE kəsilməz qiymətli optimallaşdırma məsələləri üçün təklif edilmişdi. [76, s.20]-da binar dəyişənlər üçün DE alqoritmi təklif edilir. DE-nin tamqiymətli optimallaşdırma məsələləri üçün variantları da təklif edilmişdir [217, s.1238].

Burada baxılan məsələnin həlli üçün [252, s.795]-də təklif edilmiş diskret diferensial evolyusiya (DDE) alqoritmi modifikasiya olunur. Tutaq ki, populyasiyanın fərdləri *2N*-ölçülü $x_i, \forall i \in \{1, \dots, N_p\}$ vektorları kimi təsvir edilir, burada *N* insident prosedurlarının ümumi sayıdır, N_p isə populyasiyanın həcmidir.

Mutasiya. Başlanğıcda mutasiya əməliyyatı tətbiq edilir. Mutant populyasiya üçün aşağıdakı tənlikləri istifadə etmək olar:

$$V_i^t = P_m \otimes F(x_i^{t-1}), \tag{4.3.10}$$

$$V_i^t = P_m \otimes F(x_a^{t-1}), \tag{4.3.11}$$

$$V_i^t = P_m \otimes G\left(x_g^{t-1}\right). \tag{4.3.12}$$

Burada: V_i^t – t-ci iterasiyada populyasiyanın i-ci mutant fərdidir, x_i^{t-1} – $(t-1)$-ci iterasiyada populyasiyanın i-ci fərdidir; x_a^{t-1} – $(t-1)$-ci iterasiyada populyasiyadan təsadüfi seçilmiş fərddir; x_g^{t-1} – $(t-1)$-ci iterasiyada qlobal ən yaxşı həldir. G – mutasiya operatoru, P_m – mutasiya ehtimalıdır. $\otimes$ – şərt operatorudur, onun solundakı ehtimal müəyyən şərti ödədikdə, sağındakı mutasiya operatoru yerinə yetirilir.

Tutaq ki, mutant populyasiya üçün (4.3.10) tənliyi istifadə edilir. [0; 1]-dən müntəzəm paylanmış təsadüfi r ədədi seçilir. $r < P_m$ olarsa, onda t-ci iterasiyada mutant fərdi generasiya etmək üçün $V_i^t = F(x_i^{t-1})$ operatoru istifadə edilir. Əks halda, t-ci iterasiyada mutant fərd $V_i^t = x_i^{t-1}$ kimi qəbul edilir.

Krossover. Sonra sınaq fərdi adlanan fərd yaradılır, bunun üçün mutasiya edilmiş fərd (V_i^t) ilə cari populyasiyadan olan, hədəf fərd adlanan x_i^{t-1} fərdi arasında aşağıdakı qayda ilə çarpazlaşma əməliyyatı yerinə yetirilir:

$$y_i^t = P_c \otimes CR(x_i^{t-1}, V_i^t), \tag{4.3.13}$$

burada: CR – krossover operatorudur, P_c – krossover ehtimalıdır. Əgər müntəzəm paylanmış $r \in (0,1)$ təsadüfi ədədi üçün $r < P_c$ olarsa, onda sınaq fərdini generasiya etmək üçün CR krossover operatoru tətbiq edilir: $y_i^t = CR(x_i^{t-1}, V_i^t)$. Əks halda sınaq fərdi $y_i^t = V_i^t$ kimi seçilir.

Seçmə. Mutasiya və çarpazlaşma proseslərindən sonra seçmə proseduru tətbiq edilir. Sınaq fərdinin uyğunluq qiyməti hesablanır və hədəf fərdin uyğunluğu ilə müqayisə edilir. Bu iki fərddən ən uyğun olanı növbəti populyasiyaya daxil edilir:

$$x_i^t = \begin{cases} y_i^t, \text{əgər } F(y_i^t) \le F(x_i^{t-1}) \\ x_i^{t-1}, \text{əks halda} \end{cases} \tag{4.3.14}$$

Populyasiyanın bütün fərdlərinə yuxarıdakı prosedurlar tətbiq edilməklə yeni populyasiya əldə edilir və bu əvvəlcədən təyin edilmiş dayanma meyarı ödənənə kimi təkrarlanır. Axırıncı nəslin ən yaxşı fərdi məsələnin həlli kimi götürülür.

Yuxarıda təklif edilmiş DDE alqoritmində genetik alqoritmlərdən götürülmüş mutasiya operatoru və krossover operatoru istifadə edilir.

Mutasiya operatoru. Prosedurlar ardıcıllığını mutasiya etmək üçün təsadüfi prosedur seçilir, ondan bilavasitə əvvəl gələn prosedur və ondan bilavasitə sonra gələn prosedur seçilir. Tutaq ki, onların indeksləri uyğun olaraq a və b-dir. Seçilmiş prosedur (a, b) intervalında yerləşdirilir. Bu mutasiya alqoritmi ardıcıllıq məhdudiyyətini saxlayır və buna görə həllin mümkün həllər oblastından olmasını təmin edir. CERT-qrupların təyinat vektorunu mutasiya etmək üçün belə bir strategiyadan istifadə etmək təklif edilir. İş yükü maksimum olan CERT-qrupda elə prosedurlar axtarılır ki, onları yükü minimal olan CERT-qrup yerinə yetirə bilir. Belə prosedurlardan biri iş yükü minimal olan CERT-qrupa təyin edilir.

Çarpazlaşma operatoru. Həll vektorunun birinci hissəsi – prosedurlar ardıcıllığı üçün POX (ing. precedence preserving order-based) krossover operatoru yerinə yetirilir, ikinci hissədə isə təsadüfi çoxnöqtəli krossover operatoru tətbiq edilir [134, s.368]. Bu yolla məhdudiyyət şərtlərini ödəyən yararlı nəsil generasiya etmək olar.

IV fəsil üzrə nəticələr

- DoS hücumların aşkarlanması üçün Qauss-Bernulli tipli məhdud Bolsman maşınları əsasında dərin təlim metodu işlənmişdir [183, s.1-17];
- İnT insidentlərinin emalı üzrə əməliyyatların operativ planlaşdırılması və CERT-qrupları arasında paylanması optimallaşdırma məsələsi kimi ifadə edilmiş və onun həlli üçün diskret diferensial evolyusiya alqoritmi işlənmişdir [21, s.80-91];
- E-dövlət mühitində İnT insidentlərinin emal prioritetlərinə təsir edən faktorların iyerarxik strukturu təklif edilmiş və bu faktorlar əsasında insidentlərin ranqlaşdırılması metodu işlənmişdir [178, 183-187].

V FƏSİL. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ SAHƏSİNDƏ KOORDİNASİYA MODELLƏRİ

İnformasiya təhlükəsizliyinin təmin edilməsi üçün dövlətlər arasında beynəlxalq koordinasiya da olduqca vacib əhəmiyyət daşıyır. [31]-də müasir İnT təhdidlərinin qarşısının alınması üçün dünya ölkələrinin səylərinin birləşdirilməsinin, yeni strateji yanaşmanın formalaşmasının zəruriliyi vurğulanır. Bir çox ölkə kiberfəzada oxşar kibertəhdidlərlə qarşılaşır və öz kibertəhlükəsizliyini təmin etmək üçün yetərli resurslara malik deyil. Bu vəziyyətdə ölkələrin qarşılıqlı faydalılıq əsasında öz səylərini birləşdirməsi və kibertəhlükəsizlik sahəsində koalisiya şəklində mübarizə aparması daha məqsədəuyğundur.

Bu fəsildə koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi üçün indikatorlar sistemi təklif edilir [17, s.47], ikisəviyyəli iyerarxik sistemdə İnT investisiyalarının koordinasiyası modeli [52, s.41] və İnT servislərinin təşkili üzrə beynəlxalq koalisiya modeli [22, s.76 23, s.14, 32, s.6] işlənilir.

5.1. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi modeli

İnformasiya təhlükəsizliyi üzrə koordinasiya sisteminin təkmilləşdirilməsi üzrə təkliflər işləmək üçün koordinasiyanın mövcud səviyyəsini qiymətləndirmək vacibdir. Lakin koordinasiyanın mövcud səviyyəsini və effektivliyini qiymətləndirmək olduqca çətin məsələdir.

Bu işdə koordinasiya sisteminin qiymətləndirilməsi üçün informasiya yanaşması əsas götürülür. İnformasiya koordinasiya üçün əsas resursdur, bütün koordinasiya sisteminin effektivliyi onun keyfiyyətindən, həqiqiliyindən, vaxtında olmasından asılıdır. Məsələn, analizlər göstərmişdi ki, 2005-ci ildə ABŞ-da baş vermiş Katrina qasırğası zamanı dövlət orqanları arasında meydana çıxan koordinasiya problemləri əsasən informasiya mübadiləsi problemlərindən qaynaqlanmışdı [111, s.391]. T. Malone və K. Crowston koordinasiya anlayışına "*bir neçə aktor bir aktorun təklikdə əldə edə bilməyəcəyi bir məqsədə nail olmağa çalışdıqda informasiyanın yerinə yetirilən əlavə emalı*" kimi tərif verirlər [226, s. 357-370]. Təbii fəlakətlərlə

mübarizə sistemlərində koordinasiyanın həyata keçirilməsində informasiyanın rolu [116, s.295]-da analiz edilir və vaxtında olan əlaqədar informasiyanın koordinasiyaya və fövqəladə halların aradan qaldırılmasının effektivliyinə birbaşa təsir etdiyi müəyyən edilir.

Fövqəladə halların digər növləri ilə müqayisədə İnT insidentlərinin qarşısının alınması, aşkarlanması və nəticələrinin aradan qaldırılması zamanı informasiyanın rolu daha qabarıqdır. Burada informasiya əsas resurs kimi çıxış edir, informasiyanın mübadiləsi və koordinasiyası bütün işlərin həyata keçirilməsi və qərar qəbulu üçün əsas təşkil edir. Buna görə İnT üzrə koordinasiya sisteminin təkmilləşdirilməsinə onun bütün elementlərini birləşdirən və hərəkətə gətirən komponentindən – informasiya axınlarının optimallaşdırılmasından başlamaq ən məqsədəuyğun yanaşma olardı. Bu məqsədlə bu bölmədə e-dövlətin İnT sistemində koordinasiya səviyyəsini qiymətləndirmək üçün qraflar nəzəriyyəsi və sosial şəbəkə analizi əsasında bir sıra metrikalar təklif edilir [17, s.47].

Əlaqədar işlərin icmalı

E-dövlətin İnT-nin idarə edilməsində əsas problemlərdən biri dövlət orqanları arasında effektiv koordinasiyanın təmin edilməsidir. Lakin zəruri informasiyanın olmadıqda effektiv koordinasiya mümkün deyil. İnformasiyanın olmaması təşkilatlar arasında koordinasiyanın səmərəliliyini məhdudlaşdırır, çünki koordinasiya fəaliyyət planları yalnız əldə olan informasiya əsasında qurulur. Ona görə də müvafiq təşkilatlar arasında informasiya mübadiləsi infrastrukturunu təkmilləşdirmək üçün ciddi səylər göstərilir.

İnformasiyanı sürətlə mübadilə etmək və hərəkətləri koordinasiya etmək qabiliyyəti kiberhücumların qarşısının alınması, onların aşkarlanması və nəticələrinin aradan qaldırılması üçün ən vacib funksiyadır. Hazırda kiberhücumların aşkarlanmasının bir çox məsələsi təşkilat çərçivəsində həll edilir və təşkilatlararası informasiya mübadiləsi azdır. Lakin informasiya mübadiləsi irimiqyaslı kiber-hücum situasiyalarını dərindən başa düşmək yolunda həlledici addımdır və gələcək şəbəkələrin müdafiəsində əsas konsepsiyalardan biridir. Dövlət orqanları arasında

qarşılıqlı əlaqə reqlamentlərinin standartlaşdırılması, formal informasiya paylaşımının müəyyən edilməsi və qeyri-formal informasiya paylaşımının təşviq edilməsi də aktual problemlərdəndir [17, s.47, 47, s.11].

Gizli kiberhücumların və yeni zərərli proqramların aşkarlanması, erkən xəbərdarlıqların və təhlükəsizliyin təmin edilməsi üzrə məsləhətlərin verilməsi, təhlükələr barədə məlumatların selektiv çatdırılması – informasiya mübadiləsinin bir çox istifadə variantlarından yalnız bəziləridir. [270, s.154] icmal məqaləsində kibertəhlükəsizlik sahəsində informasiya paylaşımı aspektləri analiz edilir. İnformasiya mübadiləsi sistemlərinə daha detallı tələblərin işlənməsi, təşkilati və texnoloji məsələlər, hüquqi aspektlər və standartlaşdırma istiqamətləri vurğulanır.

Kapucu N. və həmmüəllifləri [196, s.1]-da fövqəladə hadisələrin (11 sentyabr 2001-ci il terror hücumu) cavablandırılması zaman təşkilatlarası şəbəkəyə baxırlar, dövlət, özəl və ictimai təşkilatlar arasındakı formalaşan qarşılıqlı əlaqələri analiz edirlər. Tədqiqatda dinamik şəbəkə nəzəriyyəsi və mürəkkəb adaptiv sistemlər nəzəriyyəsindən alınmış nəzəri metodlar istifadə edilir. Cavablandırma sistemində iştirak edən əsas təşkilatların müəyyən edilməsi üçün təşkilati analiz metodları tətbiq edilir. Tədqiqatın nəticələrinə görə, effektiv cavab və bərpa bütün səviyyələrdə dövlət orqanları arasında, dövlət və özəl sektorlar arasında yaxşı əlaqələndirilmiş təşkilati şəbəkələr və inam tələb edir.

Abbasi A. və həmmüəllifləri tərəfindən bir neçə təşkilatın iştirak etdiyi cavablandırma əməliyyatlarında koordinasiyanın təkmilləşdirilməsi yollarına baxılır [71, s.1-17]. Fövqəladə hadisənin cavablandırılması zamanı şəxslərarası koordinasiya əməliyyatları analiz edilərək dörd zaman periodu ərzində şəbəkənin evolyusiyasına baxılır. Nəticələr göstərir ki, informasiya mübadiləsi üçün tələb edilən böyük həcmdə kommunikasiya səbəbindən zaman keçdikcə şəbəkə daha demərkəzləşmiş olur.

Koordinasiyanın effektivliyi xarakteristikaları ilə sosial şəbəkə analizindən götürülmüş kəmiyyətlərin əlaqəsi məsələsi bir sıra digər tədqiqatlarda da araşdırılmışdır [287, s.54]. Sosial şəbəkədə aktorun əlaqələrini xarakterizə edən, geniş istifadə edilən metrika mərkəzilikdir. Mərkəzilik ilə layihələr üzrə işlərin koordinasiyasının keyfiyyəti arasındakı korrelyasiya əlaqəsinin aydınlaşdırılması

məsələsi tədqiqatçıları çox cəlb edir. Dərəcə üzrə mərkəziliyi böyük olan aktorların daha keyfiyyətli koordinasiya nümayiş etdirməsi [168, s.363]-də qeyd edilir. Proqram təminatının işlənməsi layihələrində, tikinti layihələrində mərkəzilik ölçüsü ilə koordinasiyanın keyfiyyəti arasındakı əlaqə öz təcrübi təsdiqini tapır [17, s.47].

[167, s.755]-də əlaqəlilik ölçüsü ilə koordinasiyanın keyfiyyəti arasındakı korrelyasiya müəyyən edilir. Fövqəladə halların aradan qaldırılmasına cəlb olunmuş aktorlar şəbəkəsində əlaqəlilik ölçüsü böyük olduqca fövqəladə hallar zamanı informasiyanın keyfiyyəti və əlyetərliliyi artır [287, s.54]. Əlaqənin gücü agentlər arasındakı münasibətlərin keyfiyyətini qiymətləndirmək üçün vacib atributdur.

Koordinasiya sisteminin multiagent şəbəkə modeli

Bu bölmədə koordinasiya sisteminin strukturuna makrosəviyyədə – ümumdövlət səviyyəsində baxılır və İnT üzrə milli koordinasiya sisteminin multiagent şəbəkəsi şəklində modeli təklif edilir. Məlum olduğu kimi, koordinasiya formal və qeyri-formal formalarda həyata keçirilə bilər. Formal koordinasiya zamanı qarşılıqlı əlaqə prosesini tənzimləyən qaydaların sonlu çoxluğu verilir. Qeyri-formal koordinasiya etimad, qarşılıqlı fayda və münasibətlər əsasında meydana çıxır. Bu işdə formal koordinasiyaya baxılır.

Fərz olunur ki, e-dövlətin İnT sistemi ayrı-ayrı İnT domenlərindən (İTD-lərdən) ibarətdir və bu domenlər biznes proseslərin təhlükəsiz korporativ mühitdə yerinə yetirilməsi üçün müvafiq İnT servisləri göstərirlər. Bu domenlərin fəaliyyəti və onlarda həyata keçirilən müvafiq İnT tədbirləri mütləq koordinasiya edilməlidir. Bu işdə e-dövlətin İnT-nin idarə edilməsi üzrə koordinasiya strukturunu dörd idarəetmə səviyyəsinə dekompozisiya etmək təklif olunur:

- ümumdövlət (eyni vaxtda iki və ya daha artıq İTD-ini əhatə edən İnT tədbirləri – İTD-lər, xarici ölkələrin və beynəlxalq təşkilatların müvafiq) qurumları arasında koordinasiya həyata keçirilir);
- korporativ (bir İTD ilə məhdudlaşan İnT tədbirləri – İTD-nin əhatə etdiyi təşkilati strukturlar arasında koordinasiya tələb edilir);

- lokal (nəticələri bir servis (sistem) çərçivəsindən kənara çıxan İnT tədbirləri – İTD bölmələrinin fəaliyyəti koordinasiya edilir);
- obyekt (nəticələri bir servis (sistem) çərçivəsində məhdudlaşan İnT tədbirləri – obyektin istismarına məsul xidməti personal arasında koordinasiya tələb edilir).

Burada "İnT tədbirləri" geniş spektri nəzərdə tutur, xüsusi halda, məsələn, kiberhücumların aşkarlanması və nəticələrinin aradan qaldırılması tədbirləri nəzərdə tutula bilər. Qeyd etmək zəruridir ki, dördsəviyyəli dekompozisiya ideyası [61, s. 4]-nın təsiri ilə formalaşdışdır.

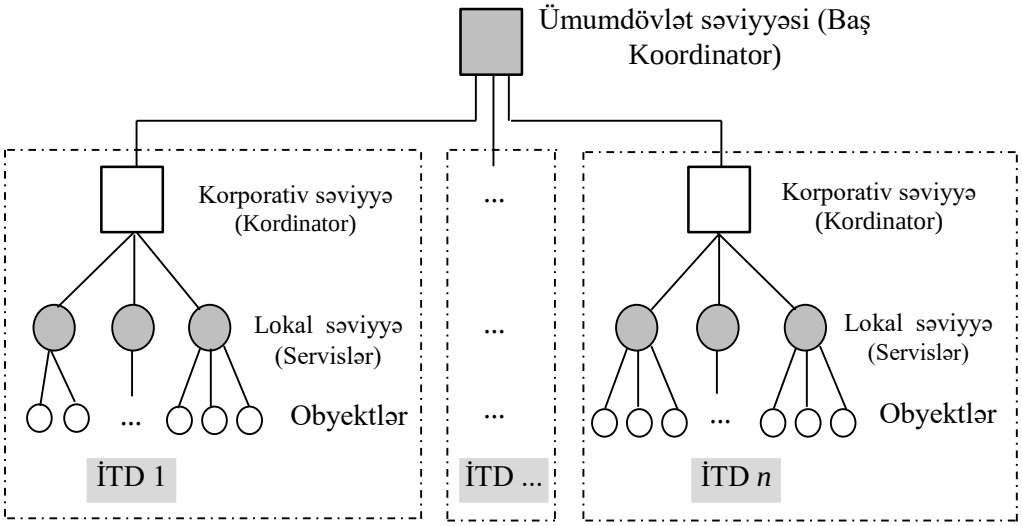
Koordinasiya sistemi çərçivəsində istənilən səviyyənin idarə edilməsi insan – qərar qəbuledən şəxs (QQŞ) tərəfindən reallaşdırılır. QQŞ məqsədəuyğun şəkildə (məqsəd qoymaq, məsələləri müəyyən etmək, onların həlli üçün vasitə və resursları seçmək yolu ilə) qərar qəbul edilməsini həyata keçirir. Buna görə A çoxluğunun hər bir A_{ij} obyektini onun modeli ilə – agentlə əvəzləmək olar. Agent digər agentlərə nəzərən avtonom və asinxron hərəkət edir. Agentlərdən hər biri öz domeninə daxil olan digər agentlərlə qarşılıqlı təsirdə olur və fəaliyyət prosesində həm xarici mühiti (digər agentlər də baxılan agentə görə xarici mühit hesab olunur), həm də öz davranışını dəyişə bilər. Fərz olunur ki, hər bir domendə bir Koordinator təyin edilmişdir və onların vəzifəsi domendaxili və domenlərarası qarşılıqlı (informasiya) əlaqəsini həyata keçirməkdir. Hər hansı agent digər domenin agentləri ilə əlaqə saxlamaq üçün öz domeninin Koordinatoruna müraciət edir.

Hər bir domenin İnT sahəsində öz maraqları var və domen Koordinatoru domenin maraqlarından çıxış edir. Bu maraqlar ümumi sistemin maraqları ilə uzlaşmaya bilər. Buna görə, maraqların uzlaşmasını və fəaliyyətin koordinasiyasını təmin etmək üçün e-dövlətin İnT sistemində Baş Koordinator (BK) nəzərdə tutulur. BK ümumdövlət səviyyəsində fəaliyyət göstərir, domenlərin fəaliyyətini tənzimləyir və bu fəaliyyətin zamana görə paylanmasına (yəni planlaşdırmaya) görə cavabdehdir.

Baş Koordinatorun əsas vəzifəsi dövlət orqanlarının İnT üzrə öz missiyalarını yerinə yetirməsi üçün zəruri olan informasiyaya giriş əldə edə bilmələrini təmin

etməkdir. O bu vəzifəni aşağıdakı sahələrdə həyata keçirir – inteqrasiya, əməkdaşlıq və koordinasiya, situasiyadan məlumatlılıq, İnT insidentlərinə reaksiya, analiz və hesabatlılıq, biliklərin idarə edilməsi, yeni texnologiyalar və idarəetmə.

Beləliklə, Baş Koordinaor, domen koordinatorları və agentlər çoxluğu iyerarxik koordinasiya sisteminin modelini – multiagent şəbəkəsini əmələ gətirir (şəkil 5.1.1).



Şəkil 5.1.1. Koordinasiya sisteminin dördsəviyyəli strukturu

Məlumdur ki, müxtəlif şəbəkələrin ən sadə və əlverişli riyazi təsviri qraflar vasitəsilə əldə edilir. Tutaq ki, e-dövlətin İnT-nin 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:

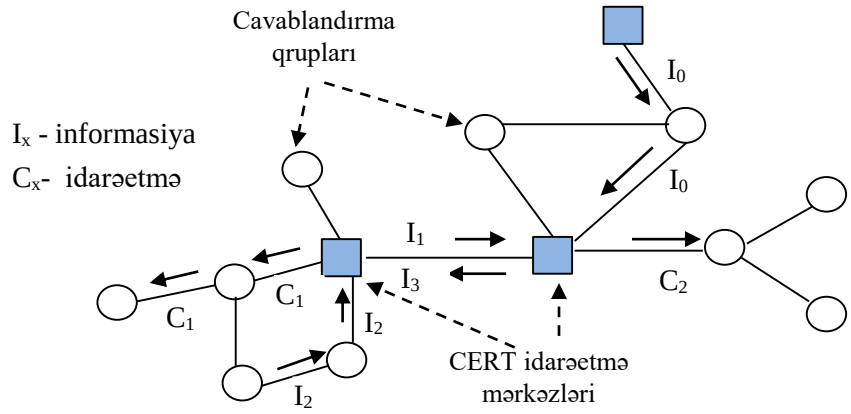
$$a_{ij} = \begin{cases} 1 - i \text{ və } j \text{ agentləri til ilə birləşir,} \\ 0 - \text{əks halda.} \end{cases} \quad (5.1.1)$$

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 olar.

Koordinasiya şəbəkəsinə aid misal

Bir (və ya bir neçə) İTD-yə daxil olan müxtəlif struktur bölmələri arasında koordinasiya məsələsi İnT insidentlərinin emalı zamanı tez-tez meydana çıxır. İnformasiya təhlükəsizliyi insidentlərinin qarşısının alınması, vaxtında aşkarlanması və qısa müddətdə nəticələrin aradan qaldırılması üçün geniş yayılmış yanaşmalardan biri CERT komandalarının təşkil olunmasıdır [56, s.15]. Hazırda müxtəlif ölkələrdə çox sayda CERT komandaları fəaliyyət göstərir. CERT komandaları akademik; dövlət; hərbi; milli; kritik infrastruktur; kommersiya; daxili; kiçik və orta biznes; ticarət kimi sektorlarda tətbiq edilir [8, s.75].

CERT-in idarəetmə mərkəzi insidentlərin cavablandırılması şəbəkəsində informasiyanın yayılması və qərar qəbulu prosesində koordinasiya mərkəzi (Koordinator) rolunu oynayır [11, s.92]. Şəkil 5.1.2-də koordinasiya şəbəkəsinin üzvləri arasında ikiistiqamətli rejimdə müxtəlif növ informasiya axınları (məsələn, xəbərdarlıq siqnalı, vəziyyət barədə hesabatlar, idarəetmə komandaları və s.) göstərilir. İnformasiya axını insidentin cavablandırılması proseslərinin gedişini obyektiv əks etdirən məlumatlar toplusudur, koordinasiyanın həyata keçirilməsi üçün kommunikasiya kanalları ilə ötürülür. Axınlar düz (idarə edən sistemdən idarə edilən sistemə) və əks (idarə edilən sistemdən idarə edən sistemə) ola bilər.



Şəkil 5.1.2. CERT-komandaların hipotetik şəbəkəsində informasiya axını

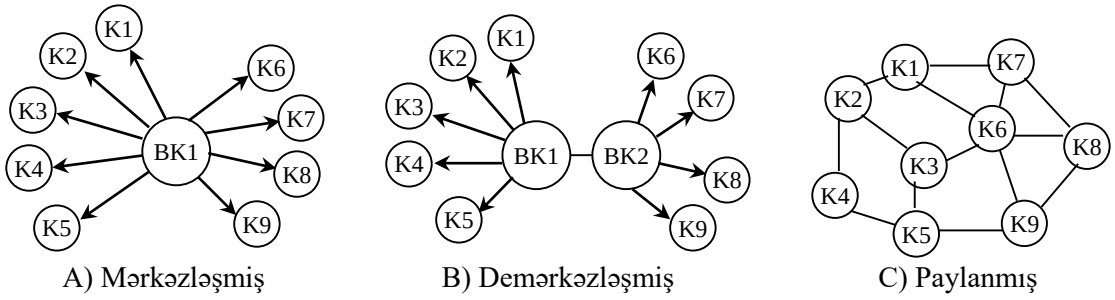
İnsidentin yeri, sinfi, ciddiliyi və s. haqqında informasiya cavablandırma vahidlərindən CERT idarəetmə mərkəzlərinə daxil olur. CERT idarəetmə mərkəzlərindən isə insidentin emalı prosedurları, tədbirlər, komandalar və s. kimi informasiya cavablandırma vahidlərinə doğru hərəkət edir. İstənilən insident

cavablandırma şəbəkəsində informasiyanın ötürülməsi marşrutu və müddəti qərar qəbulu prosesinə əhəmiyyətli təsir edir və cavablandırma vahidinin və idarəetmə mərkəzinin şəbəkədəki yerindən (mövqeyindən) asılıdır [89, s.717].

Koordinasiya şəbəkəsinin iyerarxiya dərəcəsi

Koordinasiya şəbəkəsinin yuxarıda təklif edilmiş dördsəviyyəli struktukturu iyerarxik və mərkəzləşmişdir. İyerarxik struktur tabeçilik, yəni aktorlar arasında qeyri-bərabər əlaqələr olan struktura deyilir. Bu zaman bir istiqamətdəki təsir digər istiqamətdəki təsirdən daha əhəmiyyətli olur.

Qeyd edək ki, iyerarxiyanın daxil edilməsi sistemlərin yaradılmasını və



Şəkil 5.1.3. Koordinasiya şəbəkələrinin müxtəlif növləri

işləməsini olduqca asanlaşdırır. Təbii sistemlərin mütləq əksəriyyətində müəyyən dərəcədə iyerarxiya müşahidə edilir. Lakin istənilən iyerarxiya sistemin imkanlarını, xüsusilə də çevikliyini (adaptivliyini) azaldır.

Bu işdə iyerarxiyanın və mərkəzləşmənin mənfi təsirlərini azaltmaq üçün mərkəzləşmiş koordinasiya strukturundan (şəkil 5.1.3 A) demərkəzləşmiş (şəkil 5.1.3 B) və ya paylanmış (şəkil 5.1.3 C) struktura keçmək təklif edilir. Demərkəzləşmiş struktur bir neçə mərkəzləşmiş altşəbəkədən ibarətdir, altşəbəkələr bir-biri ilə mərkəzi qovşaqları ilə birləşir. Qeyd edək ki, hazırda Azərbaycan Respublikasında İnT insidentlərinin cavablandırılması sahəsində koordinasiya strukturu demərkəzləşmişdir və şəkil 5.1.3 B-də göstərildiyi kimi iki koordinasiya mərkəzinə malikdir (şərti olaraq BK1, dövlət təşkilatlarına, BK2 isə özəl sektora, ictimai təşkilatlara və vətəndaşlara xidmət göstərir). Paylanmış şəbəkə infrastrukturunda (şəkil 5.1.3 B) mərkəzi qovşaq (Baş Koordinator) anlayışı yoxdur, bütün qovşaqlar eyniranqlıdır, koordinasiya Koordinatorlar arasında imzalanmış rəsmi razılaşmalar

əsasında həyata keçirilir (şəkildə tillər belə razılaşmaların mövcudluğunu göstərir). Belə struktur koordinasiya mərkəzlərinin sıradan çıxmalarına olduqca dayanıqlıdır.

Koordinasiya şəbəkələrinin iyerarxiya səviyyəsini ölçmək üçün iyerarxiya dərəcəsi kəmiyyətindən istifadə etmək olar. Şəbəkə iyerarxiyası aktorlar arasındakı münasibətlərin rəsmi səlahiyyət, status və ya prestij əsasında qurulduğu və idarə edildiyi şəbəkələrdə mövcuddur. Şəbəkə iyerarxiyası aktorlar cütü arasındakı birbaşa münasibətlərin (əlaqələrin) istiqamətinə baxır və biristiqamətli münasibətlərin nisbi sayını qiymətləndirir [209, s.89]. Biristiqamətli əlaqə (məsələn, tabeçilik) dedikdə nəzərdə tutulur ki, məsələn, A-dan B-yə əlaqə var, lakin B-dən A-ya əlaqə yoxdur. Şəbəkənin iyerarxiya dərəcəsi belə müəyyən edilir. Tutaq ki, V birbaşa əlaqələri simmetrik olan aktor cütlərinin sayıdır. $maxV$ isə birbaşa əlaqəsi olan aktor cütlərinin maksimal sayıdır (A ilə B, yaxud B ilə A arasında birbaşa əlaqə var). Onda şəbəkənin iyerarxiya dərəcəsini

$$H = 1 - [V/maxV] \tag{5.1.2}$$

kimi hesablamaq olar.

Koordinasiya sisteminin operativliyi metrikaları

Bu işdə koordinasiya sisteminin operativliyinin xarakteristikası kimi sistemin inersiallıq dərəcəsindən istifadə edilməsi təklif edilir [17, s.47]. Ümumiyyətlə, sistemin inersiallıq dərəcəsi ($\Delta\tau$) sistemdə çıxış siqnalı (t_{out}) ilə giriş siqnalı (t_{in}) arasındakı gecikmə kimi müəyyən olunur ($\Delta\tau = t_{out} - t_{in}$). Sistemin inersiya dərəcəsi nə qədər böyükdürsə, sistem təsirlərə bir o qədər "tənbəl" reaksiya verir.

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:

$$K(\mu) = In(\mu) - Fb(\mu). \tag{5.1.3}$$

Verilmiş koordinasiya strukturu üçün “inersiya diametri” anlayışını da daxil etmək olar. Qrafın diametri koordinasiya strukturunun kompaktlığını xarakterizə edir. Qrafın diametri $d(G)$ onun iki təpəsini birləşdirən ən qısa yolun maksimal uzunluğu kimi müəyyən edilir, yəni qrafın iki a və b təpəsi arasındakı maksimal məsafədir:

$$d(G) = \max_{a,b \in V(G)} d(a,b), \tag{5.1.4}$$

burada: a və b qrafın ixtiyari iki təpəsidir, $V(G)$ – bütün təpələrin çoxluğudur, $d(a, b)$ – a və b təpələri arasındakı məsafədir. Bu məsələnin həlli üçün Floyd-Uorşell alqoritmi ilə qrafda bütün təpələr cütləri arasında ən qısa yolları tapmaq və onlarından maksimumu seçmək olar.

Diametr ən uzaqda yerləşən bölmədən informasiyanın idarəetmə qərarlarının qəbul edildiyi mərkəzə ötürülməsi və qəbul edilmiş idarəetmə qərarının ən uzaqda yerləşən digər bölməyə çatdırılması üçün zəruri olan marşrutun maksimal uzunluğunu müəyyən edir. Aydındır ki, diametrin kiçik olması informasiyanı daha tez qəbul edib ötürməyə imkan verir. Beləliklə, qrafın diametri nə qədər kiçikdirsə, koordinasiya sisteminin arxitekturasının effektivliyi bir o qədər yüksək 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:

$$\chi_{ij} = \begin{cases} \alpha\left(T_{ij} - Out_{ij}\right), Out_{ij} \le T_{ij} \\ \beta\left(T_{ij} - Out_{ij}\right), T_{ij} \le Out_{ij} \end{cases} \tag{5.1.5}$$

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 olar:

$$\chi_{ij} = \begin{cases} \alpha\left(T_{ij} - Out_{ij}\right), Out_{ij} \le T_{ij} \\ \beta\left(T_{ij} - Out_{ij}\right), T_{ij} \le Out_{ij} \end{cases} \quad (5.1.6)$$

Bu məsələnin həlli üçün Bellman-Ford alqoritmindən istifadə etmək olar. Deykstra alqoritmindən fərqli olaraq, bu alqoritm çəkisi mənfi olan tillərlə də işləyir və qrafın bir təpəsindən digər bütün təpələrə olan ən qısa yolları tapır**.**

Koordinasiya sistemi üçün sosial şəbəkə metrikaları

Koordinasiya sistemini təsvir etmək üçün sosial şəbəkə analizinin anlayışlarını və qiymətləndirmə metodlarını tətbiq etmək olar [296, s. 3-27]. Sosial şəbəkə strukturlarının qiymətləndirilməsi metodlarına mərkəzi aktorların müəyyən edilməsi, aparıcı aktorların və şəbəkə elementlərini birləşdirən vasitəçilərin axtarışı, şəbəkə strukturlarının identifikasiyası və s. metodları daxildir [296, s. 167-168].

Şəbəkənin ilkin analizi, adətən, mərkəzi aktorların axtarışından ibarətdir. Aktorun vacibliyinin ölçüsü kimi istiqamətlənməmiş qraflarda mərkəzilik, istiqamətlənmiş qraflarda isə daxil olan əlaqələr üçün prestij, çıxan əlaqələr üçün ekspansivlik anlayışları istifadə edilir. Aktorlar üçün çox sayda mərkəzilik indeksləri təklif edilib: Aktorun mərkəziliyi üçün dərəcə əsasında mərkəzilik, yaxınlıq əsasında mərkəzilik, vasitəçilik üzrə mərkəzilik, məxsusi vektorlar əsasında mərkəzilik və s. kəmiyyətlər istifadə edilir [296, s. 169-219].

Dərəcəyə görə mərkəzilik qovşaqdan çıxan və qovşağa daxil olan tillərin cəmi kimi hesablanır. Tilin varlığı informasiyanın ötürülməsini bildirir. Onda ən böyük mərkəziliyə malik aktorlar ən informasiyalı aktor hesab oluna bilər, nəticədə belə aktorlar informasiya axınlarına nəzarət etmək imkanına sahib ola bilərlər.

i aktorunun dərəcə mərkəziliyi (C^D) belə müəyyən edilir:

$$C_i^D = \frac{\sum_{j=1}^{n} a_{ij}}{n-1} = \frac{k_i}{n-1}, \quad (5.1.7)$$

burada: k_i i aktorunun dərəcəsidir, yənu ona qonşu olan aktorların sayıdır.

Əlaqəlilik əmsalı – sistemdə qarşılıqlı əlaqələrin sayı çox olduqda kommunikasiyaların effektivliyinin artmasını əks etdirir. Kommunikasiya qrafı tam əlaqəli olduqda bütün aktorlar arasında birbaşa əlaqə olur. Mümkün birbaşa əlaqələrin sayı $n(n-1)$ olduğu üçün əlaqəlilik əmsalını belə hesablamaq olar:

$$E_{conn} = exp\left\{-\left[1 - \frac{\sum_i \sum_j a_{ij}}{n(n-1)}\right]\right\} \quad (5.1.8)$$

İnformasiya təhlükəsizliyi sisteminin *koordinasiya potensialını* analiz etmək üçün informasiya kanallarının xüsusi sayı kriteriyasını tətbiq etmək olar. İnformasiya kanallarının xüsusi sayı

$$E_{cap} = exp(N/n) \quad (5.1.9)$$

kimi müəyyən edilir, burada: N – tillərin sayı və n – təpələrin sayıdır. Bu kəmiyyət təşkilati strukturun idarəetmə potensialını xarakterizə edir. Koordinasiya kanallarının xüsusi sayı nə qədər çoxdursa, bir koordinatora düşən koordinasiya əlaqələrinin sayı da bir o qədər çoxdur və koordinasiya sistemi daha effektivdir.

Koordinasiya dərəcəsi – koordinasiya şəbəkəsində aktorların informasiya mübadiləsi qabiliyyətini ölçür. Bu kəmiyyəti modelləşdirmək üçün bir neçə yanaşma mövcuddur, ən sadə üsul koordinasiya dərəcəsinin aktorlar arasındakı məsafədən və aktorlar arasındakı əlaqənin gücündən eksponensial asılı olmasını fərz etməkdir. Bu üsulda *i* və *j* agentləri arasındakı koordinasiya dərəcəsi

$$\gamma_{ij} = \exp(-\xi_{ij} d_{ij}) \quad (5.1.10)$$

kimi müəyyən edilir, burada: d_{ij} – i və j agentləri arasındakı məsafədir, ξ_{ij} isə münasibətin gücünü ölçür.

Əlaqənin gücü agentlər arasındakı kommunikasiyanın tezliyi haqqında (gündə, həftədə, ayda, kvartalda, yarımildə, ildə, lazım gəldikdə) toplanmış məlumat əsasında Ridit metodu ilə müəyyən edilir [96, s. 172].

i təpəsinin ümumi koordinasiya dərəcəsini bu təpənin yerdə qalan təpələrlə koordinasiya dərəcələrinin cəminə bərabərdir:

$$\Gamma_i = \sum_{j=1}^{n} \gamma_{ij} \quad (5.1.11)$$

burada: *n* baxılan qrafda təpələrin sayıdır. Təpənin ümumi koordinasiya dərəcəsi bu təpənin mənsub olduğu şəbəkədən ala biləcəyi informasiyanın miqdarını ölçür.

Bütün koordinasiya şəbəkəsinin *orta koordinasiya dərəcəsini* də oxşar şəkildə müəyyən etmək olar:

$$\bar{\Gamma} = \frac{1}{n}\sum_{i=1}^{n} \Gamma_i \qquad (5.1.12)$$

Bu orta qiyməti baxılan şəbəkənin effektivliyinin ölçüsü kimi interpretasiya etmək olar, çünki o ayrıca bir aktorun şəbəkəyə nə qədər töhfə verdiyini ölçür.

Təklif edilmiş kriteriyaların qraflar nəzəriyyəsindən gələn əsas üstünlükləri onların sadəliyi, minimum ilkin informasiya tələb etmələri və təsvirin əyaniliyidir. Gələcək tədqiqatlarda koordinasiya sistemi üçün şəbəkə qrafında hərəkətlə əlaqəli indikatorların (PageRank tipli) və hibrid indikatorların işlənməsi nəzərdə tutulur.

5.2. İnformasiya təhlükəsizliyinin ikisəviyyəli iyerarxik idarəetmə sistemlərində investisiyaların koordinasiyası modeli

Təşkilatlar artmaqda olan İnT təhdidləri ilə mübarizə üçün təhlükəsizlik büdcəsini xeyli artırırlar. Bir ümumi rəyə görə, İnT texniki tədbirlərə gətirilir. Lakin nəzərə almaq lazımdır ki, yaradılan İnT sistemi təkcə texniki baxımdan yox, iqtisadi baxımdan da effektiv olmalıdır [52, s.41]. Son 20 ildə İnT-nə iqtisadi yanaşmanın müxtəlif məsələləri tədqiqatçıların diqqətini cəlb edir. Bu tədqiqat sahəsinin spesifikasını nəzərə almaqla, nəzəri-oyun yanaşması geniş tətbiq edilir və tədqiqatçılar arasında qarşılıqlı asılı təhlükəsizlik oyunları (Interdependent Security Games, IDS oyunlar) xüsusilə populyardır [211, s.231]. Bu oyunlarda eqoist, lakin bədniyyətli olmayan oyunçular İnT-nə investisiya qoymaq, yaxud qoymamaq haqqında qərar qəbul edirlər. Hər bir oyunçunun məqsədi digər oyunçuların da investisiya səviyyələrindən asılı olan öz İnT risklərini minimallaşdırmaq və eyni zamanda, İnT-nə öz investisiya xərclərini minimallaşdırmaqdır.

Bu bölmədə İnT-ni ikisəviyyəli iyerarxik idarəetmə sistemlərində investisiyaların koordinasiyası modeli təklif edilir [52, s.41]. Belə sistemlər Koordinatordan (mərkəzdən) və müəyyən sayda aşağı səviyyə altsistemlərindən ibarətdir, altsistemlər müəyyən dərəcədə müstəqildirlər. Lakin bu altsistemlər bir-birindən təcrid edilməyib, onların arasında qarşılıqlı asılılıqların müxtəlif növləri (funksional, informasiya, idarəetmə) mövcuddur və bir altsistemdə İnT-nin vəziyyəti digər altsistemlərin İnT-nə təsir edir. Bir neçə idarəetmə altsisteminin mövcudluğu

onların özəl məqsədləri arasında ziddiyyətlərə gətirib çıxarır. Bu da öz növbəsində İnT üzrə hərəkət və tədbirlərin uzlaşmamsına səbəb olur.

Bu ziddiyyətlərin aradan qaldırılması Koordinatorun əsas vəzifəsidir. Koordinator aşağı səviyyə elementlərinin fəaliyyətini koordinasiya edir, o cümlədən İnT-nə ayrılmış büdcəni onlar arasında bölür. Fərz olunur ki, bir sistemdə İnT-nin səviyyəsi ayrılmış investisiyaların səviyyəsindən müəyyən şəkildə asılıdır, lakin İnT-nin «qonşu» sistemlərdəki səviyyəsini də nəzərə almaq lazımdır. Koordinatorun məsələsi investisiyaları aşağı səviyyə sistemləri arasında elə paylamaqdan ibarətdir ki, sosial cəhətdən optimal İnT investisiyalarına nail olsun. Bu məsələ nəzəri-oyun məsələsi kimi ifadə olunur və qarşılıqlı asılı təhlükəsizlik oyunu şəklində model təklif olunur.

Əlaqədar işlərin icmalı

İnformasiya sistemlərinin (İS) operatorlarının üzləşdiyi risklər, yalnız özlərinin İnT-nin vəziyyəti ilə müəyyən edilmir, həm də digər tərəflərin İnT üzrə həllərindən çox asılıdır. İS operatorlar arasında bu qarşılıqlı asılılıq İnT həllərinin səmərəliliyini təyin edən fundamental xassədir. Oyunlar nəzəriyyəsi – bu tərəflər arasında strateji qarşılıqlı asılılıqları modelləşdirmənin ən uyğun metodudu və qarşılıqlı asılı təhlükəsizlik oyunları üzrə çox sayda tədqiqat vardır. Bu mövzu üzrə tədqiqatların ətraflı icmalı [215, s. 1-38]-də verilir.

İnT-nin iqtisadiyyatı üzrə ən çox istinad edilən məqalələrdən biri [153, s.438]-dür, burada verilmiş informasiya resursunun təhlükəsizliyi üçün investisiyaların optimal səviyyəsini müəyyən edən iqtisadi model təklif olunur. Bu model İnT-nə investisiyaların artması nəticəsində sistemdə boşluğun azalmasını qiymətləndirir. Gordon-Loeb modeli göstərir ki, ümumilikdə, İnT üzrə tədbirlərə təhlükəsizliyin pozulmasından yarana biləcək gözlənilən zərərin 37 %-dən çoxunu investisiya etmək iqtisadi cəhətdən etibarlı deyil. Lakin J. Villemson göstərmşdi ki, optimal investisiyanın səviyyəsi bu qiymətdən yüksək ola bilər [301, s.1-12].

J. Grossklags dissertasiya işində qarşılıqlı asılı təhlükəsizlik oyunlarının köməyi ilə kibertəhlükəsizlik ilə ümumi səy, ən zəif əlaqə, ən yaxşı müdafiə və ən zəif

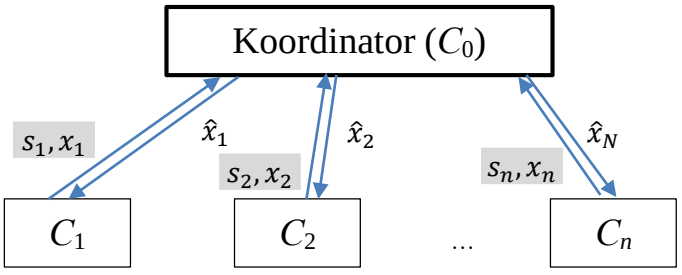
məqsəd kimi investisiya tipləri arasındakı münasibətin iqtisadi analizini yerinə yetirmişdir [154, s. 1-244].

İnvestisiyaların koordinasiyası üçün qarşılıqlı asılı təhlükəsizlik oyunu modeli

E-dövlətin İnT-nin idarə edilməsi sistemi mürəkkəb çoxsəviyyəli sistemlərə aiddir. Onu ikisəviyyəli sistem şəklində təsvir etmək olar, belə yanaşma yolverilən dir, çünki ikisəviyyəli sistemlərdə çoxsəviyyəli sistemlərin bütün əhəmiyyətli xarakteristikaları özünü göstərir və daha mürəkkəb sistemləri ikisəviyyəli sistemlərdən qurmaq olar.

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

Koordinator bütün altsistemlərdən məlumatları aldıqdan sonra, altsistemlərin İnT səviyyələrini, ümumi büdcəyə məhdudiyyəti və altsistemlərin qarşılıqlı asılılıqlarını nəzərə alaraq müəyyən kriteriyalar əsasında altsistemlərə $\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n$ investisiyalarının ayrılması barədə qərar qəbul edir (şəkil 5.2.1).



Şəkil 5.2.1. İkisəviyyəli iyerarxik sistem

Hər bir altsistem eqoist hərəkət edir və mümkün olduqca yüksək investisiya səviyyəsi əldə etməkdə və İnT insidentlərindən öz itkilərini minimallaşdırmaqda maraqlıdır. Koordinatorun məqsədi verilmiş büdcə çərçivəsində bütün sistemdə İnT insidentlərindən itkiləri minimallaşdırmaq, başqa sözlə sosial rifahı maksimallaşdırmaqdır.

Aşağıda bu məsələ qarşılıqlı asılı təhlükəsizlik oyunu kimi ifadə olunur.

n oyunçudan (İnT altsistemləri) və bir Koordinatordan ibarət sistemə baxaq. 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 qonşularının 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 oyunçu özünün $xi \geq 0$ təhlükəsizlik investisiyası səviyyəsini seçir, bu bir investisiya vahidinə $Ci > 0$ xərci çəkilməsinə səbəb olur. Bu fikri aydınlaşdırmaq üçün qeyd edək ki, təhlükəsizlik investisiya həm diskret, həm də kəsilməz ola bilər. Elmi məqalələrin çoxunda diskret investisiya binar qərarı bildirir ($x_i = 1$, əgər oyunçu investisiya qoyursa, $x_i = 0$, əgər oyunçu investisiya qoymursa). Diskret investisiya məsələn, antivirus proqram təminatı kimi İnT vasitəsinin alınmasını modelləşdirə bilər. Kəsilməz investisiya qərarlarına misal müdaxilələrin aşkarlanması sistemlərində həssaslıq səviyyəsinin müəyyən edilməsi ola bilər. Bu halda müdaxilələrin aşkarlanması sisteminin daha yüksək həssaslıq səviyyəsi nəticəsində daha çox sayda hücum siqnalları və xəbərdarlıqlar alınacaq. Onları İnT ekspertləri emel etməlidir və nəticədə daha yüksək xərc tələb ediləcək.

Tutaq ki, $\boldsymbol{x} = \{x_1, x_1, \dots, x_n\}^T$ investisiyalar vektorunu işarə edir. Kiberhücum zamanı oyunçunun gözlənilən itkilərini qiymətləndirmək üçün oyunçunun risk funksiyası anlayışını daxil edək. Bu funksiyalar oyunçuya görə dəyişə bilər, çünki

onların təhlükəsizlik tələbləri və təhlükəsizlik qarşılıqlı asılılıqları müxtəlif ola bilər. Oyunçu i üçün İnT riski onun öz investisiyalarından, həmçinin digər oyunçuların investisiyalarından asılıdır. Oyunçu i üçün riskin qiyməti f_i risk funksiyasından istifadə etməklə hesablanır:

$$f_i(\boldsymbol{x}) = f_i(x_i, \boldsymbol{x}_{-i}), \qquad (5.2.1)$$

burada: $\boldsymbol{x}_{-i}$ – oyunçu i olmadan bütün istifadəçilərin investisiyaları vektorudur. Çox zaman f_i risk funksiyası İnT insidentinin ehtimalı kimi nəzərdə tutulur, bu halda $f_i \in [0,1]$. Risk funksiyasının dəqiq forması oyunçular arasındakı qarşılıqlı asılılıq modelinə görə müəyyən edilir. Ədəbiyyatda qarşılıqlı asılılığın müxtəlif modelləri təklif edilmişdir. Qarşılıqlı asılılığın ümumi modelində f_i risk funksiyası fərziyyələr çoxluğunu ödəyən ixtiyari funksiya ola bilər. Geniş yayılmış fərziyyə ondan ibarətdir ki, təhlükəsizlik investisiyaları hər bir oyunçu üçün müsbət, lakin azalan mükafat nümayiş etdirir. Müsbət nəticələr (yəni ciddi azalan risklər) oyunçular arasında xarici müsbət təsirləri modelləşdirir: əgər bir oyunçu İnT-nə öz investisiyalarını artırırsa, onda hər bir oyunçu udur. Azalan fayda (yəni risk funksiyasının qabarıqlığı) investisiya təhlükəsizliyi investisiyalarının azalan limit faydalılığını modelləşdirir, bu hamılıqla qəbul olunmuş fərziyyədir. Formal olaraq, aşağıdakı fərziyyələri müəyyən edək:

Fərziyyə 1: hər bir i üçün $fi(\cdot)$ funksiyası diferensiallanandır və bütün xj-lar üzrə azalır: $\frac{\partial f_i(\boldsymbol{x})}{\partial x_j} < 0, \forall i, j.$

Fərziyyə 2: hər bir i üçün $fi(\cdot)$ funksiyası bütün xj-lar üçün ciddi qabarıqdır: $\frac{\partial^2 f_i(\boldsymbol{x})}{\partial x_j^2} > 0, \forall i, j.$

Oyunçu i-nin məqsədi – özünün aşağıdakı kimi müəyyən edilən u_i faydalılıq funksiyasını maksimallaşdırmaqdır:

$$u_i(\mathbf{x}) = -L_i x_i + C_i x_i - t_i\ , \qquad (5.2.2)$$

burada: L_i – İnT insidenti baş verdikdə oyunçu i-nin potensial itkiləri, C_i – oyunçu i-nin investisiyalarının (xüsusi) dəyəridir, t_i – 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.

Oyunçular barədə aşağıdakı fərziyyələri edirik:

Fərziyyə 3: bütün oyunçular rasional hərəkət edirlər və öz investisiya səviyyələrini öz faydalılıq funksiyalarını maksimallaşdırmaq üçün seçirlər.

Fərziyyə 4: i oyunçusunun C_i qiymətləri və $f_i(\cdot)$ funksiyası onun konfidensial məlumatlarıdır.

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 İnT investisiyalarının optimal vektoru sosial rifahı maksimallaşdıran və Koordinator tərəfindən həll edilən aşağıdakı məsələnin həlli kimi tapılır:

$$\max_x \sum_{i=1}^{n} u_i(x) \tag{5.2.3}$$

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

$$\sum_{i=1}^{n} C_i x_i \leq B, \tag{5.2.4}$$

Fərziyyə 2-yə görə, (5.2.3)-(5.2.4) məsələsi üçün yeganə x* sosial-optimal investisiya profili mövcuddur. Qeyd edildiyi kimi, L_i, C_i əmsalları və f_i risk fuksiyaları oyunçuların konfidensial informasiyasıdır, Koordinator bu informasiya barədə məlumatlı deyil və buna görə (5.2.3)-(5.2.4) məsələsini həll edə bilməz. Eyni zamanda, x* həllini axtarmaq üçün oyunçuların da yetərli informasiyası yoxdur, onların məqsədləri öz faydalılıq funksiyalarını maksimallaşdırmaqdır.

Buna görə bizim məqsədimniz Koordinator tərəfindən yerinə yetirilən elə koordinasiya mexanizmi tapmaqdan ibarətdir ki, induksiya olunmuş qarşılıqlı asılı təhlükəsizlik oyununun tarazlığı (5.2.3)-(5.2.4) məsələsinin həlli olsun.

Fərziyyə 4 səbəbindən baxılan oyun natamam informasiyalı oyundur. Bu oyunda Heş tarazlığını iterativ prosesin yığılma nöqtəsi kimi interpretasiya etmək olar, bu prosesdə hər bir oyunçu öz hərəkətlərini hər bir iterasiyada digər oyunçuların davranışlarını müşahidə etməsi əsasında o vaxta kimi korreksiya edir ki, birtərəfli kənarlaşmalar daha faydalı olmur [240, s. 1-8].

Sosial-optimal həllin reallaşdırılması üçün koordinasiya mexanizmi

Bu bölmədə (5.2.3)-(5.2.4)-ün sosial cəhətdən optimal həllini reallaşdıran koordinasiya mexanizmi təqdim edilir. Bunu etmək üçün Koordinator üçün Fərziyyə 4 zəiflədilir, yəni fərz edilir ki, oyunçular bu konfidensial məlumatları digər oyunçulara açıqlamamaq şərtilə Koordinatora təqdim edirlər. Bu fərziyyə üçün əsas dövlət orqanlarının İnT üzrə statistik hesabatlarını səlahiyyətli dövlət orqanına təqdim etmələri üçün qanunvericilik tələbləri ola bilər [52, s. 41]. Bu halda, Koordinator məsələni tam informasiya ilə həll edəcək və bu oyun üçün Neş tarazlığını tapa bilər.

Koordinasiya mexanizmi aşağıdakı addımların əsasında həyata keçirilir:

- hər bir oyunçu i öz konfidensial məlumatlarını Koordinatora bildirir;
- hər bir oyunçu özünün s_i cari təhlükəsizlik səviyyəsini Koordinatora bildirir.

Hər bir zaman addımında:

1. Koordinator (5.15) məsələsini həll edir və investisiyaları qlobal optimal $\hat{x}_i, i = 1,2, \dots, n$ səviyyələrini tapır; Koordinator hər bir i oyunçusuna onun özü ilə birlikdə qonşularının $B_i = \hat{x}_i + \sum_{j \in N^i} \hat{x}_j$ ümumi büdcəsini, təhlükəsizliyin orta səviyyəsini $\bar{s}_i = \frac{1}{|N^i|} \sum_{j \in N^i} s_j$, oyunçunun qonşularının investisiyalarının $\bar{x}_i = \frac{1}{|N^i|} \sum_{j \in N^i} x_j$ orta səviyyəsini, həmçinin bütün sistem üzrə investisiyaların $\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i$ orta səviyyəsini göndərir.
2. Hər bir i oyunçusu özünün s_i İnT səviyyəsini, özü ilə birlikdə qonşularının ümumi B_i büdcəsini və qonşularının ortalama verilənlərini nəzərə almaqla (5.2.3)-(5.2.4) məsələsini həll edir, özünün $x_i, x_j^i, j \in N^i$ investisiyalar profilini Koordinatora göndərir.
3. Koordinator cərimələri müəyyən edir və onu oyunçulara bildirir, cərimənin miqdarı oyunçunun investisiyalar profili ilə Koordinatorun uyğun investisiya profillərinin fərqləri cəminə bərabərdir.

Beləliklə, dövlət orqanlarında İnT üzrə investisiyaların koordinasiyası üçün işlənmiş qarşılıqlı asılı oyun modelinin sosial cəhətdən optimal həlli üçün müvafiq koordinasiya mexanizmi təklif edilmişdir. Qarşılıqlı asılı təhlükəsizlik oyununun

iştirakçılarının eqoist olduqları, lakin Koordinatora düzgün məlumat verdikləri fərz olunur. Onlar İnT səviyyəsi daxil olmaqla, öz təhlükəsizlik parametrləri haqqında Koordinatora düzgün məlumat verirlər. Gələcəkdə oyunçuların düzgün məlumat vermədikləri halı üçün auksion nəzəriyyəsi və Markov qərar qəbulu prosesləri əsasında stimullaşdırma mexanizmlərinin işlənməsi planlaşdırılır.

5.3. İnformasiya təhlükəsizliyi sahəsində beynəlxalq koalisiya modeli

Kibertəhlükəsizliyin təmin edilməsi adətən koalisiya tələb edir, ayrılıqda götürülmüş istənilən ölkə bu sahədə öz məqsədlərinə tam çata bilmir və bu məsələnin həlli üçün digər ölkələrlə kooperasiya etməyə məcburdur. Lakin bu strateji məsələdə ölkələrin əməkdaşlığı sahəsində iqtisadi, siyasi və milli təhlükəsizlik riskləri mövcuddur [23, s.14]. Ölkələr bu riskləri nəzərə almaqla İnT sahəsində öz məqsədlərinə nail olmaq üçün uyğun ölkələrlə qarşılıqlı faydalılıq əsasında koalisiyalar formalaşdırmağa cəhd edirlər [85, s.241]. Fərz olunur ki, müəyyən ölkələrin İnT sahəsində maraqlarının münaqişəsi antaqonist deyil, onların arasında bu sahədə qarşılıqlı öhdəlik olan sazişlərin bağlanması mümkündür və ölkələr koalisiyadan əldə etdikləri faydanı bölə bilərlər.

Bu bölmədə kooperativ oyunlar nəzəriyyəsi [238, s.417] əsasında İnT sahəsində ölkələr arasında beynəlxalq koalisiyanın formalaşdırılması modeli təklif edilir [23].

Məsələnin qoyuluşu

Məlumdur ki, İnT-ni təmin etmək üçün müxtəlif İnT funksiyaları (servisləri, xidmətləri) istifadə edilir. Məsələn, biometrik identifikasiya sistemləri, antivirus sistemləri, təhlükəsizlik tələblərinə uyğunluq üzrə sertifikatlaşdırılmış əməliyyat sistemləri və müxtəlif tətbiqi proqram təminatı, CERT-komandaları, kibertəhlükəsizlik təlimləri və s. Belə xidmətlərin zəruri zəmanətlərlə ölkə səviyyəsində reallaşdırılması həm böyük resurslar, həm də uzun zaman müddəti tələb edir və çox zaman ayrıca bir dövlətin onu təklikdə reallaşdırması qeyri-real olur və ya bir çox risklərlə müşayiət olunur.

Fərz edək ki, hər hansı dövlət müəyyən İnT xidmətini (tədbirini) müəyyən (məsələn, regional) dövlətlər qrupu ilə birgə reallaşdırmaq istəyir. (Qeyd edək ki,

vaxtaşırı belə real təşəbbüslər olur.) Məsələn, Çin, Yaponiya və Cənubi Koreya 2003-cü ildə birlikdə Linux əməliyyat sisteminin ümumi istifadə üçün versiyasını yaratmaq sahəsində təşəbbüs göstərmişdilər [23, s.14]. Aydındır ki, İnT funksiyasının reallaşdırılması ölkələrdən müəyyən xərclər tələb edir və reallaşdırılan funksiyadan istifadə etməklə ölkələr müəyyən fayda əldə edirlər. Aşağıda danışıqlar yolu ilə ortaq İnT xidmətinin reallaşdırılması üçün koalisiyanın formalaşdırılmasını, xərclərin və uduşun koalisiya ölkələri arasında bölgüsünü koalisiya oyunları əsasında modelləşdirən yanaşma təklif edilir.

Koalisiyaların formalaşdırılması modellərinin icmalı

Koalisiyaların (və ya alyansların) formalaşdırılması problemləri bir çox nəzəri və praktiki tətbiq sahəsində – iqtisadiyyat, politologiya, hərb elmi, sosiologiya, təhlükəsiz simsiz rabitə, multi-agent sistemləri, robototexnika və s. meydana çıxır [23]. Hazırda mövcud koalisiyaların formalaşdırılması metodları və yanaşmalarını iki qrupa ayırmaq olar [122, s. 239]:

- Bütün iştirakçıların tam məlumatlı olduğu şəraitdə koalisiyaların formalaşdırılması metodları;
- Qeyri-müəyyənlik şəraitində koalisiyaların danışıqlar əsasında formalaşdırılması metodları.

Münaqişəli situasiyanın bütün iştirakçılarının məqsədləri, resursları və strategiyaları haqqında bütün maraqlı tərəflərin tam məlumatlı olması halında, bütün oyunçuların rasional və intellektual davranışı şərtində və koalisiyanın əldə etdiyi uduşun bölgüsü mümkün olduqda koalisiyanın formalaşdırılması strategiyasının seçilməsinin kooperativ oyunlar nəzəriyyəsində alınmış ciddi analitik həlli var [238].

Qeyri-müəyyənlik şəraitində koalisiyalar maraqlı tərəflər arasında danışıqlar yolu ilə yaradılır. Burada tərəflər arasında kompromis həllər tapmaq yolu ilə hər bir tərəfin koalisiyanın yaradılmasındakı motivasiyasının dayanıqlığı təmin edilir.

Koalisiyaların formalaşdırılması metodlarının inkişafında maraqlı töhfə multi-agent sistemləri çərçivəsində avtonom intellektual agentlər arasında koalisiyaların qurulması metodlarının işlənməsi olmuşdur [263, s.231]. Multi-agent sistemi öz

aralarında ünsiyyət saxlayan intellektual agentlər çoxluğundan ibarətdir. Agentlər bir agentin təklikdə həll etməsi qeyri-mümkün olan mürəkkəb məsələlərin həlli üçün koalisiyalar yaradırlar.

Koalisiyaların formalaşdırılması modellərinin bir qrupu da koalisiya resurs oyunlarıdır [131, s.589]. Bu kooperativ oyunlarda oyunçulardan hər biri müəyyən resurslara malikdir və onlar birlikdə müəyyən məqsədlər çoxluğunu həyata keçirmək istəyirlər. Koalisiya resurs oyunlarının mümkün həllərində koalisiya üzvləri müəyyən məqsədləri əldə etməyi öhdələrinə götürürlər və öz resurs bazasından müəyyən hissəni təqdim edirlər. Müxtəlif mümkün variantlar içərisindən agent eləsini seçir ki, onun məqsədi əldə edilsin və bu zaman öz xərcləri (təqdim etdiyi resursların həcmi) minimal olsun. Məsələ kooperativ oyunlar baxımından həll edilir, buna görə aşağıdakı suallara cavab axtarılır: hansı koalisiyalar formalaşacaq və agentlərin müxtəlif nəticələrə üstünlük vermələri halında bu koalisiyalar mümkün nəticələrdən hansını seçəcək?

Qeyd edək ki, koalisiya oyunlarında müxtəlif üzvlük qaydaları ola bilər [195, s. 383-393], məsələn, açıq üzvlük, ekskluziv üzvlük, eyni vaxtda bir neçə koalisiyaya üzv olmaq və s. Müxtəlif üzvlük qaydaları ilə koalisiya strukturlarının tarazlığı məsələsinin [140, s.389]-də sistematik müqayisəsi aparılır.

Koalisiya oyunları haqqında

Ümumi şəkildə deyilsə, oyun oyunçulardan (qərar qəbul edənlərdən) ibarətdir, hər bir oyunçunun strategiyaları var, növbə ilə hər bir oyunçu strategiyalarından birini seçməklə gediş edir və oyunun nəticəsindən özünün məmnunluq səviyyəsini müəyyən faydalılıq (uduş) funksiyası ilə ölçür. Hər bir oyunçunun məqsədi öz uduşunun gözlənilən qiymətini maksimallaşdırmaqdır. Antaqonist olmayan münaqişələrdə oyunçular arasında qarşılıqlı öhdəlik olan sazişlərin bağlanması (koalisiyaların formalaşdırılması) və uduşların oyunçular arasında yenidən bölünməsi mümkündür.

Xarakteristik formada koalisiya oyunu oyunçular çoxluğu N və oyunçular çoxluğunun altçoxluqlarında – mümkün koalisiyalarda müəyyən edilən xarakteristik

funksiya ilə müəyyən edilir. Xarakteristik funksiyanın qiyməti koalisiyanın uduşunu müəyyən edir [238, s.417].

Xarakteristik formada koalisiya oyunlarında uduşun koalisiya üzvləri arasında bölünməsindən asılı olaraq koalisiya oyunlarının iki növünə: qazancı transfer edilən (ing. transferable-utility) və qazancı transfer edilməyən (ing. nontransferable-utility) oyunlara baxırlar. Qazancıı transfer edilən kooperativ oyunlarda koalisiyanın dəyəri (qiyməti) bir həqiqi ədəd ilə ifadə edilir, onu koalisiyanın uduşuna uyğun olaraq, koalisiya üzvləri arasında onların məqbul gördükləri istənilən üsulla bölmək olar və qazancı koalisiya üzvləri arasında ötürmək (transfer etmək) olar. Mövcud işlərin çoxunda transfer edilən qazanc nəzərdə tutulur. Lakin bəzi sahələrdə qazancı iştirakçılar arasında transfer etmək mümkün deyil. Məsələn, tutaq ki, müxtəlif ölkələrin alimləri birgə məqalə üzərində işləyirlər, onların təqdim etdikləri resurslara onların təcrübəsi və biliyi daxildir. Belə resursları qiymətləndirmək asan deyil və məqalə çap edildikdə bir alimin əldə etdiyi faydanı (məsələn, vəzifədə irəliləyiş) əməkdaşlıq etdiyi həmkarlarına ötürməsi, adətən, mümkün deyil. Bu bölmədə baxılan məsələdə qazancın transfer edilən olması fərz edilir.

Koalisiya oyunlarının Şepli vektoru, özək (ing. core), nüvə (ing. nucleolus) və s. kimi həll metodları məlumdur [238, s.417, 195].

Koalisiyanın qurulması prosesi

Adətən, koalisiyaların formalaşdırılması bir neçə mərhələdə həyata keçirilir. Müəyyən məsələdə koalisiyanın təşəbbüskarı olan ölkə (və ya bir neçə ölkə) digər ölkələrlə koalisiya qurulması barədə danışıqlar aparır. Beynəlxalq ticarət sahəsində təcrübə [244, s. 34-53] və tədqiqatlar [232, s.45] göstərir ki, iştirakçı aktorların sayı çox olduqca koalisiyaların meydana çıxması daha ehtimallı olur. Daha böyük gücə malik aktorlar bir-biri ilə koalisiya yaratmağa meyilli olurlar. Aktor nə qədər güclüdürsə, o, digər aktorlarla bir o qədər az halda koalisiya yaradır. Dövlətlərin bir çox məsələdə öz coğrafi qonşuları ilə koalisiya yaratmaları daha ehtimallıdır. Nəhayət, koalisiyanın gücü böyük olduqca, digər ölkələrin bu koalisiyaya qoşulması ehtimalı da böyük olur.

Ölkələr arasında İnT sahəsində koalisiyanın formalaşdırılması üçün aşağıda üç mərhələli proses təklif edilir. Bu üç mərhələli koalisiya qurulması modeli ekologiya üzrə beynəlxalq sazişlərə həsr olunmuş əksər ədəbiyyatda təsvir edilən koalisiya formalaşdırılması proseslərinə oxşardır. Aşağıda təklif edilən koalisiyanın formalaşdırılması prosesi beynəlxalq ictimai rifah üçün [206, s.1335]-da irəli sürülmüş ideyanın modifikasiyasıdır və üçmərhələli oyun formasında ifadə edilir.

Tutaq ki, n ölkə var və bütün ölkələr çoxluğunu $N = \{1,2,\dots,n\}$ ilə işarə edək. Nəzərdə tutulan ortaq İnT xidmətləri üçün $P \subseteq N$ koalisiyasının yaradılması aşağıdakı mərhələlərdən ibarətdir.

1. *İştirak mərhələsi.* Birinci mərhələdə ölkələr eyni vaxtda və asılı olmadan P koalisiyasına qoşulmaq və ya qoşulmamaq (sinqlton oyunçu olmaq) barədə qərar qəbul edirlər. Əgər ən azı üç ölkə bu barədə qərar qəbul edirsə, onlar ikinci mərhələdə baş tutacaq danışıqların "iştirakçıları" adlanırlar.

2. *Danışıqlar mərhələsi.* İştirakçılar koalisiyanın həqiqətən də həyata keçirilməsi barəsində danışıqlar aparırlar. Danışıq iştirakçıları ikinci mərhələdə onu tərk edə və ya danışığa yeni iştirakçılar qoşula bilməzlər. Təklif edilən modeldə qərarlar majoritar qaydada qəbul edilir. Ölkələr koalisiya razılaşmasının lehinə və ya əleyhinə səs verirlər. Əgər koalisiyanın həyata keçirəcəyi ortaq İnT xidməti və bu fəaliyyət üçün tələb edilən ümumi büdcə barəsində danışıqlarda razılıq əldə olunursa, onda danışıq iştirakçıları koalisiya iştirakçısına (üzvünə) çevrilirlər. $i \in P$ ölkələri koalisiya iştirakçıları, $j \notin P$ ölkələri isə iştirak etməyən ölkələr adlanırlar.

3. *Koalisiya rifahına töhfənin və koalisiya uduşunun bölgüsü mərhələsi.* Bu mərhələdə koalisiyanın iştirakçısı olan ölkələr eyni vaxtda və asılı olmadan, özlərinin koalisiya rifahına vermək istədikləri töhfənin ümumi payı və koalisiya uduşundan əldə etmək istədikləri pay barədə qərar qəbul edirlər. Bu kəmiyyətlər növbəti bölmədə izah olunurlar.

Koalisiyanın üzvlərinin uduş funksiyaları. Ölkələrin uduş funksiyalarını müəyyən etmək lazımdır. *i*-ci ölkənin uduş funksiyasını (*Ui*) onun xərcləri (*Ci*) və koalisiyadan əldə etdiyi fayda (*Bi*) vasitəsilə ifadə etmək olar:

$$U_i = B_i - C_i, \qquad (5.3.1)$$

Faydalılıq (ing. utility) funksiyasının standart xassələrə malik olduğunu fərz edirik, yəni iki dəfə kəsilməz diferensiallanandır, kvazi-qabarıqdır və ciddi monoton artandır.

Tutaq ki, koalisiyanın bütün qazancı B funksiyası ilə təsvir olunur. Ümumi qazancın ölkələr arasında bölgüsünü göstərmək üçün $\alpha_i \in (0;1)$ parametrini daxil edək, burada: α_i – i-ci ölkənin ümumi qazancdan pay bölgüsüdür və $\sum_{i\in N} \alpha_i = 1$. Koalisiyadakı i-ci ölkə bu qazancın α_i hissəsini alır, yəni $B_i(G, \alpha_i) = \alpha_i B(G)$.

Təklif edilən koalisiya oyununda ümumi uduş iki mənbədən formalaşır. Koalisiya çərçivəsində reallaşdırılan İnT funksiyasından koalisiya ölkələrinin dövlət və ictimai orqanları, özəl təşkilatları və vətəndaşları istifadə edəcək. Bu funksiyanın istifadə xarakterindən asılı olaraq onu müəyyən mənada ictimai dövlət xidməti (ing. public goods) və özəl xidmət (ing. private goods) kimi interpretasiya etmək olar [94, s. 101]. Uduşun birinci mənbəyi kimi istehlak edilən ictimai və ya özəl xidmətin ümumi dəyərini götürmək olar.

Uduşun ikinci mənbəyi baxılan İnT funksiyasının reallaşdırılması sayəsində ölkələrin müvafiq texnologiyalar sahəsində müstəqilliyinin və milli maraqlarının təmin edilməsidir. Bu cəhəti də uduş kimi qiymətləndirmək 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 daxil etmək olar. Koalisiyanın ümumi büdcəsi G olsun. i-ci ölkə koalisiyanın fəaliyyəti üçün $g_i = t_i G$ büdcəsi verir. Aydındır ki, $G = \sum_{i\in N} g_i$.

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

$$U_i(G, g_i, \alpha_i, n_i) = \alpha_i B(G) - C(g_i) - S(n_i), \qquad (5.3.2)$$

burada: n_i – i-ci ölkənin koalisiyanın təqdim etdiyi İnT xidmətindən istifadə edən istifadəçilərinin sayı, $S(n_i)$ – i-ci ölkənin bu xidmətdən istifadə üçün çəkdiyi xərclərdir.

Uduş funksiyasını Kobb-Duqlas funksiyası şəklində vermək məqsədəuyğundur. Hələlik bu işdə uduş funksiyası ümumi şəkildə verilir və tarazlıq nöqtəsinin varlığını təmin etmək üçün onun bəzi xassələrə malik olması fərz olunur.

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

Koalisiyanın dayanıqlığı

Koalisiya oyunlarında vacib məsələ koalisiyanın dayanıqlığıdır. Koalisiyalar o zaman dayanıqlı olur ki, hər bir koalisiya üzvünün koalisiyadakı uduşu koalisiyada olmadan hərəkət etdikdə onun fərdi uduşundan böyük olsun (*fərdi rasionallıq şərti*).

Koalisiyanın dayanıqlığı koalisiya uduşunun oyunçuların imtina edə bilmədikləri bölgüsü ilə təmin edilir. Ədalətli bölgü oyunçuların digər koalisiyaya keçmək stimullarının qarşısını alır, yəni koalisiyanın dayanıqlığını təmin edir.

Tədqiqatlarda müxtəlif dayanıqlıq konsepsiyaları irəli sürülür, məsələn:

- daxili dayanıqlıq (koalisiya üzvünün koalisiyanı tərk etmək stimulu yoxdur);
- xarici dayanıqlıq (koalisiyada olmayanın koalisiyaya qoşulmaq üçün stimulu yoxdur);
- koalisiyanın rentabelliyi (koalisiya hər bir üzv üçün koalisiya olmadığı haldakından daha yaxşıdır).

Bu işdə koalisiyanın xarici və daxili dayanıqlığı məsələsinə baxılır. Tutaq ki, $P\backslash\{i\}$ ilə iştirakçı ölkə i koalisiyanı tərk etdikdə qalan koalisiya, $P\cup\{j\}$ ilə isə iştirakçı olmayan j koalisiyaya birləşdikdə yaranan koalisiya işarə edilib.

(5.3.2) düsturuna daxil olan funksiyaların üzərinə aşağıdakı şərtlər qoyulur:

a) $B'(\cdot) > 0,\ B''(\cdot) \leq 0$; b) $C'(\cdot) > 0,\ C''(\cdot) > 0$; c) $S'(\cdot) > 0,\ S''(\cdot) > 0$.

Texniki baxımdan a-c fərziyyələri çökük qazanc və qabarıq xərc funksiyaları haqqında standart fərziyyələri əks etdirir. Xərc funksiyaları (C və S) ciddi qabarıq fərz olunurlar ki, tarazlıq nöqtəsinin yeganəliyi təmin edilsin.

P koalisiyası qurulduqdan sonra $g^*(P)$ tarazlıq vektoru və $\alpha^*(P)$ tarazlıq vektoru P koalisiyası və P-də olmayan bütün oyunçular arasında Neş tarazlığı kimi

tapılır. Mərhələ 3-ü 3a və 3b mərhələlərinə bölmək olar. 3b mərhələsində $\alpha^*(P)$ tarazlıq vektoru yenə də P ilə qalan oyunçular arasında Neş tarazlığı kimi təyin edilir. 3b mərhələsində seçilmiş $\alpha^*(P)$ tarazlıq vektoru 3a mərhələsində seçilmiş g^* tarazlıq vektorundan asılı olacaq, bu vektor isə öz növbəsində, 1-ci mərhələdə seçilmiş P koalisiyasından asılıdır. Deməli, 3b mərhələsi üçün $\alpha^*(g(P))$ yaza bilərik. Bunu (1) uduş funksiyasında yazsaq, 3a mərhələsində uduşllar yalnız g_i-nin funksiyası olacaq. Bu bizə 3a mərhələsində məsələni $g^*(P)$ üçün həll etməyə imkan yaradır.

Hər bir mümkün P koalisiyası üçün yeganə tarazlıq vektorunun varlığı arzu olunur. Bu bizə $U_i^*(g(P))$ əvəzinə $U_i^*(P)$ yazmağa imkan verərdi. Hələlik varlıq və yeganəlik üçün kafi şərtlərə baxmasaq da, bu fərziyyədən istifadə edərək işarələməni sadələşdirə və dayanıqlı P^* koalisiyasını aşağıdakı kimi təyin edə bilərik:

$$\text{Daxili dayanıqlıq: } U_i^*(P^*) \geq U_i^*(P^* \backslash \{i\}) \; \forall i \in P^* \qquad (5.3.3)$$

$$\text{Xarici dayanıqlıq: } U_j^*(P^*) \geq U_j^*(P^* \cup \{j\}) \; \forall j \notin P^*, \qquad (5.3.4)$$

Aydındır ki, daxili və xarici dayanıqlıq şərtləri birinci mərhələdə üzvlük strategiyalarında de fakto Neş tarazlığı müəyyən edir. P^* koalisiyasına qoşulmağı elan etmiş hər bir $\boldsymbol{i}$ oyunçusunun P^*-ni tərk etməyə (birtərəfli) stimulu yoxdur. Eyni zamanda, P^*-yə qoşulmamağı qərara alan hər bir j oyunçusunun da öz strategiyasını dəyişərək P^* koalisiyasına qoşulması üçün stimulu olmamalıdır.

V fəsil üzrə nəticələr:

- E-dövlətdə İnT-nin ikisəviyyəli iyerarxik idarəetmə sistemlərində investisiyaların sosial baxımdan optimal paylanmasının nəzəri oyun modeli təklif edilmişdir [52];
- E-dövlətin İnT üzrə koordinasiya sisteminin multi-agent şəbəkə modeli qurulmuş və koordinasiya sisteminın operativliyinin və effektivliyinin qiymətləndirilməsi üçün bir sıra sosial şəbəkə analizi indeksləri təklif edilmişdir [17];
- İnformasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması problemlərini analiz etmək üçün kooperativ oyunlar əsasında nəzəri-oyun modeli təklif edilmişdir [23].

VI FƏSİL. E-DÖVLƏTİN İNFORMASIYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ ÜZRƏ QƏRARLARIN QƏBUL EDİLMƏSİ MODELLƏRİ

Proses yanaşması idarəetməyə qarşılıqlı əlaqəli idarəetmə funksiyalarının fasiləsiz ardıcıllığı kimi baxır. Sistemli yanaşmada e-dövlətə dəyişən xarici mühit şəraitində müxtəlif məqsədlərə nail olunmasına yönəldilən insanlar, strukturlar, məsələlər və texnologiyalar kimi qarşılıqlı əlaqəli elementlərin toplusu kimi baxılır. Bu elementlərin qarşılıqlı təsirini öyrənmək üçün qeyri-səlis koqnitiv modelləşdirmədən istifadə etməklə e-dövlətin İnT-nin strateji idarə edilməsi üçün koqnitiv model qurmaq və bu model əsasında e-dövlətin İnT-nin idarə edilməsinin müxtəlif strategiyalarının nəticələrini analiz etmək mümkündür [54, s.440].

İdarəetməyə situasiya yanaşması o fikirdən çıxış edir ki, müxtəlif idarəetmə metodlarının yararlılıq dərəcəsi yaranmış situasiya ilə müəyyən edilir. Situasiya verilmiş konkret zamanda obyektin fəaliyyətinə əhəmiyyətli dərəcədə təsir göstərən hadisələrin (şəraitlərin) konkret toplusudur. Həm obyektin daxilində, həm də onu əhatə edən mühitdə mövcud faktorların sayı o qədər çoxdur ki, obyektin idarə edilməsinin vahid «ən yaxşı» üsulu yoxdur. Konkret situasiyada ən effektiv metod verilmiş situasiyaya daha uyğun olan situasiyadır və e-dövlətin İnT-nin idarə edilməsi üçün belə situasiyaların seçilməsinə presedentlər nəzəriyyəsi əsasında yanaşma təklif edilir [53, s.24].

6.1. E-dövlətin informasiya təhlükəsizliyi üzrə strateji qərarların qəbul edilməsinin qeyri-səlis koqnitiv modeli

Qeyd edildiyi kimi e-dövlətin İnT-nin idarə edilməsi zəif strukturlaşdırılmış məsələlər sinfinə aiddir [7, s.3]. Belə sistemlərin analizi və idarə edilməsi üçün hazırda koqnitiv yanaşma geniş tətbiq edilir, o qarşılıqlı əlaqəli faktorların sayı çox olduqda hadisələrin inkişaf məntiqini görməyə və başa düşməyə imkan verir [152, s.1-22, 62].

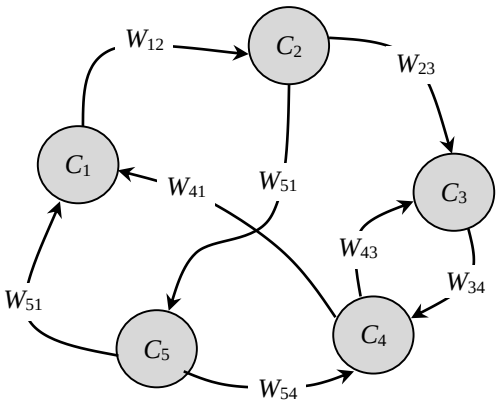
Bu bölmədə qeyri-səlis koqnitiv xəritələr (Fuzzy Cognitive Map, FCM) əsasında e-dövlətin İnT-nin strateji idarə edilməsinin koqnitiv modeli təklif edilir [54, s.440]. Təklif edilən koqnitiv modelləşdirmə yanaşması qərar qəbulunu intellektual

dəstəkləmə sistemlərinin yaradılması kontekstində perspektivlidir və onun tətbiqi e-dövlətin İnT-nin təmin edilməsi sahəsində strateji idarəetmənin effektivliyini və qəbul edilən qərarların keyfiyyətini əhəmiyyətli dərəcədə yüksəldə bilər.

Qeyri-səlis koqnitiv xəritələr. Koqnitiv xəritələr ilk dəfə amerikan psixoloqu E.Tolman tərəfindən təklif edilmişdi [54, s.440]. Labirintlərin müxtəlif növlərində siçovulların öyrədilməsi eksperimentləri əsasında Tolmen nəticəyə gəlmişdi ki, ətraf mühitlə qarşılıqlı təsir prosesində siçovulda labirintin bütün xarakteristikalarının «koqnitiv xəritəsi» və ya «fikir planı» formalaşır, mühitlə hər sonrakı qarşılıqlı təsirdə «xəritə» təkmilləşir.

Koqnitiv xəritələr çox mürəkkəb davranışları modelləşdirə bilər. R. Akselrod siyasi elitaların qərarlarının strukturunu öyrənərkən çəkili koqnitiv xəritələri və funksional koqnitiv xəritələri tətbiq etmişdi [74, s.3-17]. Çəkili koqnitiv xəritələrdə təsirin istiqamətini və kəmiyyətini müsbət və ya mənfi ədədlə göstərirlər. Funksional koqnitiv xəritələrdə hər bir səbəb əlaqəsi funksiya ilə assosiasiya edilir.

B. Kosko qeyri-səlis xəritələri [207, s.65] koqnitiv xəritələrin qeyri-səlis genişlənməsi kimi təklif etmişdi. Əslində, qeyri-səlis koqnitiv xəritə (Fuzzy Cognitive Map, FCM) çəkiləri qeyri-səlis olan çəkili koqnitiv xəritədir. Adətən, koqnitiv xəritələr ekspertlərdən informasiya toplanması yolu ilə qurulur və ekspertlər isə özlərini kəmiyyət deyil, keyfiyyət terminləri ilə ifadə etməyə daha çox meyllidirlər. Bu baxımdan qeyri-səlis koqnitiv xəritələrin istifadə edilməsi daha məqsədəuyğundur, onlarda konseptlər müvafiq qeyri-səlis çoxluqlarla linqvistik olaraq təsvir olunur.



Şəkil 6.1.1. Qeyri-səlis koqniv xəritəyə misal

FCM qeyri-səlis məntiqin və neyron şəbəkələrin bəzi aspektlərini – qeyri-səlis məntiqin sağlam düşüncə qaydaları ilə neyron şəbəkələrinin öyrənmə evristikasını birləşdirir. Bu struktur çəkili istiqamətlənmiş qraf (şəkil 6.1.1) kimi təsvir olunur, bu qrafda təpələr predmet

sahəsinin təsvir olunduğu faktorlara uyğundur, tillər isə faktorlar arasındakı qarşılıqlı təsiri göstərir.

C_i faktoru ilə C_j faktoru arasında tilin çəkisi müsbət ola bilər, bu onu bildirir ki, C_i faktorunun qiymətinin artması (azalması) C_j faktorunun qiymətinin artmasına (azalmasına) gətirir. Əgər C_i ilə C_j arasında tilin çəkisi mənfidirsə, onda C_i faktorunun qiymətinin artması (azalması) C_j faktorunun qiymətinin azalmasına (artmasına) gətirir.

Son onillikdə tədqiqatçıların bir çox sahədə qeyri-səlis modellərin qurulmasına marağı artır [60, s.148, 253, s.82]. FCM metodologiyası biliklərin təsvirində, siyasi, sosial və sosial-iqtisadi tədqiqatlarda, strateji planlaşdırmada və qeyri-səlis şəraitdə strateji qərarların qəbulunda, iqtisadi proqnozlaşdırmada, IT-layihələrin idarə edilməsində, tibbi informatikada, ekologiyada, informasiya təhlükəsizliyində [60, s.148] və s. uğurla tətbiq edilmişdir.

E-dövlətin İnT-nin idarə edilməsinin koqnitiv modelləşdirilməsi üçün aşağıdakılar zəruridir:

1) İnT vəziyyətinə təsir edən faktorların müəyyən edilməsi;

2) Faktorların qarşılıqlı təsir matrisinin qurulması;

3) İnT-nin idarə edilməsinin koqnitiv modelinin qurulması;

4) Qurulmuş model üzərində e-dövlətin İnT-nin idarə edilməsinin mümkün startegiyalarının yoxlanması.

E-dövlətin İnT-nin idarə edilməsi faktorları

FCM biliklərin təsvirinin üsullarından biridir və onun qurulması üçün predmet sahəsi ekspertlərinin bilik və təcrübəsi istifadə edilməlidir. Ekspertlər predmet sahəsini daha yaxşı təsvir edən faktorları müəyyən edirlər. Əlamətlər, vəziyyətlər və ya sistem dəyişənləri faktor ola bilər. Ekspertlər hansı faktorların sistemin modelləşdirilməsi üçün əsas olduğunu və hansı faktorların bir-birinə (pozitiv və ya neqativ) təsir etməsini müəyyən edirlər.

E-dövlətin İnT-nin idarə edilməsinə təsir edən faktorları müəyyənləşdirmək üçün bir sıra ölkələrin milli kibertəhlükəsizlik strategiyaları, həmçinin beynəlxalq

təşkilatların model kibertəhlükəsizlik strategiyaları analiz edilmişdir [186, s. 25-34, 204, s. 24-43]. Bu strategiyalar aparıcı İnT mütəxəssisləri geniş cəlb edilməklə işlənmişdir və ekspert biliklərinin toplandığı yetərincə yaxşı mənbə hesab oluna bilər. Kibertəhlükəsizlik strategiyalarının analizi gedişində e-dövlətin İnT-nin idarə edilməsinə təsir edən bir sıra faktorlar müəyyən edilmişdir, onların siyahısı cədvəl 6.1.1-də verilir.

Cədvəl 6.1.1

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinə təsir edən faktorlar

Faktorlar	**Faktorların adı**	**İşarə**
C_1	Qanunvericilik tədbirləri	Legal
C_2	Təşkilati tədbirlər	Org
C_3	Texniki tədbirlər	Tech
C_4	Potensialın inkişafı	HR
C_5	Maraqlı tərəflərin əməkdaşlığı	Coop
C_6	İnformasiya təhdidlərinin inkişafı	NewT
C_7	E-dövlətin informasiya təhlükəsizliyinin səviyyəsi	ISec

Bu faktorların qısa təsvirinə baxaq.

1. Qanunvericilik tədbirləri – İnT-nin təmin edilməsi üçün adekvat normativ-hüquqi bazanın yaradılması zəruridir. Normativ-hüquqi bazaya zəruri siyasət və tənzimləmə mexanizmlərinin planlaşdırılması və işlənməsi, maraqlı tərəflərin rollarının, hüquq və vəzifələrinin dəqiq müəyyənləşdirilməsi, İnT-nin təmin edilməsi üzrə əsas tədbirlərin işlənməsi və s. aiddir. İnT insidentlərinin təhqiqatı mexanizmlərinin işlənməsi, cinayətlərə görə məhkəmə təqibi və cəzaların daxil edilməsi də nəzərdə tutulur.

Bu qrup aşağıdakı göstəricilərdən ibarətdir:

***C*₁₁:** Cinayət qanunvericiliyi;

***C*₁₂:** Tənzimləmə və standartların tələblərinə uyğunluq.

2. Təşkilati tədbirlər – kibertəhlükəsizlik startegiyalarında İnT-nin təmin edilməsinə yönəlmiş çevik təşkilati strukturun qurulması nəzərdə tutulur. Effektiv təşkilati strukturların yaradılması İnT-nin inkişafı, kibercinayətkarlıqla mübarizə, insidentlərin

monitorinqi, qarşısının alınması və cavablandırılması, yeni və mövcud təşəbbüslər arasında idarələrarası, sektorlararası və transsərhəd koordinasiya üçün zəruridir. Altqrup aşağıdakı göstəricilərdən ibarətdir:

***C*$_{21}$:** Siyasət (rəsmi İnT strategiyaları);

***C*$_{22}$**: İdarəetmə üzrə yol xəritəsi (İnT üzrə rəsmi idarəetmə planları);

***C*$_{23}$:** Məsul orqan (İnT agentlikləri);

***C*$_{24}$:** Milli qiymətləndirmə (rəsmən təyin olunmuş İnT səviyyəsinin ölçülməsi).

3. Texniki tədbirlər – texnologiyalar kibertəhdidlər üçün müdafiənin birinci xəttidir. Adekvat texniki tədbirlər və kiberhücumların aşkarlanması və qarşısının alınması üçün potensial olmadan e-dövlət və onun subyektləri kibertəhdidlərə qarşı dayanıqsız olurlar. Buna görə e-dövlətin proqram təminatı və informasiya sistemləri üçün minimal təhlükəsizlik meyarlarının və akkreditasiya sxemlərinin müəyyən edilməsi üzrə strategiyaları inkişaf etdirmək imkanı olmalıdır.

***C*$_{31}$:** Erkən xəbərdarlıq sistemi;

***C*$_{32}$:** Standartlar;

***C*$_{33}$:** Sertifikatlaşdırma.

4. Potensialın inkişafı – insan potensialının və institusional potensialın inkişafı ilk üç tədbir (qanunvericilik, texniki və təşkilati) üçün vacibdir. Texnologiyaların, risklərin və nəticələrin başa düşülməsi daha mükəmməl qanunvericiliyin, daha effektiv siyasət və startegiyaların işlənməsinə, müxtəlif rolların və vəzifələrin daha yaxşı təşkilinə kömək edir. Altqrup aşağıdakı göstəricilərdən ibarətdir:

***C*$_{41}$:** Kadr hazırlığı*;*

***C*$_{42}$:** Əhalinin məlumatlandırılması*;*

***C*$_{43}$:** Elmi tədqiqatlar və innovasiyalar;

***C*44:** Standartların işlənməsi;

***C*45:** Dövlət təşkilatlarının sertifikatlaşdırılması.

5. Maraqlı tərəflərin əməkdaşlığı – İnT-nin idarə edilməsi üçün bütün maraqlı tərəflərin (dövlət strukturları, özəl sektor və vətəndaşların) sıx əməkdaşlığı tələb edilir. Beynəlxalq əməkdaşlıq da həyati vacibdir, çünki hamı bir kiberfəzadan asılıdır. Altqrup aşağıdakı göstəricilərdən ibarətdir:

***C*$_{51}$:** Dövlətdaxili əməkdaşlıq;

***C*$_{52}$:** İdarələrarası əməkdaşlıq;

***C*$_{53}$:** Dövlət və özəl sektorun əməkdaşlığı;

***C*$_{54}$:** Beynəlxalq əməkdaşlıq.

6. İnT təhdidlərinin inkişafı – bu işdə aşağıdakı göstəricilərə baxılır:

***C*$_{61}$**: Təhdid aktorlarının inkişafı (insayderlər, haktivistlər, kibercinayətkarlar, strateji rəqiblər, düşmən dövlətlər);

***C*$_{62}$:** Yeni hücum növlərinin meydana çıxması;

***C*$_{63}$:** Hücum hədəflərinin inkişafı.

7. E-dövlətin informasiya təhlükəsizliyinin səviyyəsi – E-dövlətin İnT-nin səviyyəsinin inteqral qiymətidir, e-dövlətin əsas risk göstəriciləri əsasında müəyyən edilir. Risklərin müvafiq səviyyələrinə uyğun olaraq İnT-nin aşağıdakı üç səviyyəsinə baxmaq olar:

– İnT-nin yüksək səviyyəsi – riskin aşağı səviyyəsinə uyğundur;
– İnT-nin məqbul səviyyəsi – riskin yolverilən səviyyəsinə uyğundur;
– İnT-nin aşağı səviyyəsi – riskin yüksək səviyyəsinə uyğundur.

Faktorların qarşılıqlı təsir matrisinin qurulması

FCM-in qurulması zamanı ən mürəkkəb məsələ faktorların qarşılıqlı təsiri çəkilərinin təyin edilməsidir. Faktorların qarşılıqlı təsir matrisinin hesablanması üçün [276, s.83]-da iki alqoritm verilir. Birinci alqoritmdə 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 qiymətləndirmə obyekti haqqında bilik və təcrübələri müxtəlif ola bilər, buna görə hər bir ekspertə mənfi olmayan inam çəkisi təyin etmək olar. Ekspertlərin inam çəkiləri nəzərə alınmaqla qarşılıqlı təsir çəkilərinin aqreqasiya olunmuş qiymətləri aşağıdakı düsturla hesablana bilər (yalnız eyni işarəli çəkilər nəzərə alınır):

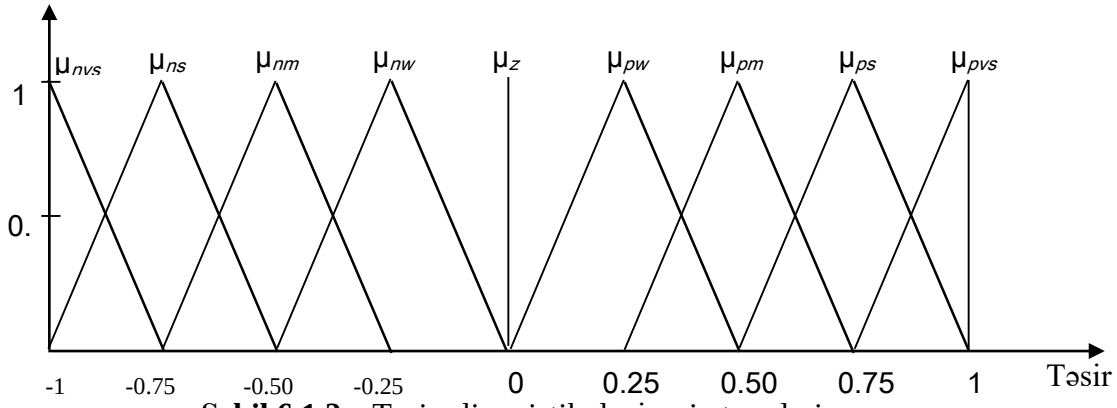
$$W_{ij} = \frac{\sum_{k=1}^{m} b_k w_{ij}^k}{m}, \qquad (6.1.1)$$

burada: w_{ij}^{k} – k-cı ekspertin C_i və C_j arasındakı qarşılıqlı təsir çəkisinə verdiyi qiymət; b_k – k-cı ekspertin inam çəkisi; m – ekspertlərin sayıdır. Əgər ekspertin qiymətləri əksər ekspertlərin qiymətlərindən fərqlənirsə, onda həmin ekspert cərimələnir – ona çox kiçik və ya sıfır inam çəkisi verilir. Bu alqoritmin təsviri ilə daha ətraflı tanış olmaq üçün [276, s.83]-ya müraciət etmək tövsiyə olunur.

FCM faktorlarının qarşılıqlı təsir matrisinin qurulması üçün ikinci alqoritm qeyri-səlis məntiqdən istifadə edir. Hər bir ekspert bir faktorun digər faktora təsirini «neqativ» və ya «pozitiv» kimi müəyyən edir və bundan sonra təsir dərəcəsini «güclü», «zəif» və s. kimi linqvistik dəyişənlərin köməyi ilə təsvir edirlər [54, s.440].

Bu metodologiyaya görə, bir faktorun digərinə təsiri [-1, 1] universal çoxluğunda qiymətlər alan linqvistik dəyişən kimi interpretasiya edilir. Onun termlər çoxluğu aşağıdakı kimi ola bilər [253, s.828]:

T(Təsir) = {neqativ çox güclü, neqativ güclü, neqativ orta, neqativ zəif, neqativ sıfır, pozitiv zəif, pozitiv orta, pozitiv güclü, pozitiv çox güclü}.



Şəkil 6.1.2. «Təsir» linqvistik dəyişənin termləri

Aşağıda semantik qayda müəyyən edilir və bu termlər mənsubiyyət funksiyaları şəkil 6.1.2-də göstərilmiş qeyri-səlis çoxluqlarla xarakterizə olunur:

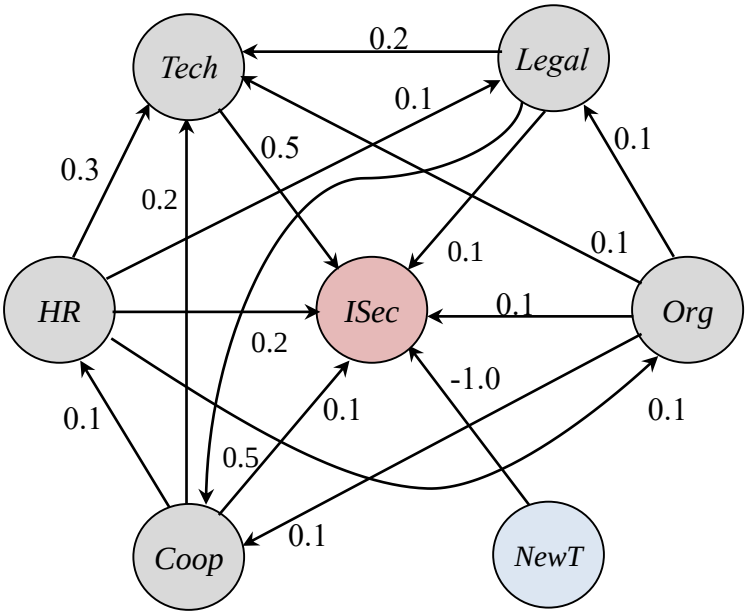
– T(Neqativ çox güclü) = «Təsir −75 %-dən aşağıdır» üçün μ_{nvs} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– T(Neqativ güclü) = «Təsir −75 %-ə yaxındır» üçün $\mu_{n}s$ mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;

– *T*(Neqativ orta) = «Təsir −50 %-ə yaxındır» μ_{nm} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(Neqativ zəif) = «Təsir −25 %-ə yaxındır» üçün μ_{nw} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(neqativ sıfır) = «Təsir 0-a yaxındır» üçün μ_z mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(Pozitiv zəif) = «Təsir 25 %-ə yaxındır» üçün μ_{pw} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(Pozitiv orta) = «Təsir 50 %-ə yaxındır» üçün μ_{pm} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(Pozitiv güclü) = «Təsir 75 %-ə yaxındır» üçün μ_{ps} mənsubiyyət funksiyası ilə qeyri-səlis çoxluq;
– *T*(Pozitiv çox güclü) = «Təsir 75 %-dən yüksəkdir» üçün μ_{pvs}. mənsubiyyət funksiyası ilə qeyri-səlis çoxluq.

Faktorların qarşılıqlı təsirlərini təsvir edən linqvistik dəyişənlər aqreqasiya edilir və ümumi linqvistik dəyişən defazzifikasiyanın köməyi ilə [-1, 1] intervalına çevrilir. Bu işdə defazzifikasiya üçün ağırlıq mərkəzi metodu istifadə edilir [102, s. 66].

Qeyri-səlis koqnitiv xəritələr də digər qeyri-səlis sistemlərinin əsas nöqsanlarına malikdir: onlar müstəqil öyrənməyi bacarmırlar. Müvafiq verilənlər olduqda neyron şəbəkələrinin öyrənmə mexanizmlərindən istifadə etməklə faktorların qarşılıqlı təsir çəkilərini yaxşılaşdırmaq olar. Belə yanaşmaların əksəriyyəti, məsələn Hebb öyrənmə metoduna əsaslanır, lakin evolyusion hesablamalardan istifadə edən yanaşmalar da mövcuddur [254, s.851].

E-dövlətin İnT-nin qeyri-səlis koqnitiv modelində faktorların qarşılıqlı təsir matrisini hesablamaq üçün İnT-nin idarə edilməsi üzrə beş ekspert cəlb edilmişdi. Ekspertlər faktorların bir-birinə təsirini yuxarıda müəyyən edilmiş linqvistik dəyişənlərlə qiymətləndirmişdilər və aqreqasiyadan və defazzifikasiyadan sonra alınmış nəticələr şəkil 6.1.3-də verilmişdir.



Şəkil 6.1.3. E-dövlətin İnT-nin idarə edilməsi üçün qeyri-səlis koqnitiv xəritə modeli

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

$$A_i^{(t+1)} = f\left(\sum_{j=1}^{n} w_{ij}A_j^{(t)}\right), i \neq j, \tag{6.1.2}$$

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.

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

$$f(x) = \frac{1}{1 + e^{-\lambda x}}, \tag{6.1.3}$$

burada: $\lambda > 0$. Bu funksiya kəsilməzdir və onun qiymətlər oblastı [0, 1] parçasıdır.

Fərz olunur ki, faktorların vəziyyətləri üç qeyri-səlis çoxluqdan ibarət olan qeyri-səlis dəyişənlər kimi müəyyən edilə bilər: Yüksək, Orta və Aşağı.

İnT-nin idarə edilməsinin müxtəlif strategiyalarının modeldə test edilməsi

Qeyd edək ki, hər bir *Cj* konsepti [0, 1] intervalından qiymətlər ala bilər, onu həm də «aktivləşdirmə səviyyəsi» adlandırırlar. Aktivləşdirmə səviyyəsini nisbi ədədlər kimi də interpretasiya etmək olar. Daha ciddi yanaşmada aktivləşdirmə səviyyəsini nisbi sayın linqvistik ölçüsünü təsvir edən qeyri-səlis çoxluqda mənsubiyyət kimi göstərmək olar (məsələn, aşağı, orta, yüksək) [207, s.65].

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 o deməkdir ki, baxılan faktor müəyyən iterasiyada sistemdə iştirak etmir, 1 qiyməti isə baxılan faktorun maksimal dərəcədə iştirak etdiyini bildirir. Digər qiymətlər aktivləşdirmə səviyyəsinin aralıq səviyyələrinə uyğun gəlir.

İnT-nin idarə edilməsinin aşağıdakı senarilərinin modelləşdirilməsinə baxaq.

A senarisi: *situasiyanın öz-özünə inkişafı* A(0) = (1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 0.0).

B senarisi: *yalnız texniki tədbirlərin tətbiqi* A(0) = (0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 0.0).

C senarisi: *«İnT təhdidlərinin inkişafı» faktorunun güclü aktivləşdirilməsi* A(0) = (0.0, 0.0, 0.0, 0.0, 0.0, 1.0, 0.0).

D senarisi: *«Potensialın inkişafı» və «İnT təhdidlərinin inkişafı» faktorlarının güclü aktivləşdirilməsi* A(0) = (0.0, 0.0, 0.0, 1.0, 0.0, 1.0, 0.0).

Hesablama eksperimentlərində $\lambda = 1$ parametri ilə siqmoid funksiyası istifadə edilmişdir. A senarisi üzrə hesablamalarda faktorların aralıq qiymətləri cədvəl 6.1.2-də verilib.

Cədvəl 6.1.2
FCM üçün stabil vəziyyətin hesablanması (A senarisi)

İterasiyalar	Legal	Org	Tech	HR	Coop	NewT	ISec
0	1.00	1.00	1.00	1.00	1.00	1.00	1.00
1	0.5498	0.5250	0.6457	0.5987	0.5498	0.5000	0.5987
2	0.5281	0.5150	0.5871	0.5619	0.5292	0.5000	0.5721
3	0.5269	0.5140	0.5821	0.5570	0.5275	0.5000	0.5633
4	0.5268	0.5139	0.5816	0.5566	0.5274	0.0000	0.5624
5	0.5267	0.5139	0.5816	0.5566	0.5274	0.5000	0.5624
6	0.5267	0.5139	0.5816	0.5566	0.5274	0.5000	0.5624

Cədvəl 6.1.2-dən göründüyü kimi, mövcud tendensiyaların saxlanması İnT-nin səviyyəsinin pisləşməsinə gətirir.

Cədvəl 6.1.3

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
İnT təhdidlərinin inkişafı	0.00	0.5000	0
İnT-nin səviyyəsi	0.00	0.6048	0.0424

Cədvəl 6.1.3-dən nəticəyə gəlmək olar ki, yalnız texniki tədbirlərin istifadə edilməsi İnT-nin səviyyəsinin əhəmiyyətli yaxşılaşmasına gətirmir (A və B senarilərinin stabil vəziyyətləri arasındakı fərq 0.0424-dür).

Cədvəl 6.1.4 göstərir ki, «İnT təhdidlərinin inkişafı» faktorunun aktivləşdirilməsi zamanı İnT-nin səviyyəsi əhəmiyyətli pisləşir, həmçinin «Texniki tədbirlər» faktorunun başlanğıc tendensiyasının pisləşməsini də qeyd etmək olar.

Cədvəl 6.1.4

C senarisi üzrə hesablamaların son nəticələri

Faktorlar	Başlanğıc qiymətlər –C senarisi	Son qiymətlər – C senarisi	A və C senarilərinin stabil vəziyyətləri arasındakı fərq
Qanunvericilik tədbirləri	0.00	0.5267	0.00
Təşkilati tədbirlər	0.00	0.5139	0.00
Texniki tədbirlər	0.00	0.5569	-0.0247
Potensialın inkişafı	0.00	0.5547	-0.0019
Maraqlı tərəflərin əməkdaşlığı	0.00	0.5267	-0.0007
İnT təhdidlərinin inkişafı	1.00	1. 00	0.5
İnT-nin səviyyəsi	0.00	0.4976	-0.0648

Cədvəl 6.1.5
D senarisi üzrə hesablamaların son nəticələri

Faktorlar	Başlanğıc qiymətlər – D senarisi	Son qiymətlər – D senarisi	A və D senarilərinin stabil vəziyyətləri arasındakı fərq
Qanunvericilik tədbirləri	0.00	0.5381	0.0114
Təşkilati tədbirlər	0.00	0.5250	0.0111
Texniki tədbirlər	0.00	0.5904	0.0088
Potensialıən inkişafı	0.00	1.0000	0.4434
Maraqlı tərəflərin əməkdaşlığı	0.00	0.5279	0.0005
İnT təhdidlərinin inkişafı	1.00	1.00	0.5
İnT-nin səviyyəsi	0.00	0.5238	-0.0386

Cədvəl 6.1.5 göstərir ki, İnT təhdidlərinin inkişafı zamanı İnT-ni məqbul səviyyədə təkcə potensialın inkişafı hesabına təmin etmək mümkün deyil; müvafiq potensialın inkişafı ilə yanaşı, bütün maraqlı tərəflərin səmərəli əməkdaşlığı şərtində İnT üzrə hüquqi, texniki və təşkilati tədbirlərin optimal uyğunluğunu tapmaq tələb olunur.

6.2. Kiber-müdafiə taktikasının seçilməsi üçün hiperoyun modeli

Nəzəri-oyun perspektivindən baxıldıqda İnT-ni bir neçə oyunçudan: hücum edənlərdən (bədniyyətlilərdən) və müdafiə olunanlardan ibarət oyun kimi qəbul etmək olar. Nəzəri-oyun yanaşması, məsələn, şəbəkə administratoruna sistemin optimal müdafiə strategiyasını tapmağa [36, s.54] və müxtəlif müdafiə strategiyalarında gözlənilən ziyanın hesablanmasına kömək edə bilər [267, s.102].

Lakin oyunlar nəzəriyyəsində bütün oyunçuların hər bir oyunçunun strategiyaları, üstünlükləri və istifadə olunan qərar qaydaları haqqında tam məlumatlı olduqları fərz olunur. Bu çox ciddi fərziyyədir, reallıqda oyunçular arasında çox zaman əhəmiyyətli informasiya asimmetriyası olur. Bir çox real situasiyada qərar qəbul edənlər həmişə hər bir oyunçunun əsl niyyətləri, strategiyaları və ya üstünlükləri haqqında bütün informasiyanı bilmirlər. Nəticədə onlar situasiyanı öz baxış nöqtələrindən qavrayırlar və onlar öz qavrayışlarında səhv edə bilərlər. Oyunlar nəzəriyyəsinin erkən inkişafından başlayaraq oyun modellərində natamam və ya

qeyri-kafi məlumatların yanlış qavrayışlarını nəzərə almaq cəhdləri edilmişdir. Lakin bu cəhdlərin əksəriyyəti ümumilikdə çox subyektiv olan kəmiyyətlərə (ehtimallar, risk faktorları və s.) əsaslanır. 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 [175, s.65]. Hiperoyunların İnT üzrə qərarların tədqiq edilməsinə tətbiqi sahəsində tədqiqat işləri olduqca azdır. Bu işdə İnT kontekstində taktiki analiz vasitəsi kimi hiperoyun yanaşması təqdim olunur [175, s.65]. Təklif olunan ikisəviyyəli hiperoyun müdafiəçinin və hücumçunun İnT situasiyası haqqında qavrayışlarını oyunlar seriyası kimi modelləşdirir.

Mövcud tədqiqatların məhdudiyyətləri. İnformasiya təhlükəsizliyinə mövcud nəzəri-oyun yanaşmalarının əksəriyyəti tam informasiyalı statik oyunlara əsaslanır [262, s.1-10]. Lakin reallıqda müdafiəçi çox zaman hücumçuya qarşı tam olmayan və qeyri-dəqiq məlumatlı dinamik oyunla üzləşir. Natamam və qeyri-dəqiq məlumatlı dinamik oyuna baxılan bəzi modellər mobil ad hoc şəbəkələrə aiddir [255, s.131], digərləri isə real hücum senarilərinə baxmırlar [262, s.1-10].

Ənənəvi oyun modellərində fərz edilir ki, hər bir oyunçu digər oyunçuların uduş funksiyasını və strategiyasını bilir. Əslində, bu şərt çox zaman yerinə yetirilmir. Əgər hər hansı oyunçu digər oyunçuların uduş funksiyalarını bilmirsə, onda Neş tarazlığından danışmaq mənasız olur.

Hiperoyunlarda oyunçuların situasiyanı səhv başa düşməsi və ya yanlış qavraması aşkar fərz edilir. Natamam məlumatlı oyunların iki modeli – hiperoyunlar və Bayes oyunları arasındakı münasibət [268, s.720]-də müzakirə edilir və göstərilir ki, hər bir hiperoyunu Bayes oyunu kimi ifadə etmək olar və hiperoyunlar üçün müəyyən edilmiş bəzi tarazlıq anlayışları Bayes oyunları üçün tarazlıq anlayışlarına ekvivalentdir.

Hiperoyunlar Fraser və Hipel oyun analizi alqoritmindən [295, s.207] istifadə etməklə analiz edilir. Əvvəlcə analiz edilən hiperoyunun nisbi aspektlərini təsvir etmək üçün yeni oyun qurulur. Bunun üçün oyunçuların situasiyanı qavramasını təsvir edən oyundan hər bir oyunçunun üstüntutma vektoru götürülür və onların birgə

kombinasiyasından yeni oyun qurulur.

Hiperoyun analizi metodları hərbi münaqişələrə, beynəlxalq mübahisələrə, iqtisadi müqavilələrə və razılaşmalara, sosial problemlərə, informasiya müharibəsinə, kibertəhlükəsizliyə və s. tətbiq edilə bilər [175, s.65].

Hiperoyun modeli. Hiperoyunun iki səviyyəsinə formal olaraq baxaq.

G oyununu, qısaca olaraq, bütün oyunçuların üstüntutma vektorlarının çoxluğu kimi nəzərdən keçirmək olar. Tutaq ki, V_A Hücumçunun üstüntutma vektoru, V_D – Müdafiəçinin üstüntutma vektorudur. Onda oyunçuları Hücumçu və Müdafiəçi olan oyunu $G = \{V_A, V_D\}$ kimi təyin etmək olar. Tam informasiyalı oyunlarda oyunçular bir-birlərinin üstüntutma vektorlarını tam və adekvat qiymətləndirirlər, buna görə də, onların hamısı eyni oyun oynayırlar.

Əgər iki-nəfər oyununda hər iki oyunçu eyni *G* oyununu oynayırsa, yəni bir-birinin üstüntutma vektorlarını düzgün qiymətləndirirlərsə, onda sıfırıncı səviyyə hiperoyunu alınır. Əgər oyunçulardan ən azı biri digər oyunçunun üstüntutma vektorunu səhv interpretasiya edirsə, onda birinci səviyyə hiperoyunu alınır. Əgər oyunçu ikinci oyunçunun səhv interpretasiya etdiyini bilirsə, onda ikinci səviyyə hiperoyunu alınır.

Tutaq ki, H^1 birinci səviyyə hiperoyununu işarə edir. Bu oyunda istifadəçilər müxtəlif oyunlar oynayırlar. Tutaq ki, V_{ij} – j oyunçusunun baxış nöqtəsindən i oyunçusunun üstüntutma vektorudur. Onda iki oyunçu – Hücumçu və Müdafiəçi – üçün refleksiv üstüntutma vektorlarının aşağıdakı növləri vardır:

V_{AA} – Hücumçunun baxış nöqtəsindən Hücumçunun üstüntutma vektoru;

V_{DA} – Hücumçunun baxış nöqtəsindən Müdafiəçinin üstüntutma vektoru;

V_{AD} – Müdafiəçinin baxış nöqtəsindən Hücumçunun üstüntutma vektoru;

V_{DD} – Müdafiəçinin baxış nöqtəsindən Müdafiəçinin üstüntutma vektoru.

Birinci səviyyə *H* hiperoyununda Hücumçunun oynadığı oyun $G_A = \{V_{AA}, V_{DA}\}$ kimi, Müdafiəçinin oynadığı oyun isə $G_D = \{V_{AD}, V_{DD}\}$ kimi işarə edilir. Uyğun olaraq, birinci səviyyə hiperoyununun özü $H = \{G_A, G_D\}$ kimi müəyyən edilir.

Birinci səviyyə hiperoyunu matris formasında cədvəl 6.2.1-də göstərilib.

Cədvəl 6.2.1

Birinci səviyyə hiperoyunu H^1 matris formasında

Oyunçular	Oyun	
	Hücumçu	Müdafiəçi
Hücumçu	V_{AA}	V_{AD}
Müdafiəçi	V_{DA}	V_{DD}
	G_A	G_D

Birinci səviyyə H hiperoyununun şərtlərinə uyğun olaraq, Müdafiəçi Hücumçunun üstüntutma vektorunu yanlış interpretasiya edir, yəni $V_{AA} \neq V_{AD}$ olması doğrudur, lakin Hücumçu Müdafiəçinin üstüntutma vektorunu düzgün qiymətləndirir, yəni $V_{DA} = V_{DD}$.

Analiz edilən situasiyanın daha real modeli ikinci səviyyə hiperoyunu ilə təsvir edilir, bu hal o zaman baş verir ki, oyunçulardan biri vəziyyətinin digər oyunçu tərəfindən səhv interpretasiya edilməsi haqqında bilir.

Tutaq ki, H_A^1 Hücumçunun və H_D^1 Müdafiəçinin birinci səviyyə hiperoyununu işarə edir. Burada: $H_A^1 = \{G_{AA}, G_{DA}\}$, $H_D^1 = \{G_{AD}, G_{DD}\}$ və:

G_{AA} = Hücumçunun baxış nöqtəsindən $G_A = \{V_{AA}, V_{DA}\}$ oyunu,

G_{DA} = Hücumçunun baxış nöqtəsindən $G_D = \{V_{AD}, V_{DD}\}$ oyunu,

G_{AD} = Müdafiəçinin baxış nöqtəsindən $G_A = \{V_{AA}, V_{DA}\}$ oyunu,

G_{DD} = Müdafiəçinin baxış nöqtəsindən $G_D = \{V_{AD}, V_{DD}\}$ oyunudur.

H_2 ikinci səviyyə hiperoyunu matris formada cədvəl 6.2.2-də göstərilmişdir.

Cədvəl 6.2.2

İkinci səviyyə hiperoyunu H^2 matris formasında

Oyunçular	Oyun	
	Hücumçu	Müdafiəçi
Hücumçu	G_{AA}	G_{AD}
Müdafiəçi	G_{DA}	G_{DD}
	H_A^1	H_D^1

Hiperoyunun analizinə hər bir oyunun stabillik üçün analiz edilməsi və sonra nəticələri müqayisə edərək stabil tarazlıq nöqtələrinin tapılması daxildir. H^2 ikinci səviyyə hiperoyunu üçün stabil nəticələrin və tarazlıq nöqtələrinin tapılması alqoritmi aşağıdakı kimidir.

1. G_{AA}, G_{AD}, G_{DA} və G_{DD} oyunlarını onların hər birinə uyğun üstünlük vektorlarını müqayisə etməklə ardıcıl analiz etməli.

2. Birinci səviyyə H_A^1 hiperoyununu analiz etməli, yalnız G_{AA} oyununda V_{AA} və G_{DA} oyununda V_{DD} üstüntutma vektorlarında nəticələrin stabilliyi haqqında informasiya nəzərə alınır. H_A^1 hiperoyununun tarazlıq nöqtələri çoxluğunu tapmalı: hücumçu üçün $E_H = E_{AA} \cap E_{DA}$ (G_{AA} və G_{DA} oyunlarına nəzərən).

3. Birinci səviyyə H_D^1 hiperoyununu analiz etməli, yalnız G_{AD} oyununda V_{AA} və G_{DD} oyununda V_{DD} üstüntutma vektorlarında nəticələrin stabilliyi haqqında informasiya nəzərə alınır. H_D^1 hiperoyununun tarazlıq nöqtələri çoxluğunu tapmalı*:* Müdafiəçi üçün $E_H = E_{AD} \cap E_{DD}$ (G_{AD} və G_{DD} oyunlarına nəzərən).

4. İkinci səviyyə H^2 hiperoyununu bütövlükdə analiz etməli. Oyunun tarazlıq nöqtələri çoxluğu tapılır, yəni G_{AA} oyununda V_{AA} üstüntutma vektorunun və G_{DD} oyununda V_{DD} üstüntutma vektorunun stabil nəticələri çoxluğunun kəsişməsi tapılır: $E = E_{AA} \cap E_{DD}$ (G_{AA} və G_{DD} oyunlarına nəzərən).

Nəticələrin stabilliyinin və oyunun ümumi həllinin necə tapılmasını göstərmək üçün bəzi yeni işarə və təriflər daxil edək.

Tutaq ki, müəyyən q nəticəsi verilib. Əgər A oyunçusu öz rəqibi D-nin sabit strategiyasında ən yaxşı seçimini edə bilirsə, yəni q-dən daha böyük üstünlük çəkisinə malik nəticə tapa bilirsə, onda A öz vəziyyətini birtərəfli yaxşılaşdıra bilər. Tutaq ki, $UI_A(q)$ $[UI_D(q)]$ A oyunçusu (D oyunçusu) üçün q nəticəsinin birtərəfli yaxşılaşmalarını təsvir edən nəticələr çoxluğunu işarə edir.

Əgər A oyunçusu öz rəqibi D-nin sabit strategiyasında bərabər və ya daha pis seçim edə bilərsə, yəni q-yə bərabər və ya ondan kiçik üstünlük çəkisinə malik nəticə tapa bilirsə, onda A öz vəziyyətini birtərəfli pisləşdirə bilər. Tutaq ki, $UD_A(q)$ $[UD_D(q)]$ A oyunçusu (D oyunçusu) üçün q nəticəsinin birtərəfli pisləşmələrini təsvir edən nəticələr çoxluğunu işarə edir.

Fərz edək ki, A oyunçusu q nəticəsinin birtərəfli yaxşılaşdırılmasına malik deyil, yəni $UI_A = \emptyset$. Bu şərti ödəyən bütün q nəticələri rasional stabil adlanır və r hərfi ilə işarə edilir.

Sanksiya rəqibinin vəziyyətinin mümkün yaxşılaşdırılmasında oyunçunun reaksiyasıdır, bu onun rəqibinə faydası özünün ilkin vəziyyətindən az və ya bərabər olan nəticəyə keçməyə səbəb olur.

Beləliklə, əgər rəqib mümkün sanksiyalar haqqında bilirsə, onu tərk etmək məcburiyyətində deyildir, çünki əgər o belə edərsə, nəticə əldə etməyəcəkdir. Sanksiyalı vəziyyət onun üçün stabildir və o bunu oyunun gözlənilən rasional həllər çoxluğuna daxil edə bilər.

Fərz edək ki, verilmiş q nəticəsi üçün A oyunçusu boş olmayan $UIA(q)$ çoxluğuna malikdir. Həmçinin fərz edirik ki, hər bir $UI_A(q)$ üçün A oyunçusunun rəqibinin – D oyunçusunun – elə UI_D və ya UD_D çoxluğu var ki, onun A üçün faydalılığı q nəticəsinin faydalılığından kiçik və ya ona bərabərdir. Onda A D-nin mümkün sanksiyalarını nəzərə alaraq öz vəziyyətinin birtərəfli yaxşılaşdırılmasından çəkinərsə, rasional hərəkət etmiş olacaq. Oyunçu üçün stabilliyi rəqibinin mümkün sanksiyalarına əsaslanan q nəticəsi *ardıcıl sanksiyalı* adlanır və s hərfi ilə işarə edilir.

Fərz edək ki, verilmiş q nəticəsi üçün A oyunçusu boş olmayan $UI_A(q)$ çoxluğuna malikdir. Əgər bir UI_A üçün A oyunçusunun rəqibinin – D oyunçusunun – sanksiyaları yoxdursa, onda q nəticəsi *qeyri-stabil* adlandırılır və u hərfi ilə işarə edilir.

A üçün bütün rasional və ya ardıcıl sanksiyalı nəticələr onun üçün oyunun mümkün həllərini təsvir edir

[295, s.207]-də qeyd edildiyi kimi, hiperoyunların həlləri bütün oyunçular üçün stabil olan nəticələrlə formalaşmaya bilər və mümkündür ki, oyunçular üçün qeyri-stabil olan nəticələr həqiqətdə hiperoyunun tarazlıq nöqtəsi olsun.

Ədədi misal. Yuxarıda təsvir edilmiş yanaşmanın ədədi illüstrasiyası üçün [175, s.65]-dən şəbəkə təhlükəsizliyi modelinin modifikasiya edilmiş versiyasından istifadə edək. Alpcan və Başar-ın modelində Hücumçunun iki seçimi var: hücuma başlamaq və heç bir şey etməmək. Müdafiəçinin seçimləri müdafiə mexanizmini işə salmaq və işə salmamaq ola bilər. Bu tədqiqatda oyunçuların hərəkətlər fəzası yalnız illüstrasiya məqsədi üçün məhdudlanıb. Bu məqsədlə həmçinin fərz edirik ki, hər bir istifadəçinin hərəkətləri bir-birini qarşılıqlı istisna edir, yəni baxılan anda oyunçu yalnız bir

hərəkətə təşəbbüs edə bilər.

Fərz edək ki, Hücumçunun iki hücum senarisi var:

#1 – Hücum senarisi 1;

#2 – Hücum senarisi 2.

Fərz edək ki, Müdafiəçi üçün hərəkətlər aşağıdakılardır:

#3 – Müdafiə mexanizmi 1;

#4 – Müdafiə mexanizmi 2;

#5 – Müdafiə mexanizmi 3.

Yuxarıda vurğulandığı kimi, hiperoyunlar natamam informasiyalı oyunlardır. Bu o deməkdir ki, ən azı bir oyunçunun oyun elementləri haqqında fərqli təsəvvürləri var. Fərz edək ki, bu oyunda oyunçuların aşağıdakı fərqli təsəvvürləri vardır:

–Oyunçular bir-birinin üstüntutma vektorlarını səhv interpretasiya edirlər;

–Hücumçunun Müdafiəçidə olan üçüncü mexanizm haqqqında məlumatı yoxdur.

İkinci səviyyə hiperoyunu aşağıdakı dörd oyundan ibarətdir:

–G_{AA} oyunu: Hücumçunun öz oyunu haqqında təsəvvürü;

–G_{DA} oyunu: Hücumçunun Müdafiəçinin oyunu haqqında təsəvvürü;

–G_{AD} oyunu: Müdafiəçinin Hücumçunun oyunu haqqında təsəvvürü;

–G_{DD} oyunu: Müdafiəçinin öz oyunu haqqında təsəvvürü.

Oyunçuların hərəkətlər çoxluğundan stratregiyaları formalaşdırılır. (Strategiya oyunçu tərəfindən edilən hərəkətlər çoxluğudur.) Bütün oyunçuların strategiyaları birlikdə *nəticə* adlandırılır. Nəticələrin sayı 2^n-ə bərabərdir, burada n - oyunçular üçün əlyetər olan bütün hərəkətlərin sayıdır. Lakin bu nəticələrin hamısı mümkün deyil. Hərəkətlərin hər biri yerinə yetirilə və ya yetirilməyə bilər. Buna görə, bu oyunda formal olaraq $2^4 = 16$ nəticə var. Lakin hücum edənin və müdafiəçinin hərəkətlərinin bir-birini qarşılıqlı istisna etdiyini nəzərə alsaq, bu hərəkətlərin hər ikisinin eyni vaxtda yerinə yetirildiyi bütün nəticələr praktiki cəhətdən mümkün deyildir. Həmçinin oyunçuların hərəkətlərdən birini yerinə yetirməli olduğu fərz edilir. Buna görə də, G_{AA} (G_{DA}, G_{AD}) oyununda 16-12 = 4 nəticə var.

Hiperoyunun analizində növbəti addım istifadəçilərin üstünlüklərini müəyyən

etməkdir. Fərz edirik ki, həm Hücumçunun, həm də Müdafiəçinin nəticələr üçün müxtəlif faydalılıq funksiyaları var və hər bir oyunçu tərəfindən onun fərdi üstünlüklərinə görə ən böyük üstünlükdən ən kiçik üstünlüyə doğru nizamlanıb (məsələn, 4 = ən böyük üstünlük; 3 = sonrakı ən böyük üstünlük; 2 = sonrakı ən kiçik üstünlük; l = ən kiçik üstünlük).

Bu ədədi misal HYPANT hiperoyun analizi aləti istifadə edilməklə həll edilmişdir [175, s.65]. Qeyd edək ki, HYPANT ilə analiz edilməsi üçün hiperoyun modelləri xüsusi HML (Hypergame Modeling Language) formatında yazılmalıdır.

G_{AA} oyununda Hücumçu (A) və Müdafiəçi (D) üçün fərdi üstüntutma vektorlarının və nəticələrin stabilliyinin hesablanması nəticələri cədvəl 6.2.3-də verilmişdir.

Cədvəl 6.2.3-də Y işarəsi müvafiq fəaliyyətin yerinə yetirildiyini, N – müvafiq fəaliyyətin yerinə yetirilmədiyini göstərir. Nəticələr 1-dən 4-ə kimi nömrələnir.

Üstüntutma vektoru oyunçunun mümkün nəticələri ranqlaşdırmasını göstərir. Müvafiq nəticələr üçün üstüntutma vektorları cədvəl 6.2.3-ün birinci sətrində (Hücumçu üçün) və dördüncü sətrində (Müdafiəçi üçün) göstərilib.

Cədvəl 6.2.3
İkinci səviyyə hiperoyunu G_{AA}

A-nın üstüntutma vektoru	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D-nın üstüntutma vektoru	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Nəticə	1	2	3	4
A üçün stabillik	*r*	*r*	*s*	*u*
D üçün stabillik	*u*	*r*	*u*	*r*
Tarazlıqlar		*E*		

Aşağıda Hücumçu üçün nəticələrin stabilliyinin hesablanması göstərilir:

q = 1; $UI_A(1) = Ø$. Yəni q = 1 nəticəsi A üçün rasionaldır və r ilə işarə edilir.

q = 2; $UI_A(2) = Ø$. Yəni q = 2 nəticəsi A üçün rasionaldır və r ilə işarə edilir.

q = 3; $UI_A(3) = \{1\}$. $UI_D(1) = \{4\}$. $w_D(4) = 1 \succ w_A(3) = 3$. Yəni q = 3 nəticəsi A üçün ardıcıl sanksiyalıdır.

$q = 4$; $UI_A(4) = \{2\}$. $UD_D(2) = \{3\}$. $w_D(3) = 3 \succ w_A(4) = 4$. Bu o deməkdir ki, $q = 4$ nəticəsi A üçün qeyri-stabildir.

Ümumi stabillik hansı nəticələrin hiperoyun üçün mümkün həllər olduğunu göstərir. G_{AA} oyunu üçün tarazlıq E_{AA}= {{#2 Hücum senarisi 2, #4 Müdafiə mexanizmi 2}}-dir.

G_{DA}, G_{AD} və G_{DD} oyunlarının nəticələri uyğun olaraq Cədvəl 6.2.4, 6.2.5, 6.2.6-də verilib. Qeyd edək ki, G_{DD} oyununun 6 nəticəsi vardır.

G_{DA} oyunu üçün tarazlıq nöqtəsi E_{DA}= {{#2 Hücum senarisi 1, #4 Müdafiə mexanizmi 2}}-dir.

Hücumçu üçün H_A^1 hiperoyununun tarazlıq nöqtələri çoxluğu $E_H = E_{AA} \cap E_{DA}$={{#2 Hücum senarisi 2, #4 Müdafiə mexanizmi 2}} olur.

Cədvəl 6.2.4

İkinci səviyyə hiperoyunu G_{DA}

A-nın üstüntutma vektoru	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D-nin üstüntutma vektoru	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Nəticə	1	2	3	4
A üçün stabillik	*r*	*r*	*s*	*u*
D üçün stabillik	*u*	*r*	*u*	*r*
Tarazlıqlar		*E*		

Cədvəl 6.2.5

İkinci səviyyə hiperoyunu G_{AD}

A-nın üstüntutma vektoru	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D-nin üstüntutma vektoru	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Nəticə	1	2	3	4
A üçün stabillik	*r*	*r*	*s*	*u*
D üçün stabillik	*u*	*r*	*u*	*r*
Tarazlıqlar		*E*		

G_{AD} oyunu üçün tarazlıq nöqtəsi E_{AD} = {{#2 Hücum senarisi 2, #4 Müdafiə

mexanizmi 2}}-dir.

Cədvəl 6.2.6

İkinci səviyyə hiperoyunu G_{DD}

A-nın üstüntutma vektoru	1	2	3	4	5	6
#1	Y	N	N	Y	N	Y
#2	N	Y	Y	N	Y	N
D-nin üstüntutma vektoru	6	5	4	3	1	2
#3	Y	Y	N	N	N	N
#4	N	N	Y	N	N	Y
#5	N	N	N	Y	Y	N
Nəticə	1	2	3	4	5	6
A üçün stabillik	*r*	*s*	*r*	*r*	*s*	*u*
D üçün stabillik	*u*	*u*	*u*	*s*	*r*	*r*
Tarazlıq nöqtəsi				*E*	*E*	

G_{DD} oyunu üçün tarazlıq nöqtələri E_{DD} = {{#1 Hücum senarisi 1, #5 Müdafiə mexanizmi 3}, {#2 Hücum senarisi 2, #5 Müdafiə mexanizmi 3}} olur.

Müdafiəçi üçün H_D^1 hiperoyununun tarazlıq nöqtələri çoxluğu E_H ={{#1 Hücum senarisi 1, #5 Müdafiə mexanizmi 3}, {#2 Hücum senarisi 2, #5 Müdafiə mexanizmi 3}}-dir.

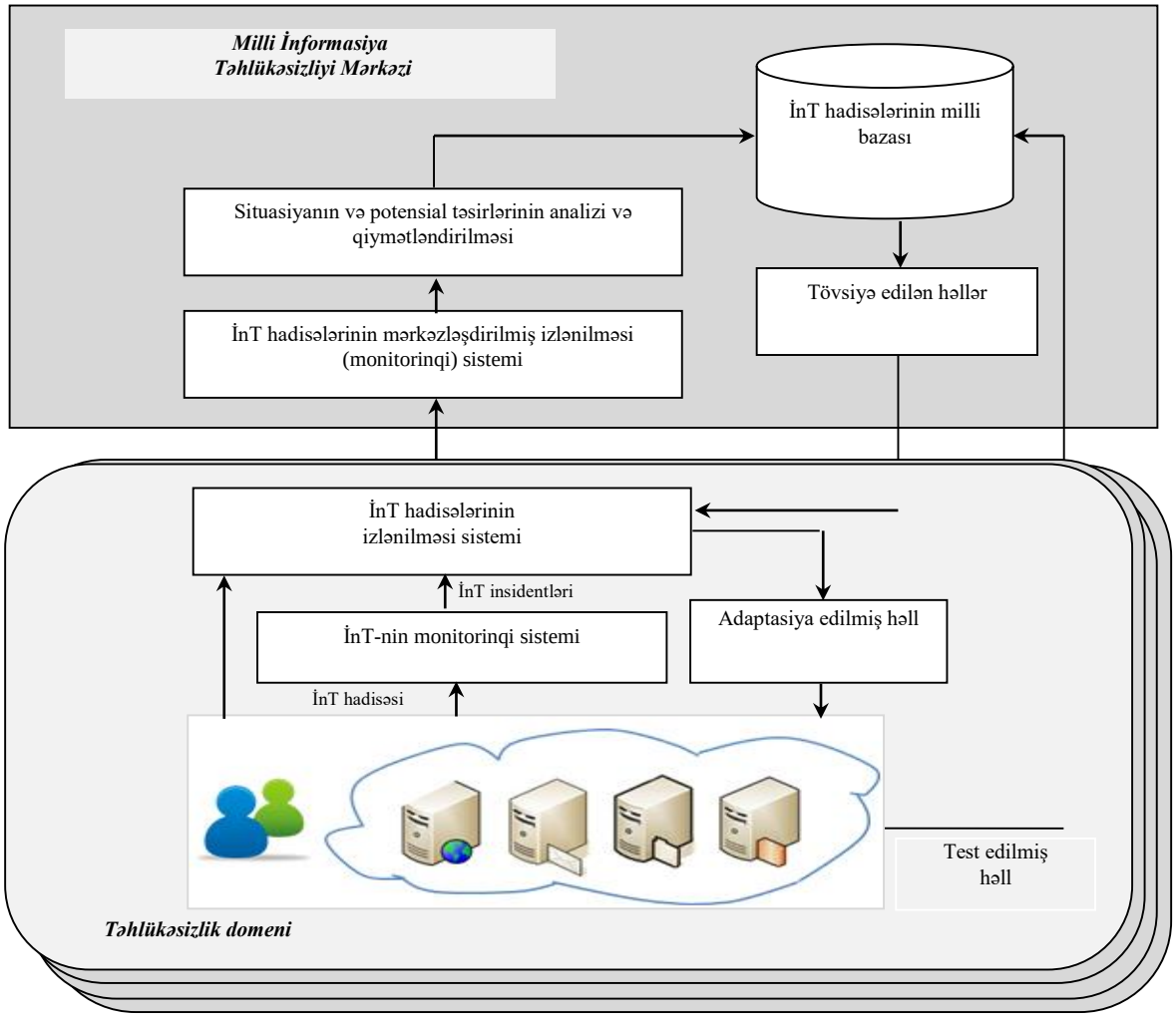
Hiperoyun nəzəriyyəsinin İnT üzrə qərar qəbuletmə üçün istifadəsinin mümkünlüyü tədqiq edilmişdir. Təklif olunan iki səviyyəli hiperoyun yanaşması müdafiə olunanın və hücum edənin İnT situasiyasını qavramasını oyunlar seriyası kimi modelləşdirir. Şəbəkə təhlükəsizliyi kontekstində ən yaxşı hücum və müdafiə mexanizmləri üzrə qərar qəbuluna dair bir illüstrativ misal da verilmişdir.

6.3. E-dövlətin informasiya təhlükəsizliyini situasiyalar üzrə idarəetmə modeli

İdarəetmə nəzəriyyəsi obyektin vəziyyəti haqqında məlumatlar əsasında obyektə idarəetmə təsirlərinin sürətli və dəqiq seçilməsi üçün bir çox effektiv mexanizmlər yaratmışdır. Onlardan biri – süni intellekt nəzəriyyəsinin ideyalarına əsaslanan mürəkkəb obyektlərin situasiya idarəetməsi metodudur [53, s.24].

Bu bölmədə e-dövlətin İnT-ni situasiya idarə etməsinin konseptual modeli işlənir və konseptual modelin reallaşdırması üçün presedentlər nəzəriyyəsi əsasında konseptual yanaşma təklif edilir [53, s.24].

E-dövlətin İnT-nin situasiya idarəetməsinin təklif edilən konseptual modelində e-dövlətin informasiya infrastrukturu (şəkil 6.3.1) ayrı-ayrı təhlükəsizlik



Şəkil 6.3.1. E-dövlətin informasiya təhlükəsizliyinin situativ idarə edilməsinin konseptual modeli

domenlərindən ibarətdir. Hər bir təhlükəsizlik domenində domenin İnT siyasəti əsasında İnT-nin monitorinqi həyata keçirilir. İnT-nin monitorinqi dedikdə İnT təhdidlərinin reallaşdırmasına səbəb olmuş və ya səbəb ola biləcək hadisələrin vaxtında aşkarlanması və aradan qaldırılması məqsədi ilə İnT hadisələrinin daimi müşahidəsi prosesi başa düşülür. İnT-nin monitorinqinə şəbəkə və sistem aktivliyinin, istifadəçilərin aktivliyinin, qorunan resurslara girişlərin, informasiya sistemlərinin vəziyyətinin izlənilməsi və informasiya axınlarının məzmununun monitorinqi daxildir. Qeyd edək ki, ISO/IEC 27001-2006 standartında İnT hadisəsi dedikdə "sistemin, xidmətin və ya şəbəkənin İnT siyasətinin mümkün pozulmasını göstərən

müəyyən edilmiş vəziyyətinin baş verməsi, mühafizə vasitələrinin imtinası (işləməməsi), həmçinin təhlükəsizliklə bağlı ola bilən daha əvvəl rastlanmayan vəziyyətin baş verməsi" nəzərdə tutulur.

Təhlükəsizlik domeninin monitorinq sistemi İnT hadisələri haqqında məlumatların toplanması, emalı və analizinin (konsolidasiya, filtrasiya, normallaşdırma, aqreqasiya, korrelyasiya) mərkəzi nöqtəsidir, məlumatlar domenin müxtəlif komponentlərindən (şəbəkələrarası ekranlar, əməliyyat sistemləri (ƏS), müdaxilələrin aşkarlanması sistemləri, şəbəkə avadanlığı, antivirus sistemləri, tətbiqi proqramlar və s.) daxil olurlar.

Emaldan sonra bəzi İnT hadisələri insident kimi identifikasiya oluna bilər. İnformasiya təhlükəsizliyi insidenti – biznes-prosesləri pozma və informasiya təhlükəsizliyinə təhlükə yaratma ehtimalı böyük olan hadisə və ya hadisələr ardıcıllığıdır [8, s.37]. Qeyd edək ki, bəzi hadisələri avtomatik aşkarlamaq olmur (məsələn, administratorun vəzifə reqlamentlərini pozması ilə bağlı hadisələri). Eləcə də, istifadəçilər özləri də İnT hadisələri haqqında məlumat verə bilərlər. Hadisə aşkarlandıqdan sonra reqlamentə uyğun olaraq hadisələrin monitorinqi sisteminin reyestrində (jurnalında) qeydiyyata alınır, hadisənin kateqoriyası və prioritet səviyyəsi təyin edilir. Hadisələrin idarə edilməsi (qeydiyyatı, analizi və emalı) xüsusi CERT komandaları tərəfindən həyata keçirilir [8, s.6].

İnT hadisələrinin idarə edilməsinin mövcud metodikalarında mərkəzi idarəedici orqan yoxdur, bir domenə məxsus olan CERT-komandaları zəruri olduqda digər domenlərin CERT-komandaları ilə hadisə haqqında informasiya mübadiləsi edirlər. Təklif edilən konseptual modeldə İnT hadisələri haqqında məlumatlar lokal reyestrdə qeydiyyata alınır və İnT hadisələrinin vahid monitorinqi mərkəzinə - Milli İnformasiya Təhlükəsizliyi Mərkəzinə ötürülür (MİTM). MİTM bütün təhlükəsizlik domenlərindən hadisələr haqqında məlumatları toplayır, onların emalını, analizini (aqreqasiya, korrelyasiya) və vizuallaşdırılmasını həyata keçirir. Bu verilənlərdən istifadə edərək MİTM İnT situasiyasının bütöv mənzərəsini qurur, situasiyanı analiz edir və İnT hadisəsinin potensial təsirlərini təkcə bir domen səviyyəsində deyil, bir neçə qarşılıqlı əlaqəli və qarşılıqlı asılı təhlükəsizlik domenləri miqyasında da

qiymətləndirməyə imkan verir. MİTM hadisənin cavablandırılması üçün uyğun üsulu İnT hadisələrinin milli bazasından seçir və tövsiyə edilən həlləri müvafiq təhlükəsizlik domenlərinə ötürür. İnT hadisələrinin milli bazası hadisələr və onların emalı üsulları haqqında mərkəzi biliklər bazasıdır, burada İnT hadisələrinin emalı üzrə koordinasiyalı tədbirlərin şablonları da saxlanır. Təhlükəsizlik domenlərində MİTM-in tövsiyə etdiyi həll cari hadisəyə adaptasiya edilir və hadisənin emalı həyata keçirilir (məsələn, aparat və proqram təminatının konfiqurasiyasında zəruri dəyişikliklər edilir). Bu məqsəd üçün zəruri texniki resurslar ayrılır, hadisənin emalı qrupu təyin edilir, bu qrup texniki və digər mütəxəssislərdən (ekspertlərdən) və qərar qəbul edən şəxsdən ibarət olur. Hadisənin emalı gedişində hadisənin emalı qrupu adaptasiya olunmuş həllə zəruri dəyişikliklər edə bilər. Hadisənin emalından sonra hadisənin test edilmiş emalı üsulu İnT hadisələrinin milli bazasına daxil edilir, hadisəni emal edən ekspertlər qrupu və qərarı qəbul edən şəxslər də bazada saxlanılır.

Təklif edilmiş arxitektura dövlət orqanlarına e-dövlətin informasiya infrastukturunun digər hissələrində baş vermiş hadisələr haqqında, xüsusi halda, bilavasitə onların domenlərinə təsir edən hadisələr haqqında məlumat əldə etməyə imkan yaradır. Təhlükəsizlik domenləri təhlükəsiz veb-portala girişə malikdir, burada onlar öz sistemlərindəki hadisələr haqqında informasiya ilə tanış ola bilərlər.

Təklif edilmiş model mövcud yanaşmalarla müqayisədə bir neçə üstünlüyə malikdir. Hadisələr haqqında məlumatların korrelyasiyası və bir neçə təhlükəsizlik domeni arasında informasiya mübadiləsi İnT mütəxəssislərində və qərar qəbul edən şəxslərdə e-dövlətin İnT-nin vəziyyəti haqqında geniş təsəvvür yaratmağa imkan verir. Təklif edilmiş model kritik İnT hadisələri haqqında məlumatların toplanmasına və informasiya mübadiləsinə dövlət orqanları tərəfindən sərf edilən vaxtı əhəmiyyətli dərəcədə azaldır (bir neçə gündən bir neçə saata qədər). Bu dövlətə İnT hadisələrinin analizi və qarşısının alınması potensialını möhkəmləndirməyə, hadisələrə reaksiya verilməsini kökündən yaxşılaşdırmağa imkan verərdi.

Presedentlər nəzəriyyəsinin əsas elementləri

Situasiya idarəetməsi mürəkkəb sistemdə yaranan problemli (fövqəladə) və problemsiz (ştat) situasiyaların nizamlanması üzrə idarəetmə qərarlarının qəbul

edilməsini nəzərdə tutur. Problemli vəziyyətlərdən fərqli olaraq ştat vəziyyətləri onunla səciyyələnir ki, onların nizamlanması mexanizmləri apriori məlumdur.

İdarəetmə fəaliyyətində situasiya yanaşması R. Mokler tərəfindən 1971-ci ildə təklif edilmişdi [41, s.112]. Bir neçə onillik ərzində inkişafına baxmayaraq situasiya idarəetməsinin metodları praktikada lazımlı tətbiq tapmamışdır. Bu bir tərəfdən onun klassik elmi rasionallıq prinsipləri əsasında işlənməsi ilə bağlıdır, digər tərəfdən belə bir baxış da var ki, situasiyaların idarə edilməsi elmdən daha çox sənətdir [41, s.112].

Situasiya idarəetməsi nəzəriyyəsinin inkişafı ilə praktika göstərdi ki, problemli yeni situasiyanın yaranması zamanı presedentlər əsasında mühakimə metodundan (Case Based Reasoning, CBR) istifadə etmək məqsədəuyğundur. Bu yanaşmanın universallığının və geniş imkanlarının anlaşılması "presedentlər nəzəriyyəsinin" yaramasına və sürətli inkişafına gətirib çıxardı.

CBR metodologiyasının mahiyyəti aşağıdakından ibarətdir. Presedent <situasiya, həll metodu> cütlüyüdür. Zaman ötdükcə yaranan situasiyalar və onların həll metodları xüsusi bazada – presedentlər bazasında saxlanılır. Yeni situasiya meydana çıxdıqda presedentlər bazasında oxşar situasiya tapırlar və onun həll metodunu baxılan situasiyaya uyğunlaşdırırlar.

CBR metodologiyası dörd prosesdən ibarət olan tsiklik prosedur kimi həyata keçirilir (bu prosesləri çox zaman 4Re-prosesləri adlandırırlar) [53]:

1. Konkret presedent üçün oxşar presedentin axtarışı (ing. Retrieve);
2. Presedentin həll metodunun konkret situasiyaya tətbiqi (ing. Reuse);
3. Zəruri olduqda alınmış həllin yoxlanması və korreksiyası (adaptasiyası) (ing. Revise);
4. Alınmış həllin sonrakı istifadə üçün presedentlər bazasında saxlanılması (ing. Retain).

CBR metodologiyası ən müxtəlif predmet sahələrində klassifikasiya, diaqnostika, proqnozlaşdırma, planlaşdırma və layihələndirmə üçün tətbiq edilmişdir və çox yaxşı nəticələr göstərmişdir. CBR həmçinin İnT-nin müxtəlif aspektlərinə də – risklərin qiymətləndirilməsinə, müdaxilələrin aşkarlanmasına, şəbəkə təhlükəsizliyi vəziyyətinin analizinə tətbiq edilmişdir [53, s.24].

CBR metodologiyası ekstremal situasiyalarda qərarların qəbul olunmasını təmin etmək üçün xüsusilə əhəmiyyətlidir, belə situasiyalar kəskin vaxt çatışmazlığı və tez dəyişən şəraitlə səciyyələnir. Ekstremal situasiyalarda həll edilən məsələlərin bir hissəsi daha əvvəl həll edilmiş ola bilərlər və mövcud həlləri həll variantlarını operativ tapmaq üçün istifadə etmək olar [53, s.24].

CBR-sistemin qurulması aşağıdakı məsələlərin həllini nəzərdə tutur:

- Situasiya və mümkün həllər haqqında biliklərin təsviri üsulunun işlənməsi;
- Presedentlərin seçilməsi metodunun işlənməsi;
- Həllərin uyğunlaşdırılması (adaptasiyası) metodunun işlənməsi;
- Presedentlərin indeksləşdirilməsi metodunun işlənməsi.

Belə sistemlərin qurulması zamanı qarşıya çıxan iki əsas problemi ayırmaq olar: ən uyğun presedentlərin axtarışı və tapılmış həllin sonrakı adaptasiyası. CBR tətbiqinin daha bir problemi presedentlərin təsviri və presedentin əlamətlərinə müvafiq çəkilərin təyin edilməsi ilə bağlıdır, bu həmin sistemlərin müxtəlif predmet sahələrində tətbiq edilməsini çətinləşdirir.

İnformasiya təhlükəsizliyi hadisəsi haqqında biliklərin təsviri

Presedentə aşağıdakılar daxildir:

1. Situasiyanın və ya problemin təsviri;
2. Baxılan situasiyada və ya baxılan problem üçün qəbul edilmiş qərar;
3. Qərarın tətbiqinin nəticəsi.

Bunu nəzərə alaraq, e-dövlətin İnT situasiyasının formal modelini aşağıdakı şəkildə vermək olar.

Tutaq ki, e-dövlətin informasiya infrastrukturu m təhlükəsizlik domenindən ibarətdir. E-dövlətin İnT-nin $t_i \in T$ zaman anında vəziyyəti təhlükəsizlik domenlərində bu ana qədər qeydə alınmış və aradan qaldırılmamış İnT hadisələrinin $X = \{x_{i1}, \dots, x_{im}\}$ çoxluğu ilə təsvir olunur, burada: x_{ij} – t_i zaman anında j-cu təhlükəsizlik domenində olan İnT hadisələri çoxluğudur. Aydındır ki, bəzi zaman anlarında bu çoxluq boş ola bilər.

Qeyd edək ki, hadisə digər hadisələrin ardıcıllığı ola bilər, belə hadisəni *mürəkkəb hadisə* adlandıraq. Bundan başqa, qeydə alınma və ilkin analiz zamanı hadisəyə bəzi digər parametrlər də mənimsədilir (kateqoriya (tip), mənbə, mümkün təsirlər, kritiklik səviyyəsi, prioritet və s.).

Bu işdə İnT hadisələrinin təsviri üçün aşağıdakı struktur təklif edilir:

$$x = (ID, D, DT, rb, e_1, e_2, \ldots, e_k, CAT, Or, Im, Sev, Pr, V), \quad (6.3.1)$$

burada:

ID – hadisənin unikal identifikatoru;

D – hadisənin aşkarlandığı təhlükəsizlik domeninin identifikatoru;

DT – hadisənin qeydə alındığı vaxt və zaman;

rb – hadisənin aşkarlandığı mənbəyə inam dərəcəsi,

$e_1, e_2, \ldots, e_k$ – baxılan mürəkkəb hadisəni təşkil edən İnT hadisələrinin ardıcıllığı (xüsusi halda $k = 1$ ola bilər);

CAT – hadisənin kateqoriyası (tipi). Hadisənin kateqoriyasını müəyyənləşdirmək üçün müxtəlif metodikalar var. Məsələn, ISF (Information Security Forum) metodikasında [53, s.24] İnT hadisələrinin bu kateqoriyaları müəyyən edilir: xarici hücum, daxili qeyri-düzgün istifadə və sui-istifadə, oğurluq, sistemin nasazlığı, xidmətin kəsilməsi, insanın səhvləri və dəyişikliyin nəzərdə tutulmamış nəticələri. Qeyd edək ki, hadisəyə bir neçə kateqoriya mənimsədilə bilər.

Or – hadisənin mənbəyi (daxili, domenlərarası, xarici, naməlum);

Im – hadisənin mümkün təsirləri (təsirə məruz qalann aktivlər). Məsələn, [112, s. 12] funksional təsiri və informasiya təsirini fərqləndirir.

Sev – hadisənin ciddiliyi. Hadisənin ciddiliyi onun biznes-proseslərin və informasiyanın fəaliyyətinə və ya tamlığına təsir dərəcəsinin subyektiv ölçüsüdür. Hadisənin ciddiliyi müəyyən edilərkən aşağıdakı faktorlar nəzərə alınır [112, s. 12]: təsirin miqyası, sistemin və ya xidmətin kritikliyi, sistem və ya xidmət vasitəsilə emal edilən informasiyanın konfidensiallıq səviyyəsi, digər seqmentlərə yayılma ehtimalı. Hadisənin ciddiliyi üçün dörd səviyyə istifadə edilə bilər: yüksək, orta, aşağı, NA

(“Not Applicable” – tətbiq edilmir, insident kimi qəbul edilmiş, lakin araşdırmadan sonra təsdiqlənməmiş hadisələr üçün istifadə olunur).

Pr – hadisənin prioriteti. Prioritet hadisənin emal növbəsini müəyyən edir. ITIL metodikasında hadisənin prioriteti hadisənin ciddiliyinə və aradan qaldırılmasının təcililiyinə görə cədvəl əsasında müəyyən edilir (1 – kritik, 2 – yüksək, 3 – orta, 4 – aşağı, 5 – planlaşdırılan) [189, s. 278-283].

$V = (v_1, \ldots, v_n)$ – tətbiq sahəsindən asılı olaraq hadisənin təsviri üçün tələb edilən digər atributlar (məsələn, IP-ünvan, protokol, portun nömrəsi və s.).

Qeyd edək ki, konkret hadisənin təsviri formatı İnT siyasəti ilə müəyyən edilir və bura tətbiq sahəsi üçün maraqlı ola biləcək bütün məlumatlar daxil edilə bilər. Bundan başqa, adətən İnT hadisələrinin təsvirinə mətn informasiyası da daxil olur, məsələn, hadisənin simptomları, təzahürləri, səhvlər haqqında məlumatlar və s. Bu verilənlərin təsviri üçün aşağıda latent semantik indeksləmə (Latent Semantic Analysis, LSA) metodundan istifadə edilməsi təklif olunur [137, s.683].

LSA mətn sənədini semantik vektora çevirir. Bu vektorun yaradılması üçün LSA sənədlər toplusunda sözlərin tezliyini təsvir edən matrisdən istifadə edir. Tutaq ki, m sənəddən ibarət toplu verilib və bu sənədlərdə n terminə (sözə) rast gəlinir. Tutaq ki, müəyyənlik üçün $A_{m\times n}$ matrisinin sütunları sənədlərə, sətirləri isə sənədlərdə rast gəlinən terminlərə uyğundur. $A_{m\times n}$ matrisinin hər bir a_{ij} elementi aşağıdakı kimi hesablanır:

$$a_{ij} = \frac{n_{ij}}{t_j} \log \frac{N}{T_i}, \qquad (6.3.2)$$

burada: n_{ij} – i-ci terminin j-cu sənəddə rastgəlmə sayı; t_j – j-cu sənəddə terminlərin sayı; N – sənədlərin sayı, T_i – i-ci terminin olduğu sənədlərin sayıdır.

Sinqulyar vuruqlara ayırma (SVD – Singular Value Decomposition) [72, s. 433] üsulundan istifadə etməklə $A_{m\times n}$ matrisini üç matrisin hasilinə ayırırlar: $A = U\Sigma V^{\mathrm{T}}T$, burada: U – $m \times r$ ölçülü ortoqonal matris, V – $n \times r$ ölçülü ortoqonal matris, $\Sigma = diag(\sigma_1, \ldots, \sigma_r)$ – $r \times r$ ölçülü diaqonal matrisdir, $r = rank(A)$, σ_i – A-nın sinqulyar qiymətidir və $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r$.

LSA s ən böyük sinqulyar qiyməti götürməklə sinonimlik və polisemiyanı azaldır, nəticədə A matrisinin ranqı kiçilir; $A_s = U_s V_s V_s^{\mathrm{T}}$. s-in optimal qiyməti r-dən asılı olmaqla seçilir. Sənədlərin semantik vektorları V_s sıraları ilə indekslənir. Yeni sənədin və ya sorğunun semantik vektoru U_s, Σ_s istifadə edilməklə hesablanır [72].

Ümumi halda, qərar dedikdə aşağıdakılar başa düşülə bilər:

– əvvəllər analoji situasiyalarda yerinə yetirilmiş hərəkətlər və onların nəticələri;

– verilmiş situasiyada reqlamentlər əsasında hərəkətlərə göstərişlər (rəhbərlik);

– hərəkətlərin necə yerinə yetirilməsi barədə ekspert tövsiyələri;

– qərarın qəbulu və icrası zamanı tələb edilən sorğu kitabları və digər sənədlər.

Qərarın tətbiqinin nəticəsinin – İnT hadisəsinin emalının təsvirinə aşağıdakılar daxil ola bilər:

– hadisənin planlaşdırılmış və faktiki emal müddətləri;

– hadisəni və fəsadlarını aradan qaldırmaq üçün icra edilmiş hərəkətlər;

– hadisənin emalının nəticəsi;

– hadisənin qarşısını almaq üçün zəruri hərəkərlərin siyahısı.

Nəticənin təsvirində digər hadisələrə (presedentlərə) istinadlar ola bilər.

Situasiyanın və qərarın təsvirindən sonra presedenti formal olaraq aşağıdakı kimi müəyyən edə bilərik: p presedenti $\langle s, r, h, z \rangle$ kortejindən ibarətdir, burada: $s \in S$ situasiyası və onunla bağlı $r \in R$ qərarı $z \in Z$ qərar qəbul edən şəxsin rəhbərliyi altında $h \in H$ ekspertlər qrupu tərəfindən yerinə yetirilir.

Hər bir s situasiyasına bir neçə qərar uyğun ola bilər, beləliklə, $\langle s, r \rangle$ və $\langle s, r' \rangle$ şəklində presedentlərin mövcud olmasını qəbul etmək olar, onlar $r \neq r'$ şərtində fərqlənirlər.

Hər bir $p_i \in \{p\}$ presedentinə $s_i \Rightarrow r_i, i = \overline{1,n}$ şərti implikasiyası kimi baxmaq olar. Əgər müəyyən $s_i \approx s_j, j = \overline{1,n}, i \neq j$ situasiyası verilibsə və $p_i = \langle s_i, r_i, h_i, z_i \rangle$ presedenti mövcuddursa, onda r_j həllinin s_i situasiyası üçün təqribi həll olduğunu iddia etmək olar. s_i situasiyası s_j situasiyasına nə qədər yaxındırsa, r_j-un s_i üçün həll olması bir o qədər həqiqətəoxşardır.

Presedentlərin seçilməsi

Verilmiş presedentə ən "yaxın" presedentin presedentlər bazasından seçilməsi problemi CBR-əsaslı sistemlərin ən vacib hissəsidir. Ənənəvi verilənlər bazalarında və CBR-sistemlərdə axtarış mexanizmləri fərqlidir. CBR-sistemlərdə axtarış əsasən iki metoda əsaslanır: qərarlar ağacının qurulması üçün induktiv alqoritmlərdən istifadə edən induktiv metodlar və əvvəlcədən təyin edilən yaxınlıq metrikaları əsasında presedentləri klassifikasiya edən ən yaxın qonşu metodları [53, s.24].

Ən yaxın qonşular metodu geniş yayılmış və çox istifadə edilən yanaşmadır. k ən yaxın qonşu (*K*-nearest neighbors, *k-NN*) metodunda əvvəlcə presedentlər bazasından k oxşar presedent tapılır (adətən, $k = 3$ və ya $k = 5$), sonra seçilmiş yaxınlıq metrikası əsasında onların arasından baxılan presedentə ən yaxın olan presedent müəyyən edilir.

İki presedentin yaxınlıq dərəcəsi presedentlərin müvafiq əlamətlərinin yaxınlıq dərəcəsi əsasında tapılır. Hər bir əlamətə onun nisbi vacibliyini əks etdirən çəki əmsalı verilir. Bütün əlamətlər üzrə iki presedentin yaxınlıq dərəcəsini tapmaq üçün aşağıdakı düsturdan istifadə etmək olar:

$$sim(i,k) = \frac{\sum_{j=1}^{n} w_j \cdot sim(e_{ij}, e_{kj})}{\sum_{j=1}^{n} w_j}, \qquad (6.3.3)$$

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 bu seçimdən əhəmiyyətli dərəcədə asılıdır. Presedentlərin yaxınlıq metrikaları kimi ənənəvi olaraq Evklid məsafəsi, Mahalanobis məsafəsi, Manhetten metrikası, Hemminq, Rocers-Tanimoto yaxınlıq ölçüsü istifadə edilir. Digər yaxınlıq metrikaları da istifadə edilir [120, s.1532]: Rao, Jakkar, Qauss əmsalları, Mirkin yaxınlıq ölçüsü, Brey-Kertis metrikası və s.

İnT hadisələrinin 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. Bu nəzərə alınmaqla, iki növ yaxınlıq metrikasından istifadə olunması təklif olunur.

Ədədi və nominal qiymətlər alan əlamətlərin yaxınlığını heterogen məsafə funksiyasının (Heterogeneous Euclidean-Overlap Metric, HEOM) [302, s.1-34] əsasında müəyyən etmək təklif edilir, burada əlamətlərin müxtəlif növləri üçün fərqli məsafə funksiyaları istifadə edilir: nominal əlamətlər üçün örtülmə metrikası və ədədi əlamətlər üçün normallaşdırılmış Evklid məsafəsi. HEOM istifadə edilməklə iki x və c əlamətlər vektorları arasındakı $sim_v(x,c)$ məsafəsi aşağıdakı düsturla müəyyən edilir:

$$sim_v(x,c) = \sqrt{\sum_{i=1}^{m} d(x_i,c_i)^2}, \text{ burada} \tag{6.3.4}$$

$$d(x_i,c_i) = \begin{cases} 1, \text{əgər } x_i \text{ və } c_i - \text{nin tipləri məlum deyilsə,} \\ overlap(x_i,c_i), \text{əgər } x_i \text{ və } c_i \text{ simvol tiplidirsə,} \\ \dfrac{|x_i - c_i|}{max_i - min_i}, \text{əks halda} \end{cases}, \tag{6.3.5}$$

$$overlap(x_i,c_i) = \begin{cases} 0, \text{əgər } x_i \neq c_i \\ 1, \text{əgər } x_i = c_i \end{cases}. \tag{6.3.6}$$

İki semantik $a = (a1, a2, ..., an)$ və $b = (b1, b2, ..., bn)$ vektorları arasındakı yaxınlıq bu vektorlar arasındakı bucağın kosinusu ilə müəyyən edilir:

$$sim_s(a,b) = \frac{ab^T}{\|a\| \cdot \|b\|} \tag{6.3.7}$$

Verilmiş c və x presedent vektorlarının uyğun hissələrinin $sim_v(x,c)$ və $sim_s(x,c)$ yaxınlıqları əsasında x və c presedentləri arasındakı S yaxınlığı aşağıdakı funksiya ilə hesablanır:

$$S(x,c) = \alpha \cdot sim_v(x,c) + \beta \cdot sim_s(x,c). \tag{6.3.8}$$

α və β parametrləri yaxınlıq metrikalarının vacibliklərini müəyyən edirlər, məsələn, $\alpha = 0{,}6$ və $\beta = 0.4$ qəbul etmək olar.

Əlamətlərin çəkilərinin PSO metodu ilə optimallaşdırılması

CBR metodunda hər bir əlamət üçün uyğun çəkinin seçilməsi dəqiqliyə böyük təsir göstərir. Əgər presedentlər cütü arasında oxşarlığın müəyyən edilməsi prosesində əlamət vacibdirsə, onun çəkisi böyük olmalıdır. Son dövrlər çəkilərin optimallaşdırılması və əlamətlərin seçilməsi üçün genetik alqoritmlər (GA),

hissəciklər sürüsü ilə optimallaşdırma (Particle Swarm Optimization, PSO) və evolyusiya strategiyaları kimi evristik yanaşmalar geniş istifadə olunur.

Mövcud tədqiqatlar göstərir ki, çəkiləri PSO və ya GA ilə optimallaşdırılmış CBR metodu qiymətləndirmə nəticələrini əhəmiyyətli dərəcədə yaxşılaşdıra bilər [53, s.24]. Bundan başqa, CBR üçün optimal çəkilərin axtarışında PSO yanaşması GA-dan üstün ola bilər [53, s.24]. Buna görə, baxılan işdə CBR metodu üçün əlamətlərin optimal çəkilərinin tapılması üçün PSO metodu tətbiq edilmişdir.

PSO metodu qlobal optimallaşdırma məsələlərinin təqribi həllərinin tapılmasının effektiv metodlarından biridir. PSO ilk dəfə 1995-ci ildə C.Kennedi və P.Eberhart tərəfindən [201, s.39] qeyri-xətti funksiyaların optimallaşdırılması üçün təklif edilmişdi, sonradan çoxsaylı modifikasiyaları işlənmişdi. PSO qrupun, məsələn, quş dəstəsinin və balıq sürüsünün davranışının modelləşdirilməsinə əsaslanır. Genetik alqoritmlərdə olduğu kimi, PSO da axtarış fəzasının araşdırılması üçün potensial həllər populyasiyasından istifadə edir. Başlanğıc PSO populyasiyasını təsadüfi generasiya etmək olar. Potensial həllərin yeni nəslini generasiya etmək üçün PSO populyasiyanın fərdləri (hissəcikləri) arasında informasiya mübadiləsinə söykənir. Mahiyyətcə, hər bir fərd öz trayektoriyasını özünün əvvəlki ən yaxşı mövqeyinə (*pbest* – personal best) və özünün lokal qonşuluğunda əldə olunmuş əvvəlki ən yaxşı mövqeyə (*gbest* – global best) nəzərən tənzimləyir.

Hər bir mümkün həll ayrıca bir fərdin mövqeyinə uyğun gəlir. Fərdin cari mövqeyi (vəziyyəti) həllər fəzasında koordinatlar ilə xarakterizə olunur. Fərz edək ki, həllər fəzası d-ölçülüdür, sürünün i-ci fərdini d-ölçülü $X_i = (x_{i1}, \dots, x_{id})$ vektorudur, sürünün ən yaxşı fərdini (funksiyanın maksimal qiymətinə malik olanı) g indeksi ilə işarə edək. i-ci fərdin ən yaxşı mövqeyini $P_i = (p_{i1}, \dots, p_{id})$ ilə, i-ci fərdin sürətini (mövqeyinin dəyişməsi) isə $V_i = (v_{i1}, \dots, v_{id})$ ilə işarə edək.

PSO iterativ prosesdir. Hər bir iterasiyada əvvəlcə hər bir fərdin cari sürəti yenilənir; bu zaman fərdin cari sürəti, cari mövqe ilə əvvəlki ən yaxşı fərdi və qlobal mövqe arasındakı məsafə nəzərə alınır. Sonra hər bir fərdin mövqeyi bu fərdin yeni sürətinin qiyməti istifadə edilməklə yenilənir. Fərdlərin sürət və mövqe vektorlarının yenilənməsi aşağıdakı düsturlarla yerinə yetirilir (yuxarı indeks iterasiyanı bildirir):

$$V_i^{k+1} = wV_i^k + c_1 r_{i1}^k \left(P_i^k - X_i^k\right) + c_2 r_{i2}^k \left(P_g^k - X_i^k\right)$$
$$X_i^{k+1} = X_i^k + P_i^k, \tag{6.3.9}$$

burada: $i = 1, \dots, N$ və N – populyasiyanın sayıdır, w – inersiya əmsalıdır, c_1 və c_2 – *koqnitiv* və *sosial* parametrlər adlanan müsbət sabitlərdir, r_{i1} və r_{i2} – [0, 1] intervalında müntəzəm paylanmış təsadüfi ədədlərdir.

c_1 və c_2 parametrləri [0,2] intervalından seçilir, c_1 və c_2-nin kiçik qiymətləri fərdə hədəf fəzadan uzaqda gəzişməyə icazə verir, böyük qiymətlər isə axtarış sahəsinə və ya onun sərhədlərində kənara yetərincə sürətlə hərəkət etməyə şərait yaradır.

İnersiya əmsalı PSO-nun yığılması üçün vacibdir, onu əvvəlki sürətlərin cari sürətə təsirinə nəzarət etmək üçün istifadə edirlər. Eksperimentlər göstərir ki, axtarış fəzasının qlobal araşdırılması üçün başlanğıcda inersiya əmsalının qiymətini böyük seçmək, sonra isə inersiya əmsalını tədricən azaldaraq optimal həlli daha az sayda iterasiya ilə əldə etmək olar.

PSO metodunun əsas məqsədi yararlılıq funksiyasının optimallaşdırılmasından ibarətdir. Bu tədqiqatda isə əsas məqsəd əlamətlərin presedenti ən yüksək dəqiqliklə söyləməyə imkan verən optimal optimal çəkilərinin tapılmasıdır. Verilənlərin T test toplusu üçün yararlılıq funksiyası (f_T) aşağıdakı düsturla müəyyən olunur:

$$\max f_T = \sum_{k=1}^{n} hit_k, \tag{6.3.10}$$

burada: n – verilənlərin T test toplusunun ölçüsü, hit_k – gözlənilən nəticə (EO_k) ilə faktiki nəticənin (AO_k) üst-üstə düşmələrinin sayıdır, yəni əgər $EO_k = AO_k$ olarsa, $hit_k = 1$, əks halda $hit_k = 0$.

VI fəsil üzrə nəticələr

- E-dövlətin İnT-nin strateji idarə edilməsi üçün qeyri-səlis koqnitiv model təklif edilmiş və e-dövlətin İnT-nin idarə edilməsi sisteminin inkişafının müxtəlif strateji senariləri analiz edilmişdir [54, s.440-447];

- E-dövlətin İnT-nin idarə edilməsi strategiyalarının optimal seçilməsi üçün hiperoyun modeli işlənilmişdir [175, s.65-70];
- E-dövlətin İnT-nin situasiyalar üzrə idarə edilməsi üçün konseptual modeli işlənmiş və modelin presedentlər və PSO metodu əsasında reallaşdırılması üçün yanaşma təklif edilmişdir [53, s.24-33].

VII FƏSİL. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ METODLARI VƏ MODELLƏRİ

E-dövlətin İnT-nin səviyyəsinin qiymətləndirilməsi sahəsində elmi tədqiqatlar erkən mərhələdədir, onların metodoloji əsaslandırılması qənaətbəxş və tam deyil. E-dövlətin vətəndaşlarla və özəl sektorla əsas təmas xətti e-xidmətlərdən keçir və e-xidmətlərin İnT səviyyəsi, ümumiyyətlə, e-dövlətin İnT-nin idarə edilməsinin effektivliyi barədə fikir yürütməyə imkan verir. Bu səbəbdən baxılan fəsildə e-xidmətlərin təhlükəsizlik səviyyəsinin qiymətləndirilməsi üçün metod təklif edilir [182, s.1-4]. Mövcud kompozit indekslərdə onlara daxil olan fərdi indikatorların çəkiləri ya bərabər götürülür, ya da subyektiv təyin olunur. Bu nöqsanı düzəltmək üçün kompozit milli kibertəhlükəsizlik indekslərində indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi metodu təklif edilir və dinamik kibertəhlükəsizlik indeksləri daxil edilir [26, s.26]. E-dövlətin İnT səviyyəsini qiymətləndirmək üçün əks-əlaqənin ölçüsü kimi istifadəçilərin rəylərini nəzərə alan indikatorların işlənməsi də məqsədəuyğundur. Bu ideyanı həyata keçirmək üçün bu fəsildə e-dövlətin İnT-nə vətəndaşların etimadını qiymətləndirmək üçün bir model irəli sürülür [181, s.1-6].

7.1. E-xidmətlərin informasiya təhlükəsizliyinin qiymətləndirilməsi metodu

E-xidmətlər dövlət və özəl sektor xidmətlərinin İnternet üzərindən geniş istifadəçi kütləsinə təqdim olunmasının ümumi qəbul edilən metodudur. İnternetin əsas problemlərindən biri İnT olduğu üçün e-xidmətlərin təmin edilməsində də əsas amildir.

E-xidmətlərin iki əsas tətbiq sahəsi var: e-biznes (e-ticarət) və e-dövlət. E-dövlət seqmentində e-xidmətlərin İnT-nin təmin edilməsinin öz spesifik tələbləri var. Burada dövlət təşkilatları ikili rol oynayırlar – onlar həm e-xidmətlərin provayderləridir; eyni zamanda onlar digər dövlət orqanlarının məlumatlarından istifadə edərək e-xidmətlərin istehlakçısı kimi çıxış edirlər. E-dövlət xidmətlərinin digər istifadəçiləri kommersiya təşkilatları və fiziki şəxslərdir.

E-xidmətlərin İnT üçün müxtəlif təhlükəsizlik mexanizmlərindən geniş istifadə edirlər: şəbəkələrarası ekranlar, istifadəçilərin identifikasiyası və autentifikasiyası vasitələri, müdaxilələrin aşkarlanması və qarşısının alınması sistemləri, antivirus vasitələri, eləcə də təşkilati tədbirlər və s. Lakin bu mexanizmlərlə təmin edilən təhlükəsizlik səviyyəsinin qiymətləndirilməsi çox çətin məsələdir.

Bu bölmədə e-xidmətlərin təhlükəsizliyinin qiymətləndirilməsi modeli təklif edilir. İnformasiya təhlükəsizliyinin qiymətləndirilməsinə yanaşmalardan biri İnT-nin təmin edilməsi proseslərinin İnT tələblərinə uyğunluğunu qiymətləndirməkdir. Bu tələblər ən yaxşı təcrübə, standartlar və qaydalar əsasında müəyyən edilə bilər. Bunun üçün dayaq nöqtəsi rolunu İnT risklərinin analizi oynayır. Bəzi e-xidmətlər üçün spesifik təhlükəsizlik tələbləri vardır (məsələn, e-ticarət üçün PCI DSS, e-səhiyyə xidmətləri üçün HIPAA). Əlbəttə, təhlükəsizlik tələblərinin tam siyahısını tərtib etmək qeyri-mümkündür. Bu qeydə baxmayaraq, biz bütün e-xidmətlər üçün ümumi olan (X.800 təkliflərinə oxşar) bir neçə əsas təhlükəsizlik servisi müəyyən etməyin və onlar üçün müvafiq təhlükəsizlik tələbləri formalaşdırmağın mümkün olduğuna əminik.

Əlaqədar işlər. E-xidmətlərin təhlükəsizliyi məsələləri son 20 ildə tədqiqatçıların diqqətini cəlb etməkdədir [130, s.1, 82, s.47, 157, s.155, 259, s.1066, 197, s.1]. E-xidmətlər sahəsində təhlükəsizlik məsələlərinin ilk icmalı 2000-ci ildə aparılmışdır [233, s.157]. Bu icmalda e-xidmətlərin təsnifatı verilmiş və e-xidmət tətbiqlərində təhlükəsizlik tələblərinin analizi üçün model təklif edilmişdir.

E-dövlət xidmətlərindən istifadə edərkən güclü təhlükəsizliyin təmin edilməsi problemi [130, s.1-5]-da vurğulanır və bu sahədə son onillikdəki inkişaf təhlil edilir, dövlət e-xidmətləri üçün aktual təhlükəsizlik problemlərinin icmalı verilir.

E-xidmətlərin təhlükəsizliyi elmi ədəbiyyatda əsasən texnoloji baxımdan analiz edilir [233, s.157]. E-dövlət xidmətlərinin təhlükəsizliyində əsas problemlər istifadəçilərin identifikasiyası, autentifikasiyası, avtorizasiyası, tranzaksiyaların imzalanması, açıq və konfidensial informasiyanın təhlükəsiz şəkildə saxlanması, emalı, konfliktlərin həlli, İnT-nin auditi və s.-dir.

E-dövlət xidmətlərinin təhlükəsizlik tələbləri üçün təşkilati model e-dövlət sistemində hər bir xidmətin təhlükəsizlik risklərini müəyyənləşdirməyə imkan verir [182, s.1]. Bu təşkilati modelə əsaslanaraq [213, s.1873]-də e-dövlətin hər bir xidməti üçün təhlükəsizlik tələbləri təsnif edilir və açıq açarlar infrastrukturu (Public Key Infrastructure, PKI) əsasında bu tələbləri ödəyən inteqrativ platforma təklif edilir. Müəlliflər bu təhlükəsizlik tələblərinin həyata keçirilməsinin mümkünlüyünü e-dövlət modelinin Webocrat sistemində (www.webocrat.com) yoxlayırlar.

[82, s.47]-də məlumatlara giriş şablonları əsasında e-dövlət veb saytları üçün çoxsəviyyəli təhlükəsizlik arxitekturası təklif edilir və seçilmiş İordaniya e-dövlət veb saytlarının cari təhlükəsizlik səviyyəsini qiymətləndirilir.

E-dövlət sistemlərinə təhlükəsiz giriş e-dövlət xidmətlərində təhlükəsizlik və etimad üçün vacibdir. [157, s.155]-də e-dövlət xidmətlərinə giriş üçün istifadə edilən təhlükəsiz eID sistemini analiz edilir, bu sistemlərin e-xidmətlərin geniş istifadəsi üçün bazis olduğu və e-xidmətlərin legitimliyinin yüksəlməsinə gətirəcəyi fikri vurğulanır.

E-dövlət xidmətlərinin praktiki reallaşdırılmasında veb-servis texnologiyaları geniş istifadə olunur. E-dövlətin İnT-ni təkmilləşdirmək üçün veb-servis texnologiyalarında girişin idarə edilməsi modeli [311, s.210]-də təklif edilir. E-dövlət sisteminin [311]-də təklif edilən girişin idarə edilməsi arxitekturası autentifikasiya, avtorizasiya (PKI istifadə edilir) və rola əsaslanan girişə nəzarət (ing. Role Based Access Control – RBAC) hissələrindən ibarətdir.

Veb servislər e-xidmətlər və onların istehlakçıları arasında "əlaqələndirici körpü" kimi geniş istifadə olunur. [259, s.1066] veb servislərin tranzaksiya davranışını öyrənmək, əsas tranzaksiya protokollarını analiz etmək və onların təhlükəsizlik xassələrini verifikasiya etmək üçün model təklif edir.

[197, s.1-9] texniki və təşkilati təhlükəsizlik servislərinin "E-dövlətin yetkinlik modellərinə" (e-Government maturity model, eGMM) inteqrasiya edilməsi üçün "hərtərəfli çərçivə" hazırlamışdır. Bu çərçivə İnT-nin yetkinlik modeli mərhələlərini eGMM ilə birləşdirir və inteqral model dövlət qurumlarının təhlükəsiz e-xidmətlər göstərə biləcəyi bir yanaşma təmin edir.

E-xidmətlər üçün təhlükəsizlik servisləri

E-xidmətlər üçün təhlükəsizlik tələblərini e-xidmət provayderinin təhlükəsizlik siyasətində müəyyən etmək olar. Təhlükəsizlik siyasətinin tələbləri təhlükəsizlik servisləri ilə həyata keçirilir, öz növbəsində, təhlükəsizlik servisləri isə bir və ya daha çox təhlükəsizlik mexanizmləri ilə həyata keçirilir. Digər paylanmış sistemlər kimi, e-xidmətlər üçün də aşağıdakı İnT servisləri qurulmalı və istismar edilməlidir:

Avtorizasiya və ya girişə nəzarət servisi e-xidmətin və resursların icazəsiz istifadəsindən müdafiəni təmin edir. Giriş sorğusuna icazə verilməsinə və ya imtina edilməsinə qərar verərkən bu servis girişə nəzarət siyahılarından, giriş biletlərindən, parollardan və ya digər autentifikasiya məlumatlarından istifadə edə bilər.

Autentifikasiya servisi kommunikasiya tərəflərinin və informasiyanın mənbəyinin həqiqiliyini təsdiqləyir. Autentifikasiya biristiqamətli (adətən müştəri öz kimliyini serverə sübut edir) və qarşılıqlı ola bilər. Hazırda güclü autentifikasiya üçün ümumi qəbul edilən yanaşma Kerberos sisteminə və ya X.509 sertifikatları ilə kataloq xidmətlərinə əsaslanır [233, s.157].

Hesabatlılıq servisi kimin nəyi və nə vaxt etdiyinə dair sübutlar təmin edir.

Əlyetərlik servisi xidmətin hər tələb olunan zaman əlyetər olmasını təmin edir.

Konfidensiallıq servisi məlumatın icazəsiz açıqlanmasından qoruyur: konfidensial məlumatlara yalnız müvafiq giriş hüququ olan istifadəçilərə giriş imkanı verir və belə hüquqları olmayan istifadəçilərə məlumatın icazəsiz açıqlanmasının qarşısını alır. Adətən, məlumatın konfidensiallığı şifrləmə ilə təmin olunur.

Tamlıq servisi verilənlərə qəsdən və ya təsadüfən icazəsiz dəyişikliklər edilməsinin qarşısını alır. Servis tamlığın pozulması təhdidlərinə qarşı kriptoqrafik heş funksiyalardan və məlumatı autentifikasiya kodlarından istifadə edir.

İnkarın mümkünsüzlüyü servisi məlumatın mənşəyinin isbatını və çatdırılmasının isbatını təmin edir. Təminatı etibarlı üçüncü tərəf təqdim edir, onun təminatına etibar etmək üçün yetərli informasiya təmin edilir. Adətən, bu servis rəqəmsal imzalara əsaslanır.

Audit servisi e-xidmətlərin təhlükəsizliyinə təsir edən hadisələrin qeydiyyatını və İnT-ni pozmaq cəhdlərini aşkarlamaq üçün toplanmış məlumatların analizini təmin

edir. Analiz olunacaq hadisələrin tam siyahısı təhlükəsizlik siyasəti ilə müəyyən edilir. Aktiv audit ilə şübhəli hadisələr real zamanda monitorinq edilir.

E-xidmətin informasiya təhlükəsizliyinin qiymətləndirilməsi

E-xidmətin İnT-nin qiymətləndirilməsi iki mərhələdə həyata keçirilir:

1. E-xidmətdə bir İnT servisinin təmin etdiyi təhlükəsizlik səviyyəsinin qiymətləndirilməsi.
2. E-xidmətin ümumi təhlükəsizlik səviyyəsinin qiymətləndirilməsi.

Birinci mərhələdə bir təhlükəsizlik servisinin təhlükəsizlik reytinqi qiymətləndirilir. Təhlükəsizlik servisinin ranqı onun təmin edə bildiyi təhlükəsizlik səviyyəsinə görə müəyyənləşdirilir.

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

Xüsusi İnT indikatorlarının qiymətləndirilməsi aşağıdakı şkala ilə aparılır:

0 – tələblər yerinə yetirilmir;

0.25 – tələblər cüzi dərəcədə yerinə yetirilir;

0.5 – tələblər müəyyən dərəcədə yerinə yetirilir;

0.75 – tələblər, demək olar, tam yerinə yetirilir;

1 – tələblər tam yerinə yetirilir.

Qrup indikatorları $S_i, i = 1, .., m$ xüsusi indikatorların bərabər çəkilərə malik olmasını fərz etməklə, bu indikatorların ədədi ortası kimi müəyyən edilir:

$$S_i = \frac{1}{n_i} \sum_{j=1}^{n_j} M_{ij}, \qquad (7.1.1)$$

burada: M_{ij} – i-ci təhlükəsizlik servisi üçün j-ci xüsusi indikatorunun qiyməti; n_i – i-ci təhlükəsizlik xidməti üçün bütün xüsusi indikatorların sayıdır.

Xüsusi indikatorlar müxtəlif çəkilərə malik olduqda qrup indikatorları aşağıdakı kimi hesablanır:

$$S_i = \sum_{j=1}^{n_j} \alpha_{ij} M_{ij}, \qquad (7.1.2)$$

burada: α_{ij} – i-ci təhlükəsizlik servisi üçün j-ci xüsusi indikatorun çəkisidir.

E-xidmətin İnT-nin mövcud səviyyəsini (SL) ən zəif halqa qaydası ilə müəyyən etmək olar:

$$SL = \min_i S_i. \qquad (7.1.3)$$

7.2. Milli kibertəhlükəsizlik indeksinin qiymətləndirilməsi metodu

Mövcud və yeni yaranan kibertəhlükəsizlik təhdidlərinə qarşı effektiv əks-tədbirlər haqqında optimal qərarların qəbulu üçün milli kibertəhlükəsizliyin cari vəziyyətini qiymətləndirmək – ölçmək tələb edilir. Lakin kibertəhlükəsizliyin səviyyəsinin ölçülməsi məsələsi kifayət qədər mürəkkəb məsələdir. Kibertəhlükəsizlik səviyyəsinə təsir edən faktorlar kifayət qədər çoxdur, onlar dinamik dəyişirlər və bir-birilə mürəkkəb qarşılıqlı əlaqələri vardır. Seçilmiş indikatorlar çoxluğu əsasında formalaşdırılan indeks kibertəhlükəsizlik vəziyyətini ayrılıqda götürülmüş bir indikatordan daha dolğun əks etdirir. Bu baxımdan milli kibertəhlükəsizlik indeksinin işlənməsi vacibdir.

Mövcud milli kibertəhlükəsizlik indekslərinin analizi

Ölkələrin kibertəhlükəsizlik səviyyələrini qiymətləndirmək üçün bir sıra indekslər təklif edilmişdir, məsələn: Beynəlxalq Telekommunikasiya İttifaqının qlobal kibertəhlükəsizlik indeksi (Global Cybersecurity Index, GCI) [150, 151], Koreya İnternet və Təhlükəsizlik Agentliyinin təklif etdiyi *milli informasiya təhlükəsizliyi indeksi* (National Information Security Index, NISI) [26, s.16], milli kibertəhlükəsizlik indeksi (**National Cyber Security Index, NCSI**) [245], *kibertəhlükəsizlik indeksi* [26, s.16] və *milli kibertəhlükəsizliyin idarə edilməsi sisteminin yetkinlik modeli* (National Cybersecurity Management System Maturity Model, NCSecMS) [133, s.236]. Bu indekslərdən yalnız GCI və **NCSI** üçün ölkələr

üzrə qiymətləndirmələrin aparılması məlumdur. [309, s.1-9]-da texnoloji, hüquqi, iqtisadi, mədəni və beynəlxalq faktorları nəzərə almaqla kibertəhlükəsizlik indeksinin formalaşdırılması üçün ümumi konseptual model irəli sürülür. Aşağıda bəzi kibertəhlükəsizlik indekslərinin qısa icmalı verilir.

Qlobal kibertəhlükəsizlik indeksi GCI dövlətlərin kibertəhlükəsizlik səviyyəsini 5 əsas sahədə ölçmək və ranqlaşdırmaq məqsədi qoyur:

1) Hüquqi tədbirlər (kibercinayətkarlıq üzrə qanunvericilik, tənzimləmə);

2) Texniki tədbirlər (CERT, standartlar, sertifikatlaşdırma);

3) Təşkilati tədbirlər (siyasət, idarəetmə üzrə yol xəritəsi – strategiya, cavabdeh təşkilat, milli etalon qiymətləndirmə);

4) Potensial qurulması tədbirləri (standartların işlənməsi, insan resurslarının inkişafı, peşəkarların sertifikatlaşdırılması, təşkilatların sertifikatlaşdırılması);

5) Əməkdaşlıq (idarələrarası, idarədaxili, dövlət-özəl sektor, beynəlxalq).

GCI bu beş istiqaməti xarakterizə edən 25 indikatoru bir indeksdə birləşdirən kompozit indeksdir. Ölkələrin GCI indeksinin müəyyən edilməsi üçün ölkələrdən məlumatların toplanması 2014-cü ildən həyata keçirilir. Cədvəl 7.2.1-də bəzi ölkələrin 2015-ci il üçün GCI indeksləri göstərilir.

Cədvəl 7.2.1

Bəzi ölkələrin GCI indeksləri (2015) [151]

Ölkə	**Hüquqi**	**Texniki**	**Təşkilati**	**Potensial**	**Əməkdaşlıq**	**İndeks**	**Ranq**
Avstraliya	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	3
Rusiya	1.0000	0.3333	0.5000	0.3750	0.5000	0.5000	12
Polşa	1.0000	0.3333	0.6250	0.6250	0.2500	0.5294	11
Pakistan	0.2500	0.1667	0.0000	0.3750	0.1250	0.1765	23
Gürcüstan	0.7500	0.6667	0.7500	0.2500	0.2500	0.5000	12
Ukrayna	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	17
Albaniya	0.7500	0.3333	0.1250	0.1250	0.0000	0.2059	22
Keniya	1.0000	0.3333	0.2500	0.2500	0.5000	0.4118	15
Nepal	0.5000	0.0000	0.1250	0.0000	0.1250	0.1176	25

Bir çox ölkə eyni reytinqə malikdir, bu onların eyni hazırlıq səviyyəsinə malik olduğunu göstərir. Beləliklə, indeksin qranulyarlıq səviyyəsi aşağıdır, indeks ölkənin detallı potensialını və ya mümkün zəifliklərini xarakterizə etməyə deyil, kibertəhlükəsizlik hazırlığının səviyyəsini əks etdirməyə yönəlib.

NCSI milli kibertəhlükəsizlik **indeksi** – Estoniyada e-Governance Academy tərəfindən işlənmişdir [245].

Müəlliflərə görə, NCSI indeksinin məqsədi milli kibertəhlükəsizlik barədə dəqiq, aktual və əlyetər informasiya təmin edən kompleks ölçmə aləti təqdim etməkdir. Milli kibertəhlükəsizlik indeksi ölkənin əsas kibertəhdidlərin baş verməsinin qarşısının alınmasına hazırlığını və kiberinsidentlərin, kibercinayətlərin, irimiqyaslı kiber-krizislərin idarə edilməsinə hazırlığını ölçür. NCSI milli kibertəhlükəsizlik potensialının qurulmasında bir alət kimi istifadə edilə bilər.

İndeks ölkənin e-servislərdə imtinalar, verilənlərin tamlığının pozulması, verilənlərin konfidensiallığının pozulması kimi əsas kibertəhdidlərə qarşı nə dərəcədə yaxşı hazırlandığını ölçür. NCSI metodologiyası aşağıdakı istiqamətlər üzrə 12 indikatoru əhatə edir:

- Ümumi indikatorlar (1. Siyasətin işlənməsi; 2. Təhdidlərin qiymətləndirilməsi; 3. Kibertəhlükəsizlik təhsili)
- Baza indikatorları (4. Baza təhlükəsizliyi; 5. E-servislərin təhlükəsizliyi; 6. E-identifikasiya və e-imza; 7. Kritik informasiya infrastrukturunun təhlükəsizliyi)
- İnsidentlərin idarə edilməsi indikatorları (8. Kiberinsidentləri 24/7 rejimində cavablandırma mərkəzi; 9. Krizislərin idarə edilməsi; 10. Kibercinayətlərlə mübarizə; 11. Hərbi potensial)
- Beynəlxalq əməkdaşlıq indikatorları (12. Beynəlxalq təsir)

Bu 12 indikator bir neçə sub-indikatora və ölçülən aspektlərə malikdir.

Hər bir indikator qiymətə malikdir ki, bu onun indeksdəki nisbi vacibliyini göstərir. Qiymətlər aşağıdakılar nəzərə alınmaqla ekspertlər qrupu tərəfindən verilir:

- 1 bal – Müəyyən sahəni tənzimləyən hüquqi sənəd.
- 2-4 bal – Kibertəhlükəsizlik üzrə müəyyən cavabdehliyi olan bölmə.
- 2 bal – əməkdaşlıq formatı (şura, komitə və s.)
- 1-3 bal – Nəticə (sənəd, təlimlər, texnologiyalar və s.)

NCSI version 1.0-da maksimal qiymət 99 baldır. İndeks cədvəlində ölkənin NCSI faizi indeksin maksimal qiymətinə nisbətdə hesablanır. İndikatorların əlavə

edilməsindən və ya çıxarılmasından asılı olmayaraq, NCSI maksimal qiyməti həmişə 100 (100%) olur.

İndeksin ideyası milli səviyyədə əlyetər mənbələrdən verilənlərin toplanması və indeksi faktiki materiallar əsasında hesablamaqdır. Yəni, indeks yalnız əlyetər veb-saytlarla və ya rəsmi sənədlərlə təsdiqlənə bilən məlumatlardan istifadə edir.

NCSI metodologiyasında NCSI indeksinə əlavə olaraq, informasiya cəmiyyətinin inkişafı indeksi də (ISD Score) daxil edilir. ISD indeksi "ICT Development" və "Networked Readiness" indekslərinin ədədi ortası kimi hesablanır.

Ratio = NCSI Score – ISD Score fərqi NCSI və ISD indeksləri arasındakı asılılığı göstərir. Müsbət nisbət ölkədə milli kibertəhlükəsizliyin səviyyəsinin informasiya cəmiyyətinin inkişafına uyğun olduğunu və ya onu qabaqladığını göstərir. Mənfi nisbət göstərir ki, ölkənin elektron cəmiyyəti milli kibertəhlükəsizlik sahəsi ilə müqayisədə daha çox inkişaf edib.

NCSI v 1.0 indeksinin nöqsanı kimi bu indeksin mərkəzi hökumət tərəfindən milli səviyyədə həyata keçirilən kibertəhlükəsizlik tədbirlərinin mövcudluğunu qiymətləndirdiyini qeyd etmək olar. NCSI v 1.0 bu tədbirlərin keyfiyyətini və əməliyyat effektivliyini qiymətləndirmir.

Kibertəhlükəsizlik indeksi [26, s.16] İnT və risk menecmenti üzrə iki mütəxəssis (D. Geer və M. Pareek) tərəfindən təklif edilib. Bu indeks 2011-ci ilin aprelindən başlayaraq hər ay veb-saytda dərc olunur. İndeks 300-ə yaxın respondentin rəy sorğusu əsasında hesablanır. Sorğuya hücum aktorları (5 sual), hücum silahları (5 sual), hücum edənlərin motivasiyaları (3 sual), hücum hədəfləri (6 sual), müdafiə (2 sual), ümumi fikirlər (3 sual) daxildir. Respondent beş cavab variantından birini seçir: "sürətlə azalır", "azalır", "dəyişmir", "yüksəlir", "sürətlə yüksəlir".

NCSecMS modeli [133, s.236] metodologiya baxımından ISO 27001 və Cobit yanaşmasına əsaslanır. Bu modelə görə milli kibertəhlükəsizliyin maraqlı tərəfləri dövlət, özəl sektor, vətəndaş cəmiyyəti, akademiya (universitetlər, elmi tədqiqat təşkilatları və s.) və kritik infrastrukturdur. NCSecMS idarəetmə platforması 5 domendən ibarətdir: 1) strategiya və siyasət; 2) reallaşdırma və təşkiletmə; 3)

maarifləndirmə və kommunikasiya; 4) uyğunluq və koordinasiya; 5) qiymətləndirmə və monitorinq.

Kiberhazırlıq indeksi (Cyber Readiness Index, CRI) [148, s. 86] – beş sahədə: milli strategiya, insidentlərin cavablandırılması, e-cinayətlərlə mübarizə, informasiyanın paylaşılması və elmi-praktiki tədqiqatlar üzrə ilkin qiymətləndirmələr əsasında 35 ölkənin özlərinin İKT investisiyalarını və İnterneti qorumaqda yetkinliyini və öhdəliklərini müqayisə edir.

Kibergüc indeksi (Cyber Power Index, CPI) [148, s. 85-86] – bu indeksin məqsədi G20 ölkələrinin "kiberhücumlara qarşı durmaq və produktiv və təhlükəsiz iqtisadiyyat üçün zəruri olan rəqəmsal infrastruktur qurmaq" qabiliyyətlərini ölçməkdir. İndeksdə 4 kateqoriyada təşkil edilmiş 39 kəmiyyət və keyfiyyət indikatoru istifadə edilir.

"Security and Defence Agenda" tərəfindən aparılmış tədqiqatda 23 ölkənin kibertəhlükəsizlik hazırlığı qiymətləndirilmişdir [148, s. 55-72]. Tədqiqatın nəticəsində alınmış ranqlaşdırma baxılmış digər indekslərdən fərqli olaraq subyektiv ekspert qiymətləndirməsindən istifadə edir. O, dövlət, özəl sektor, beynəlxalq təşkilatlar və akademiyadan olan 80-dən çox kibertəhlükəsizlik eksperti arasında keçirilmiş sorğuya əsaslanır. Hesabatda kiberhücumlara qarşı dayanıqlığı qiymətləndirmək üçün Robert Lentz tərəfindən işlənmiş *kibertəhlükəsizlik yetkinlik modeli* istifadə edilir. Bu model kibertəhlükəsizlik hazırlığını və dayanıqlığını yaxşılaşdırmaq üçün beş-mərhələli yol xəritəsi təqdim edir. Bu mərhələlər kompüter təhlükəsizliyi gigiyenasının baza qaydalarının tətbiqindən başlayır, standartların istifadəsinə, prediktiv kiber hazırlığa və təchizat zəncirində risk menecmentinə keçir. Bu model ölkələrin kibertəhlükəsizlik hazırlığının qiymətləndirilməsi üçün ölçmə aləti kimi də istifadə edilir.

Kibertəhlükəsizliyin ölçülməsi üçün indikatorlar

Kibertəhlükəsizliyin ölçülməsinin bir sıra nəzəri və metodoloji problemləri mövcuddur.

Birinci problem kibertəhlükəsizlik indikatorlarının seçilməsi ilə əlaqəlidir: hansı ölçülər relevantdır və neçə ölçü götürülməlidir, qiymətləndirmə prosesində hansı informasiya istifadə edilməlidir? Bu seçim çox zaman statistikanın mövcudluğu ilə şərtlənir, lakin onun dərin nəzəri nəticələri vardır və qiymətləndirmənin nəticələrinə böyük təsir göstərir.

Bununla əlaqəli texniki problem seçilmiş hər bir ölçünü adekvat əks etdirən indikatorların seçilməsi ilə əlaqəlidir.

Adətən, kibertəhlükəsizliyin ölçülməsini riskin qiymətləndirilməsi ilə əlaqələndirirlər, lakin kibertəhlükəsizlik risklərini dəqiq müəyyən etmək çətindir. Bundan başqa, kibertəhlükəsizliyin təmin edilməsi üzrə fəaliyyət geniş məsələləri əhatə edir və onun ölçülməsini təkcə risklərin qiymətləndirilməsi ilə məhdudlaşdırmaq düzgün deyil.

Kibertəhlükəsizliyin ölçülməsi üzrə elmi tədqiqatlar və praktiki təşəbbüslər 2000-ci illərdən intensivləşir. Müvafiq elmi-tədqiqat və praktiki fəaliyyət istiqaməti *informasiya təhlükəsizliyi metrikaları* adlandırılır (ing. security metrics) [29, s.1-4].

Metrika, ölçü və indikator terminləri çox zaman sinonim kimi işlədilir. Bir çox halda bu üç termin arasında semantik fərq çox kiçik olsa da, onların məna müxtəlifliyini başa düşmək bəzi kontekstlərdə faydalı ola bilər. Bu anlayışların məzmununa qısa nəzər salaq. Ədəbiyyatda metrika anlayışının müxtəlif tərifləri rast gəlmək mümkündür. Bu işdə aşağıdakı tərif əsas götürülür [29, s.1]:

"*Metrika (ing. metrics) – fəaliyyətin məhsuldarlığı ilə əlaqəli relevant verilənlərin toplanması, analizi və hesabat verilməsi yolu ilə qərar qəbul edilməsini asanlaşdırmaq, faəliyyətin məhsuldarlığını və hesabatlılığı yaxşılaşdırmaq üçün tətbiq edilən alətlərdir.*" Sadə yanaşmada metrika ölçmə standartı və ya sistemidir. Baxılan halda, metrikalar təhlükəsizliyi ölçmək, xüsusilə təşkilatın təhlükəsizlik səviyyəsini ölçmək üçün standartdır.

İnformasiya təhlükəsizliyi metrikaları üzrə bir neçə milli və beynəlxalq standart işlənmişdir. Onlardan NIST SP 800-55 – informasiya sistemləri üçün təhlükəsizlik metrikaları üzrə qaydaları, NIST SP 800-80 – İnT üçün fəaliyyət məhsuldarlığı metrikalarının işlənməsi üçün qaydaları, ISO/IEC 21827 – sistemlərin təhlükəsizlik

mühəndisliyi üçün potensialın yetkinlik modelini və ISO/IEC 27004 standartını qeyd etmək olar. ISO/IEC 27004 standartında İnT-ni idarəetmə sisteminin effektivliyini qiymətləndirmək üçün müvafiq metrikaların yaradılması və istifadəsi üzrə tövsiyələr verilir.

Məlumdur ki, başqa fəaliyyət sahələrində fəaliyyətin məhsuldarlığını və qarşıya qoyulmuş məqsədlərə nail olunmasını ölçmək üçün bir sıra indikatorlar mövcuddur [29, s.1-4], məsələn, fəaliyyət məhsuldarlığının əsas indikatorları (Key Performance Indicators, KPI), kritik uğur faktorları (Critical Success Factors, CSF), əsas məqsəd indikatorları (Key Goal Indicators, KGI), balanslaşdırılmış indikatorlar sistemi (Balanced ScoreCard, BSC), təhlükəsizlik üzrə yetkinlik modelləri (COBiT, CERT/CSO, ISM3) və s.

Bu modellərin kibertəhlükəsizlik üçün modifikasiyaları üzərində işlər aparılır, lakin burada kibertəhlükəsizliyin xarakterindən irəli gələn bir sıra kritik problemlər mövcuddur.

Ümumiyyətlə, metrikaların işlənməsi üçün ən effektiv yol – biznes-məqsədin altməqsədlərə ayrılması, uyğun hərəkətlərin müəyyən edilməsi və onların hər birinə aid metrikanın seçilməsidir. Metrikaların biznes-məqsədlərə bağlı olmasını təmin edən ən sadə yanaşma isə GQM (Goal Question Metric) adlanan modeldir. Bu modeldə məqsədi aydınlaşdıran suallar verilir və hər suala uyğun metrika seçilir.

Kibertəhlükəsizlik metrikaları təhlükəsizliyin məqsədləri ilə əlaqəlidir. Təhlükəsizliyin məqsədləri arzu edilən nəticəni, metrikalar isə ona nail olunmasında irəliləyişi əks etdirir. Lakin İnT məqsədləri ilə İnT üzrə fəaliyyət arasında birbaşa əlaqə yoxdur. Təhlükəsizlik proseslərinə müəyyən təsir edərək, siz heç zaman deyə bilməzsiniz ki, təhlükəsizlik məqsədlərinə həqiqətən də yaxınlaşmısınız. Daha bir problem ölçmələrin fəaliyyətlə əlaqələndirilməməsidir, ölçmələr çox zaman nəticələrə fokuslanır. Nəticədə, kibertəhlükəsizlik məqsədləri üçün metrikaları tapmaq çətindir və onlar İnT-nin idarə edilməsi üçün o qədər də faydalı olmurlar.

Adətən, yaxşı metrikaların yaradılması üçün SMART (Specific, Measurable, Achievable, Relevant, Timely) metodikası istifadə edilir. Yaxşı metrikaların

yaradılması üçün digər yanaşmalar da mövcuddur [29, s.1-4]: PRAGMATIC, PURE, CLEAR və s.

Kibertəhlükəsizliyin təmin edilməsi proseslərinin və tədbirlərinin nəticəliliyini və effektivliyini izləmək üçün başlanğıcda hiss edilən nəticəsi olmayan və qiymətləndirilməsinə əhəmiyyətli zəhmət tələb edilən çox sayda metrika fikirləşmək lazım deyil. Əsas proseslər və tədbirlər üçün bir neçə metrika müəyyənləşdirmək lazımdır ki, kənarlaşma və potensial kənarlaşma haqqında vaxtında siqnal verə bilsin. Beləliklə, müəyyən kənarlaşma müşahidə etdikdə diaqnostika məqsədləri üçün operativ olaraq əlavə metrikalar daxil etmək olar ki, onlar da qiymətləndirilən prosesdə problemin daha diqqətli diaqnostikasına imkan yaradır. Eyni zamanda, bu metrikaların qiymətləndirilməsi periodunu və bu metrikalardan istifadəyə lüzum olmadığını müəyyən edən meyarları da müəyyən etmək zəruridir.

İkinci problem toplanmış informasiyanın istifadəsi ilə bağlıdır. Sonrakı bölmələr bu problemə həsr olunacaq. Müvafiq ölçülər və indikatorlar seçildikdən (və normallaşdırıldıqdan) sonra dəyərləndirmə etmək üçün onları zaman və/və ya fəzada müqayisə etmək lazımdır. Bir neçə indikatorla müqayisə aparmaq üçün ən azı iki alternativ üsul var: 1) "inkişaf profilləri"ndən istifadə etmək; 2) müxtəlif indikatorları kompozit indeksdə birləşdirmək.

Kompozit indekslərin qurulması problemləri

Kompozit indekslərin qurulmasında sıx əlaqəli olan addımların "ideal ardıcıllığı" [248, s. 19-43]-də geniş izah edilir. Kompozit indekslərin qurulmasında əsas problem informasiyanın necə aqreqasiya edilməsidir. Aqreqasiya probleminin qarşılıqlı əlaqəli iki aspekti var: 1) aqreqasiya zamanı komponentlərə çəkilərin təyin edilməsi və 2) aqreqasiya funksiyasının seçilməsi.

Çəkilərin təyin edilməsi metodları çoxdur: bərabər çəkilər, əsas komponentlər metodu/faktor analizi, iyerarxiyaların analizi metodu, birgə analiz (ing. conjoint analysis), "büdcənin paylanması" və s. İdealda, çəki hər bir indikatorun kompozit (inteqral) indeksə töhfəsini əks etdirməlidir. Bir çox kompozit indeks bərabər çəkilərə əsaslanır. Bu bütün indikatorların eyni dəyərə malik olması halına uyğun gələ bilər.

Alternativ kimi, bu səbəb nəticə əlaqələri haqqında yetərli biliyin olmaması və yaxud alternativ həllər haqqında konsensusun olmamasından da qaynaqlana bilər. Həmçinin, yüksək dərəcədə korrelyasiya edən dəyişənlərin kombinasiyası nəticəsində indeksə ikiqat hesablama elementi də daxil edilə bilər. Çəki verilənlərin keyfiyyətini də əks etdirə bilər, statistik etibarlı verilənlərə daha yüksək çəki verilə bilər.

İlk baxışda çəkilərin faktor analizi (əsas komponentlərin analizi) təyin edilməsi metodu daha obyektiv görünür, çünki çəkilər ekspertlər tərəfindən müəyyən edilmir, statistika metodu ilə verilənlərdən alınır. Lakin bu yanaşmanın bir neçə ciddi nöqsanı vardır. Birincisi, çəkilər verilənlərdən alındıqda onlar məkan və zamana görə sabit olmurlar, bu isə müqayisəni olduqca çətinləşdirir. İkincisi, faktor analizi çəkiləri ilkin verilənlərin dispersiyası (variasiyası) və kovariasiyası əsasında təyin edir. Bu kriteriya müxtəlif dəyişənlərin nisbi sosial-iqtisadi vacibliyini həmişə əks etdirmir. Buna görə də, statistik yanaşma ilə çəkilər obyektiv görünsələr də, onların yaxşı nəzəri bazası yoxdur.

İndikatorlar normallaşdırıldıqdan (standartlaşdırıldıqdan) sonra bir neçə aqreqasiya strategiyası var [248, s. 102-116]: xətti aqreqasiya, həndəsi aqreqasiya və çoxkriteriyalı aqreqasiya.

Xətti aqreqasiya metodunda hər bir alternativ indikatorların hər birinə görə qiymətləndirilir və indikatorların çəkilərinə vurulur. Konkret alternativ üçün bu hasillərin bütün indikatorlar üzrə cəmi həmin alternativin indeksini (ranqını) verir:

$$R_i = \sum_{j=1}^{n} w_i a_{ij} \qquad (7.2.1)$$

burada: R_i – i-ci alternativin indeksi, n – indikatorların sayı, a_{ij} – i-ci alternativin j-cu indikatora görə qiyməti (dəyəri), w_j – j-cu indikatorun çəkisidir, $0 \leq w_i \leq 1, \sum_{i=1}^{m} w_i = 1$.

Xətti aqreqasiya çox sadə olduğundan və tətbiqinin və interpretasiyasının asanlığı səbəbindən geniş yayılıb. Xətti aqreqasiya fərdi indikatorlar eyni ölçü vahidinə malik olduqda və miqyas effekti sayəsində sonrakı çoxqiymətlilik aradan qaldırıldıqda faydalıdır.

Xətti aqreqasiya metodunda fərz olunur ki, konkret indikatorun yekun indeksə payı digər indikatorların qiymətindən asılı deyil.

Həndəsi aqreqasiya metodunda alternativin hər bir indikator üzrə qiyməti həmin indikatorun çəkisinə qüvvətə yüksəldilir və bütün indikatorlar üzrə hasil hesablanır. *i*-ci alternativin *Ri* indeksi belə hesablanır:

$$R_i = \prod_{j=1}^{n} (a_{ij})^{w_j} \qquad (7.2.2)$$

burada: n – indikatorların sayı, a_{ij} – i-ci alternativin j-cu indikatora görə qiyməti, w_j – j-cu indikatorun çəkisidir, $0 \leq w_i \leq 1, \sum_{i=1}^{m} w_i = 1$.

Yuxarıdakı funksiyadan fərqli olan digər həndəsi aqreqasiya operatorları da vardır [121, s.1-18]. Həndəsi aqreqasiya xətti aqreqasiya ilə müqayisədə nəticədə daha çox dəyişkənlik yarada bilər. İndikator qiymətləri vurulduğundan, bir indikatorda kiçik ölçmə səhvi indeksdə əhəmiyyətli dəyişiklik yarada bilər. Bu cəhət onu indikator qiymətləri böyük variasiya mümkün olan subyektiv qiymətləndirmə nəticəsində alınması halı üçün daha az münasib edir.

Kompozit indekslərdə son dövrlər fundamental məsələyə – indeksin komponentləri arasında kompensasiya edilməmə məsələsinə xüsusi fikir verilir (bir ölçüdəki defisit digər ölçüdəki izafiliklə kompensasiya edilir). Kompensasiya etməyən yanaşma getdikcə daha çox tətbiq edilir. Məsələn, 2010-cu ildə BMT İnkişaf Proqramı tərəfindən hesablanan Human Development Index-də həndəsi orta istifadə edilir [121, s.1-18].

Kompensasiya edilməmə və verilənlərin zamana görə müqayisə edilə bilməsi kompozit indekslərin qurulmasında əsas məsələdir [237, s.1513]. Kompensasiya edilməyən kompozit indekslər qeyri-additiv yanaşmalarla əldə edilə bilər. Müqayisə edilmə məsələsi isə əsasən normallaşdırma metodundan asılıdır.

Xətti aqreqasiyada kompensasiya edilmə sabitdir, həndəsi aqreqasiyada isə kompozit indeksdə kiçik qiymətləri olan indikator olduqda kompensasiya edilmə aşağı olur.

Əgər kompensasiya yolverilən dirsə və həndəsi aqreqasiya istifadə edilirsə, onda bir indikator üzrə kiçik qiymətləri olan ölkə vəziyyəti düzəltmək üçün digər indikatorlar üzrə daha böyük qiymətlər almağa çalışmalıdır.

Müxtəlif məqsədlər eyni hüquqa və vacibliyə malikdirsə, onda kompensasiya edilməmə tələbi zəruri ola bilər. Bu kompozit indeksdə müxtəlif ölçülər cəlb edildiyi hala uyğundur, məsələn, ekologiya indeksində fiziki, sosial və iqtisadi verilənlər aqreqasiya edilə bilər. Əgər bir indikatordakı artımın digər indikatordakı azalmanı kompensasiya edə bilmədiyi qəbul edilirsə, onda nə xətti, nə də həndəsi aqreqasiya yararlı olmur. Bu halda aqreqasiya məsələsini multi-kriteriyalı yanaşma həll edə bilər, bu yanaşmada iki və daha çox məqsəd arasında kompromisin tapılması məsələsi formallaşdırılır. Məsələn, [313, s.169]-də aqreqasiya məsələsi çoxkriteriyalı optimallaşdırma məsələsi kimi həll edilir.

İndikator çəkilərinin hesablanması üçün entropiya metodu

İndikatorların çəkisini tapmaq üçün bir çox metod təklif edilmişdir. Lakin heç bir metod daha dəqiq nəticəyə zəmanət verə bilmir və qərar verən eyni şəxs müxtəlif çəkilər ala bilər, həm də hansı çəkinin doğru olmasını müəyyənləşdirmək üçün kriteriya yoxdur [26, s.16].

Bu tədqiqatda çəkiləri hesablamaq üçün entropiyadan istifadə edilir. İndikatorlara çəki təyin etmək üçün entropiya metodu aşağıdakı faktlara görə xüsusilə faydalıdır [26, s.16]: (1) bu metod hər hansı qərar qəbul edənin indikatoru ranqlaşdırmasını tələb etmir; (2) hər bir indikatorun nisbi çəkisini asan hesablamalarla əldə etmək olar. Başqa sözlə, qərar qəbul edənlər çəkilərin hesablanması üçün ölkələrin real göstəricilərindən istifadə edə bilərlər. Buna görə entropiya metodunun obyektiv çəki üsulu olduğunu iddia etmək olar. Beləliklə, çəkilərin hesablanmasına xas subyektivlik aradan qaldırılır.

Entropiya konsepsiyası fərz edir ki, əgər bir indikator üçün alternativlərin qiymətləri eyni olarsa, onda bu indikatoru irəlidə nəzərə almamaq olar. Oxşar olaraq, əgər bir indikator üçün bütün alternativlərin qiymətləri yaxın olarsa, bu indikatora təyin olunmuş çəki daha kiçik ola bilər. Digər tərəfdən, müəyyən alternativlər üzrə

indikatorun qiymətləri arasında fərqlər böyük olduqda indikator daha vacib hesab edilir.

Tutaq ki, *m* alternativin *n* indikatora görə qiymətləndirilməsi matrisi *D* verilib:

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccccccc} X_1 & X_2 & \cdots & X_j & \cdots & X_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ x_{i1} & x_{i2} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \ldots & \vdots & \cdots & \vdots \\ x_{m1} & x_{m2} & \ldots & x_{mj} & \cdots & x_{mn} \end{bmatrix} \end{array}, \qquad (7.2.3)$$

burada: A_i – baxılan *i*-ci alternativ (ölkə); x_{ij} – *i*-ci alternativin *j*-cu indikatora görə qiymətləndirilməsidir.

İndikatorların çəkilərini tapmaq üçün entropiya alqoritmini aşağıdakı kimi ifadə etmək olar:

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

$$r_{ij} = \frac{x_{ij} - \min\limits_i\{x_{ij}\}}{\max\limits_i\{x_{ij}\} - \min\limits_i\{x_{ij}\}} \qquad (7.2.4)$$

Addım 2. Entropiyanın hesablanması

n obyektin *m* indikatora görə qiymətləndirilməsi məsələsində *i*-ci indikatorun entropiyası belə müəyyən edilir:

$$H_j = -k\sum_{i=1}^{n} f_{ij} \ln f_{ij}, j = 1,2,\ldots,m, \qquad (7.2.5)$$

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

Addım 3. Entropiya çəkisinin müəyyən edilməsi

j-cu indikatorun entropiya çəkisini belə təyin etmək olar:

$$w_j = \frac{1-H_j}{m-\sum_{j=1}^{m} H_j}, \quad (7.2.6)$$

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

Cədvəl 7.2.2-də (7.2.3)-(7.2.6) düsturları əsasında MDB ölkələri üçün 2017-ci il qlobal kibertəhlükəsizlik indeksi verilənləri [150] ilə hesablanmış indikatorların entropiya və çəki qiymətləri verilmişdir. Göründüyü kimi, entropiyaya əsaslanan yanaşmada "Texniki" və "Potensialın inkişafı" indikatorlarına daha yüksək çəkilər verilir.

Cədvəl 7.2.2
İndikatorların entropiyaları və çəkiləri

İndikator	Entropiya	Entropiya əsasında çəki	Çəki (GCI metodologiyası)
Hüquqi	0.929	0.108	0.200
Texniki	0.821	0.273	0.200
Təşkilati	0.903	0.147	0.200
Potensialın inkişafı	0.805	0.296	0.200
Əməkdaşlıq	0.884	0.176	0.200

Statik və dinamik kibertəhlükəsizlik indeksləri

Aşağıda təklif edilən statik və dinamik kibertəhlükəsizlik indekslərinin işlənməsi zamanı [231, s.253]-də irəli sürülən yanaşma əsas götürülmüşdür.

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 Cybersecuriy Index, SCI) aşağıdakı kimi təyin etmək olar:

$$SCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^t}{x_{rj}^t}\right)^{\frac{1}{m}}, \quad (7.2.7)$$

burada: x_{rj}^t – j-cu indikatorun t zamanında istinad və ya baza qiymətidir, məsələn, indikatorun dünya üzrə orta qiymətdir. SCI-nin 1-dən böyük (kiçik) qiymətləri istinad qiymətindən yuxarı (aşağı) indikatorlara malik ölkələri göstərir.

Cədvəl 7.2.3-də (7.2.7) düsturu ilə MDB ölkələri üçün 2017-ci il qlobal kibertəhlükəsizlik indeksi verilənləri [150] əsasında hesablanmış statik kibertəhlükəsizlik indeksi qiymətləri verilmişdir. Hesablamalarda indikatorların baza

qiymətləri kimi MDB ölkələri üçün həmin indikatorların orta qiymətləri götürülmüşdür.

Cədvəl 7.2.3

Bəzi ölkələrin statik kibertəhlükəsizlik indeksləri

Ölkə	GCI	SCI
Azərbaycan	0.559	1.2383
Belarus	0.592	1.3295
Ermənistan	0.196	0.0406
Gürcüstan	0.819	1.9250
Qazaxıstan	0.352	0.6986
Qırğızıstan	0.270	0.4661
Moldova	0.418	0.8832
Özbəkistan	0.277	0.5772
Rusiya	0.788	1.8498
Tacikistan	0.292	0.1688
Türkmənistan	0.133	0.0477
Ukrayna	0.501	1.0120

Hər bir ölkə üçün t_0 zamanından t_1-ə verilənləri analiz etmək üçün aşağıdakı düsturla verilən "dinamik" kibertəhlükəsizlik indeksi (Dynamic Cybersecuriy Index, DCI) qurmaq olar:

$$DCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^{t_1}}{x_{ij}^{t_0}} \right)^{\frac{1}{m}}. \qquad (7.2.8)$$

Cədvəl 7.2.4-də (7.2.8) düsturu ilə MDB ölkələri üzrə t_1 = 2017 və t_0 = 2015-ci illər üçün qlobal kibertəhlükəsizlik indeksi verilənləri əsasında hesablanmış dinamik kibertəhlükəsizlik indeksləri verilmişdir.

Cədvəl 7.2.4

Bəzi ölkələrin dinamik kibertəhlükəsizlik indeksləri

Ölkə	DCI		Ölkə	DCI
Azərbaycan	2.0032		Ermənistan	5.05
Belarus	0.1396		Özbəkistan	12.16
Gürcüstan	1.7439		Rusiya Federasiyası	1.8471
Qazaxıstan	0.1396		Tacikistan	0.0629
Qırğızıstan	0.0629		Türkmənistan	0.0250
Moldova	1.4332		Ukrayna	1.2186

Çəkili qüvvətə əsaslanan SCI və DCI indeksləri ən böyük dəyişkənlik göstərən komponentlərə daha böyük çəki verir, DCI həm də mütləq zamana görə müqayisə etməyə imkan yaradır. DCI, aqreqasiya funksiyası istisna olmaqla, Kanada rifah indeksinə oxşardır [236, s.e-342].

Qeyd etmək vacibdir ki, statik indeks kompensasiya edilməmə xassəsinə malikdir, dinamik indeks isə indikatorların zamana görə müqayisə olunmasına imkan verir. Bu xassələr kompozit indekslər üçün olduqca vacibdir.

Gələcək tədqiqatlarda milli kibertəhlükəsizlik üçün digər indikatorları da əhatə edən yeni indeksin işlənməsinə ehtiyac vardır. Bu indeks kibertəhlükəsizliyə milli hazırlıq səviyyəsi ilə yanaşı, kibertəhlükəsizliyin cari səviyyəsini də əks etdirməlidir, o cümlədən, ölkənin informasiya infrastrukturunun inkişaf səviyyəsini və kiberhücumlar üçün cəlbediciliyini də nəzərə almalıdır.

Bu işdə indikatorların çəkilərinin hesablanmasında istifadə edilmiş entropiya yanaşmasını inkişaf etdirərək sistemin vəziyyətinin indikatoru kimi bütövlükdə milli kibertəhlükəsizlik sisteminin vəziyyətini qiymətləndirmək üçün istifadə etmək olar. Başqa sözlə, gələcək tədqiqatlarda entropiya yanaşması əsasında milli kibertəhlükəsizlik indeksinin işlənilməsinə də baxmaq olar.

7.3. E-dövlətin informasiya təhlükəsizliyinə vətəndaş etimadının qiymətləndirilməsi modeli

E-dövlət İKT-dən istifadə edilməklə, dövlət orqanlarının və vətəndaşların qarşılıqlı əlaqələrinin həyata keçirilməsinə imkan verən müəyyən kommunikativ infrastrukturun qurulmasını nəzərdə tutur. E-dövlətin əsas məqsədi dövlət orqanları arasında koordinasiyanın yaxşılaşdırılmasını (G2G, government to government), dövlət orqanları tərəfindən vətəndaşlara yüksək keyfiyyətli xidmətlərin göstərilməsini (G2C, government to citizens), dövlət orqanları ilə biznes sektoru arasında qarşılıqlı əlaqənin effektivliyinin yüksəldilməsini (G2B, government to business), qərarların qəbulunda dövlətlə vətandaşlar arasında qarşılıqlı əlaqənin tənzimlənməsini (G2N, government to non-government organizations), dövlət və elm, texnologiya,

innovasiya sektoru arasında qarşılıqlı əlaqəni (G2K, government to knowledge) təmin etməkdir [78, s.644].

Lakin vətəndaşların e-dövlət xidmətlərindən istifadə səviyyəsi bir sıra səbəblərdən arzu olunan səviyyədən aşağıdır [269, s. 113]. E-dövlət sistemlərinə etimadın olmaması e-dövlət xidmətlərinin yayılmasına əsas maneələrdən biridir [115, s.31]. Onlayn mühitdə etimad üçün maneələr qeyri-müəyyənlik şəraitindən qaynaqlanır, bu faktor e-dövlət xidmətlərindən istifadə zamanı İnT risklərini artırır. Etimad risklə birbaşa bağlıdır və qərar qəbul etdikdə nəzərə alınır. Istifadəçilərin e-dövlət xidmətlərindən istifadə etmək qərarı onların e-dövlətin İnT-nə olan etimadının səviyyəsindən asılıdır. Beləliklə, e-dövlət xidmətlərinin istifadəsi zamanı İnT-nə etimad məsələsi ön plana çıxır.

Etimad anlayışı. Etimad fundamental insan davranışıdır. Etimadı çox zaman cəmiyyətin "yapışqanı" adlandırırlar. Cəmiyyətin həyatı onun üzvləri arasındakı etimaddan çox asılıdır. Etimad bütün növ sosial institutların əsası hesab olunur. Etimad şəxsiyyətin sosial qruplarla və təşkilatlarla qarşılıqlı əlaqəsinin vacib amilidir.

Etimad humanitar (sosiologiya, psixologiya, iqtisadiyyat, politologiya) və texniki elmlərin müxtəlif sahələrində mühüm rol oynayır [181, s.1-6]. Etimada tərif vermək çətindir, çünki etimadın müxtəlif növləri var və onlar konkret kontekstdən asılı olurlar.

Kompüter elmləri sahəsindəki tədqiqatçılar bütün bu tədqiqatların nəticələrindən faydalanaraq e-kommersiya, p2p şəbəkələri, qrid kompütinq, semantik veb, veb servislər və mobil şəbəkələr sahəsində etimadın rolunu öyrənirlər [181, s.1-6].

Bu işdə etimad termini aşağıdakı kimi başa düşülür.

Etimad münasibətlərinin qurulması zamanı əsasən iki aktor çıxış edir – *etibar edən aktor* (inamın subyekti, ing. truster) və *etibar edilən aktor* (inamın obyekti, ing. trustee).

Etimad – A subyekti tərəfindən irəli sürülən subyektiv ehtimaldır, ehtimalın edilməsində məqsəd B subyektinin müəyyən bir əməliyyatı icra edib-etmədiyini proqnozlaşdırmaqdır.

Burada etimad dedikdə etibarlılıq başa düşülür, etimadın subyektivliyi vurğulanır, asılılıq (hərəkətlərə kənar təsirin göstərilməsi) və mənfəət faktorları (aktor öz qazancını maksimumlaşdırmağa cəhd edir) göstərilir. Agentlər arasında qarşılıqlı əlaqənin təkrarlanan olduğu güman edilir.

Etimad müxtəlif elm sahələrində və müxtəlif tədqiqatçılar tərəfindən müxtəlif bucaqlardan öyrənilsə də, ümumi olan bəzi əsas cəhətləri müəyyən etmək olar:

- Etimad yalnız ətraf mühit qeyri-müəyyən və riskli olduqda rol oynayır.
- Etimad əsasında müəyyən qərarlar qəbul edilir.
- Etimad əvvəlki bilik və təcrübə əsasında qurulur.
- Etimad fərdi rəy və dəyərlərə əsaslanan subyektiv anlayışdır.
- Etimad yeni biliklə və zamanla dəyişir, lakin təcrübənin köhnə etimad üzərində üstün təsiri var.
- Etimad kontekstdən asılıdır.
- Etimad çoxşaxəlidir.

Etimad *statik* və *dinamik* ola bilər. Statik etimadın qiyməti zamanla dəyişmir. Dinamik etimadın qiyməti isə zamana görə dəyişir. Etimad situasiyadan asılıdır. Məsələn, subyekt etimada əsaslanan qərarında situasiyadan asılı olaraq sərhəd qiymətinə dəyişiklik edə bilər.

A agenti B-nin etibarlılığı (ing. trustworthiness) haqqında inama malik olduqda A və B arasında *etimad münasibəti* mövcud olur. Lakin əks istiqamətdə inam (B agenti A-nın etibarlılığı haqqında) olmaya bilər, başqa sözlə, etimad münasibəti biristiqamətlidir (qeyri-simmetrikdir). Əgər iki agent arasında qarşılıqlı etimad münasibəti varsa, onu iki ayrı etimad münasibəti kimi təsvir etmək onları asılı olmadan emal etmək baxımından əlverişlidir.

Etimad münasibətlərinin *birbaşa etimad, tövsiyə olunan etimad, reputasiya əsasında qurulan etimad* kimi növləri vardır [181, s.1-6]. Əgər A B-yə etimad edirsə, bu münasibət birbaşa etimad münasibəti adlanır. Əgər A B-nin digər agentin etibarlılığı haqqında verdiyi tövsiyəyə etimad edirsə, onda A və B arasında tövsiyə olunan etimad münasibəti vardır. Reputasiya əsasında qurulan etimad münasibəti

paylanmış şəbəkə mühitində hamının etimad etdiyi etibarlı üçüncü tərəf mümkün olmadıqda daha çox istifadə edilir. Agentin reputasiyası onun keçmiş davranışları haqqında onunla qarşılıqlı təsirdə olan digər agentlərin verdiyi reytinq qiymətlər əsasında hesablanır.

Etimad və informasiya təhlükəsizliyi. Etimad məsələsi informasiya texnologiyaları üçün yeni deyil. Paylanmış sistemlərin etibarlılğı, multi-agent sistemləri, qeyri-müəyyənlik şəraitində qərar qəbulu üçün müəyyən etimad modelləri istifadə edilir. Paylanmış sistemlərdə İnT-nin təmin olunması funksiyalarından autentifikasiyanın, elektron imzanın, avtorizasiyanın reallaşdırılması etimad münasibətlərinə əsaslanır.

İnformasiya təhlükəsizliyi ilə etimad arasında mürəkkəb münasibət mövcuddur. Onlayn mühitdə İnT-nin təmin edilməsi mexanizmlərindən (məsələn, kriptoqrafik metodlardan) istifadə edilməsi etimadın yaranmasına və yüksəlməsinə şərait yaradır [20, s.12], eyni zamanda, İnT-nin pozulması halları da etimadı zədələyə bilər. Qanunvericilik bazasının, sertifikatlaşdırma, monitorinq və nəzarət sisteminin mövcudluğu kiberfəzada etimadın möhkəmləndirilməsinə kömək edir. Bundan başqa, qeyd edildiyi kimi, bir sıra İnT mexanizmlərinin (autentifikasiya, şifrləmə, e-imza və kriptoqrafik protokollar) paylanmış sistemlərdə reallaşdırılması tərəflər arasındakı etimad münasibətlərinə əsaslanır.

Onlayn mühitdə İnT-nin təmin edilməsi mərkəzləşdirilmiş etimad – üçüncü tərəf vasitəsilə qurulmuş etimad infrastrukturu və ya etimad şəbəkəsi ilə həyata keçirilir. Mərkəzləşdirilmiş etimad infrastrukturu e-dövlət mühitində açıq açarlar infrastrukturu əsasında sertifikat xidmətləri mərkəzləri şəbəkəsinin yaradılması ilə qurula bilər [57, s.18]. Bu şəbəkə e-imza sertifikatlarının vahid dövlət reyestrinin qurulmasına, dövlət informasiya sistemlərinin istifadəçiləri üçün e-imza sertifikatlarının hazırlanmasına və sertifikatların həyat tsiklinin təmin edilməsinə və vahid etimad fəzasının fəaliyyətinin təmin edilməsinə xidmət edir.

İnT ilə etimad arasındakı münasibətlər baxımından İnT mexanizmlərinə zəmanət (ing. information security assurance) anlayışına da toxunmaq zəruridir.

Etimad modelləri

Paylanmış sistemlərdə praktiki etimad sistemlərinin qurulması üçün bir sıra etimad modelləri təklif edilmişdir. Bu bölmədə bəzi etimad modellərinə qısa nəzər salınır.

Etimad binar (etimad/etimadsızlıq), diskret və kəsilməz qiymətlər ala bilər. Etimadın kəsilməz qiymətlər oblastı 0 – qeyri-müəyyənlik və 1 – tam etimad olmaqla [0, 1] parçası və ya 0 – tam etimadsızlıq, 0.5 – qeyri-müəyyənlik və 1 tam etimad olmaqla [0, 1] parçası ola bilər.

Bir sıra modellərdə etimad bir qiymətlə deyil, bir neçə qiymətlə (məsələn, etimadın qiyməti, etimadsızlığın qiyməti və qeyri-müəyyənliyin qiyməti) və ya intervalla göstərilə bilər. Bəzi modellərdə isə etimad reytinqlə, ranqla, ehtimalla, inamla (ing. belief), qeyri-səlis qiymətlərlə ifadə olunur.

Subyektiv məntiqə əsaslanan rəy modeli qeyri-müəyyənlik şəraitində etimad qiymətlərini hesablamaq üçün maraqlı yanaşmadır [190, s.34]. Modelin üstünlüyü rəylər barəsində fikir yürütmə imkanı və konsensus, tövsiyə və nizamlama operatorlarıdır. Zəif cəhəti – istifadəçilərin uyğun kəmiyyətləri dəqiq təyin edəcəklərinə zəmanət vermək mümkün deyil.

Stiven Marş geniş istinad edilən dissertasiyasında *etimadın formal modeli*ni təklif edir [230, s. 82-95]. Modeldə [-1; 1] parçasında tam etimadsızlıqdan tam etimada kimi etimadın qiymətini almaq üçün subyektiv dəyişənlər çoxluğu və onların kombinasiyası üsulu təklif edilir. Dəyişənlərin hər biri zamandan və kontekstdən asılıdır. Təsvir olunan sistemdə insan əvəzinə daha ümumi anlayış – agent anlayışı istifadə edilir. Marş etimadın üç növünü müəyyən edir [230, s. 55-58]: *baza etimadı* – istənilən kontekst üçün; *ümumi etimad* – iki agent arasında və onların qarşılıqlı əlaqəsinin istənilən konteksti üçün; *situasiya etimadı* – iki agent arasında konkret kontekst üçün.

Bayes yanaşmasına əsaslanan etimad modelləri reputasiyanın hesablanması üçün Bayes qaydasına və beta ehtimal paylanması funksiyasına əsaslanırlar [141, s.24]. Reputasiyanın aposterior qiyməti yeni qiymətlərin (reytinqlərin) aprior qiymətlərinin kombinasiyası kimi hesablanır. Reputasiyanın qiyməti α və β

parametrləri ilə verilmiş beta funksiyanın riyazi gözləməsi kimi göstərilə bilər, burada α – iştirakçının müsbət qiymətlərinin, β – mənfi qiymətlərinin sayıdır.

Etimadın hesablanması üçün *reputasiya modelləri* daha geniş yayılıb [265, s.33]. Reputasiya – müəyyən subyektin keyfiyyətləri, üstünlükləri və çatışmazlıqları əsasında formalaşmış ictimai fikirdir. Reputasiyanın qiyməti müsbət və mənfi rəylərin cəmi kimi hesablanır (məsələn, eBay). Belə metod primitiv və reputasiyanın qiyməti qeyri-dəqiq olsa da, şəffaflıq və istifadəçiyə anlaşıqlı olması onun vacib üstünlüyüdür.

SemanticWeb – bu etimad modelində iki agent arasında etimadı hesablamaq üçün onları birləşdirən bütün yollar hesablanır [141, s.24]. Hər bir yoldakı tilə aid edilən reytinq qiymətləri vurulur, yekun etimad qiymətinin hesablanması üçün bütün yollar üzrə qiymətlər toplanır.

FIRE (latınca "fides" ("etimad") və "reputasiya" hecalarından yaranıb) etimad və reputasiyanın dörd müxtəlif növünü inteqrasiya edir [171, s.119]:

Qarşılıqlı əlaqə etimadı keçmişdəki birbaşa qarşılıqlı əlaqə təcrübəsindən alınır. Qiymətləndirici hədəf agentin etibarlılığını müəyyənləşdirmək üçün onunla əvvəlki qarşılıqlı əlaqə təcrübəsindən istifadə edir.

Şahid reputasiyası agentin davranışı haqqında şahid məlumatlarından hesablanır. Agentlərin öz təcrübələrini bölüşəcəyinə ümid edərək, qiymətləndirici hədəf agent ilə qarşılıqlı əlaqəsi olan agentlərin rəylərini toplaya bilər. Bu məlumatlar şahid fikirləri əsasında hədəf agentin etibarlılığını qiymətləndirmək üçün istifadə oluna bilər.

Rola əsaslanan etimad agentlər arasında rola əsaslanan müxtəlif münasibətlərlə müəyyən olunur. Agentin keçmiş davranışı ilə yanaşı, etimadı tapmaq üçün digər məlumatlardan da istifadə etmək olar. Bunlar qiymətləndirici və hədəf agent arasında olan müxtəlif münasibətlər və ya sahə bilikləri ola bilər (məsələn, normalar və ya qanunvericilik sistemi). Məsələn, agentin sahibi onun etibarlı olmasını təsdiq edə bilər və ya etibarlı qrupun üzvü olan digər agentə etimad göstərə bilər.

Təsdiqlənmiş reputasiya agentin özü tərəfindən təqdim olunmuş üçüncü tərəf arayışlarından qurulur. Əvvəlki hallarda qiymətləndirici tələb olunan informasiyanı

özü toplamalıdır. Lakin qiymətləndirən agent də öz etibarlılığı haqqında arqumentlər təqdim etməklə qiymətləndiricinin etimadını qazanmağa çalışa bilər.

E-dövlətin İnT-nə etimadın faktorları

E-dövlətin İnT-nə etimad aşağıdakı faktorlar əsasında qurulur: fərdi məlumatların təhlükəsizliyi; İnT-nin təmin edilməsi mexanizmləri; e-dövlətlə vətəndaşlar arasında əks-əlaqə; İnT-ndən istifadənin rahatlığı.

Fərdi məlumatların və özəl yazışmaların təhlükəsizliyi (ing. privacy) informasiya sistemlərinə etimadın qurulmasında mühüm rol oynayır. Hazırda informasiya sistemləri fərdi məlumatları asanlıqla toplayır və onlara asan girişi təmin edir. Buna görə, fərdi məlumatların konfidensiallığının qəsdən və ya bilməyərəkdən pozulması riskləri artır və nəticədə istifadəçilərin informasiya sistemlərinin təhlükəsizliyinə etimadını azaldır.

İnformasiyanın konfidensiallığının, tamlığının və əlyetərliyinin pozulması da istifadəçilərin informasiya sistemlərinin təhlükəsizliyinə etimadını azaldır. Həyat tsiklinin bütün mərhələlərində müvafiq İnT mexanizmlərinin reallaşdırılması etimadın təmin olunması üçün vacib məsələdir.

Etimadın möhkəmləndirilməsinin əhəmiyyətli elementlərindən biri də e-dövlət və vətəndaşlar arasında əks-əlaqədir. Vətəndaşların e-dövlətin fəaliyyəti barədə məlumatlandırılması, İnT sahəsində görülən tədbirlər barədə məlumatlılıq səviyyəsinin artırılması, informasiya texnologiyaları və İnT sahəsində əhalinin maarifləndirilməsi etimadın qurulmasında vacib rol oynayır.

Etimada təsir edən digər atribut İnT-ndən istifadənin rahatlığıdır (ing. usability). Tədqiqatlar göstərir ki, istifadənin rahatlığı faktorları istifadəçilərin informasiya sistemlərinə, xüsusilə də veb-saytlara etimadına təsir edir, çünki onların qavranılan imkanlarını artırır. Bundan başqa, istifadənin rahatlığı etimadın zəruri şərtidir, çünki insanlar proqram təminatı sistemlərini düzgün istifadə etdiklərinə inanmaları zəruridir.

E-dövlətin İnTnə etimadın qiymətləndirilməsi modeli

E-dövlətin İnT-nə *etimad indeksi* anlayışı daxil etmək olar. Bu indeksin rəy sorğusu əsasında hesablanması nisbətən sadədir. “Siz elektron dövlətin İnT-nə etimad

edirsinizmi?" tipli sual və "Etimad edirəm", "Etimad etmirəm" və "Cavab verməkdə çətinlik çəkirəm" tipli cavablar olan rəy sorğusunun keçirilməsi nəzərdə tutulur. Etimad indeksi etimad edənlər və etimad etməyənlərin say fərqinin bütün respondentlərin sayına olan nisbəti kimi daxil edilir. Lakin bu yanaşma etimadın necə formalaşması sualına cavab verə bilmir.

Təklif edilən modeldə fərz olunur ki, vətəndaşın e-dövlətin İnT-nə etimadı onun informasiya əldə etdiyi müxtəlif mənbələr əsasında formalaşır:

– şəxsi təcrübə;
– sosial şəbəkə (qonşuların və dost-tanışların) rəyləri;
– KİV-lərdə ifadə olunan rəylər;
– dövlət orqanlarının təqdim etdikləri sertifikatlar və ya öhdəliklər.

Bu mənbələri modelin komponentləri adlandıraq və uyğun olaraq *I*, *W*, *M* və *S* simvolları ilə işarə edək.

Etimad qiymətini hesablamaq üçün e-dövlətin keçmiş davranışı haqqında modelin komponentləri üzrə relevant reytinqlər toplanmalıdır. Toplanmış reytinqlər çoxluğu e-dövlətin gələcək davranışını – gələcək qarşılıqlı təsirdə gözlənilən reytinq qiymətini qiymətləndirmək üçün istifadə olunur. Bu qiyməti hesablamaq üçün ümumi üsul çoxluqdakı bütün reytinqlərin ədədi ortasını hesablamaqdır. Lakin bu reytinqlər gözlənilən reytinq qiymətini hesablayarkən eyni dərəcədə relevant deyillər. Məsələn, bəzi reytinqlər digərlərindən köhnə ola bilər və daha az əhəmiyyətli görünə bilərlər. Bəzi reytinqlər daha etibarlı mənbələrdən gələ bilər ki, digərləri ilə müqayisədə ona daha böyük çəki verilməlidir. Buna görə də modelin hər bir komponenti üçün reytinq çəkisi funksiyası daxil edilir. Etimad qiyməti əlyetər bütün reytinqlərin çəkili ortası kimi hesablanır:

$$T_K(a,c) = \frac{\sum_{r_i \in R_K(a,c)} w_K(r_i) \cdot v_i}{\sum_{r_i \in R_K(a,c)} w_K(r_i)}, \qquad (7.3.1)$$

burada: *K* indeksi modelin komponentlərini bildirir və *I*, *W*, *M* və ya *S* ola bilər, $T_K(a,c)$ – *a* agentinin e-dövlətin İnT-nə etimadın *c* faktoruna nəzərən *K* komponenti üzrə hesablanmış etimad qiymətidir. $R_K(a,c)$ – *K* komponenti tərəfindən etimadı

hesablamaq üçün toplanmış reytinqlər çoxluğudur. $w_K(r_i) - r_i$ reytinqinin relevantlıq (etibarlılıq) dərəcəsini hesablamaq üçün reytinq çəki funksiyasıdır ($w_K(r_i) \geq 0$). $v_i - r_i$ reytinqinin qiymətidir. Çəkilərin cəminə bölməklə etimad qiyməti $[-1, 1]$ diapazonuna normallaşdırılır. Reytinq çəki funksiyaları $w_K(r_i)$ hər bir komponent üçün ayrıca müəyyən olunur.

Ümumi etimad qiyməti

$$T(a,c) = \frac{\sum_{K \in \{I,W,M,S\}} W_K \cdot T_K(a,c)}{\sum_{K \in \{I,W,M,S\}} W_K} \qquad (7.3.2)$$

kimi hesablanır, burada W_K müvafiq olaraq, komponentlərin uyğun çəki əmsallarıdır. Bu əmsallar baxılan məsələ üçün hər komponentin vacibliyinə uyğun olaraq seçilir.

E-dövlət kontekstində etimadın müxtəlif növlərinin araşdırılması həm elmi tədqiqatlar, həm də praktiki tətbiqlər üçün olduqca əhəmiyyətlidir. Gələcək tədqiqatlarda e-dövlətin İnT-nə etimadın tərkib hissələrinin və onların qarşılıqlı münasibətlərinin, etimad domenlərinin (obyektlərinin) xarakteristikalarının və etimadın qurulması mexanizmlərinin modelləşdirilməsi, e-dövlət kimi multi-agent sistemlərində etimad münasibətlərinin dəstəklənməsi üçün vahid infrastrukturun arxitektur modelinin işlənməsi nəzərdə tutulur.

VII fəsil üzrə nəticələr

- E-xidmətlərin dörd abstraksiya səviyyəsindən ibarət formal modeli və bu səviyyələrə yönəlmiş təhdidlərin qarşısını alacaq təhlükəsizlik servisləri təsvir edilmiş, e-xidmətlərin təhlükəsizlik səviyyəsi fərdi təhlükəsizlik servislərinin reytinqlərinin çəkili cəmi kimi müəyyən edilmişdir [182, s.1-6];
- Kompozit milli kibertəhlükəsizlik indekslərinə daxil olan indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi metodu işlənilmiş, statik və dinamik kibertəhlükəsizlik indeksləri təklif edilmişdir [26, s.16-27];
- E-dövlətin İnT-nə vətəndaşların etimadının qiymətləndirilməsi üçün müxtəlif mənbələrdən toplanmış etimad məlumatlarının mənbələrin relevantlıq dərəcələri əsasında aqreqasiyası modeli təklif edilmişdir [181, s.1-4].

NƏTİCƏ

Dissertasiya işində qoyulmuş məsələlərin həlli zamanı əldə olunmuş əsas elmi-nəzəri və elmi-praktiki nəticələr aşağıdakılardan ibarətdir:

1. E-dövlətin İnT-nin idarə edilməsi problemlərinin müasir vəziyyəti analiz və tədqiqi edilərək bu sahədə aktual multi-dissiplinar elmi-nəzəri və elmi-praktiki problemlər müəyyən edilmişdir [7, 10, 19, 30, 73, 77, 78, 79]. Bu nəticə informasiya təhlükəsizliyi sahəsində gələcək elmi-praktiki tədqiqatların planlaşdırılması və təşkili, həmçinin müvafiq təhsil pillələri üçün resursların yaradılması üçün sistemləşdirilmiş informasiya bazası kimi əhəmiyyətlidir.
2. E-dövlətin İnT-nin idarə edilməsinin konseptual modeli [18] və e-dövlətin İnT sisteminin konseptual arxitekturası təklif edilmişdir [179]. 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 [15] işlənmiş, qarşılıqlı asılı kritik informasiya infrastrukturlarında risklərin qiymətləndirilməsi metodu [49] və İnternet infrastrukturunun dayanıqlığının qiymətləndirilməsi modelləri [51] 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 [176] və barmaq izlərinin həqiqiliyinin aşkarlanması metodu [47] təklif edilmiş və barmaq izlərinin tekstur deskriptorları əsasında biometrik kriptosistemin sintezi üçün metod [185] işlənmişdir. Nəticənin elmi-praktiki əhəmiyyəti elektron identifikasiya (o cümlədən, e-pasport) sistemləri üçün yeni xidmətlər və məhsullara imkan yaradan texniki konsepsiyaların eksperimental isbatıdır.

5. İnT insidentlərinin aşkarlanması metodu [183] işlənmiş, insidentlərin çoxmeyarlı prioritetləşdirilməsi metodu [178] və insidentlərin emalı üzrə işlərin optimal planlaşdırılması metodu [21] təklif edilmişdir. Nəticənin praktiki əhəmiyyəti milli CERT sisteminin təkmilləşdirilməsi və müvafiq xidmətlərin təşkilində metodoloji baza təklif edilməsi ilə əsaslanır.
6. E-dövlətin İnT sahəsində koordinasiya səviyyəsinin qiymətləndirilməsi modeli [17], İnT-nin ikisəviyyəli iyerarxik idarəetmə sistemində investisiyaların koordinasiyası modeli [52] işlənmiş, beynəlxalq koalisiya modeli [23] 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 İnT-nin strateji idarə edilməsi üçün qeyri-səlis koqnitiv model [54], kibermüdafiə taktikasının seçilməsi üçün hiperoyun modeli [175] və operativ idarəetmə üçün situasiya üzrə idarəetmə modeli [53] 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 İnT səviyyəsinin qiymətləndirilməsi metodu [182], statik və dinamik kibertəhlükəsizlik indekslərinin qiymətləndirilməsi metodu [26] və e-dövlətin İnT-nə vətəndaş etimadının qiymətləndirilməsi modeli [181] işlənmişdir. Nəticənin elmi-praktiki əhəmiyyəti təklif edilmiş yanaşmaların elmi-praktiki əhəmiyyəti informasiya təhlükəsizliyi üzrə milli statistik hesabatlılıq sisteminin formalaşdırılması və informasiya təhlükəsizliyi səviyyəsini yüksəltmək məqsədilə müxtəlif istiqamətlərdə statistik analizlərin aparılmasında tətbiqi imkanları ilə əsaslanır.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI

1. Azərbaycan 2020: gələcəyə baxış inkişaf konsepsiyası // Azərbaycan Respublikası Prezidentinin 2012-ci il 29 dekabr tarixli 800 nömrəli Fərmanı ilə təsdiq edilmişdir. // URL: https://president.az/files/future_az.pdf. – 39 s.
2. Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı // Azərbaycan Respublikası Prezidentinin 2007-ci il 13 fevral tarixli 1963 nömrəli Sərəncamı ilə təsdiq edilmişdir. // URL: http://www.e-qanun.az/alpidata/framework/data/12/c_f_12804.htm
3. Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya // Azərbaycan Respublikası Prezidentinin 2014-cü il 2 aprel tarixli Sərəncamı ilə təsdiq edilmişdir // Respublika. – 2014, 3 aprel, – s. 5-6.
4. Azərbaycan Respublikasında yeni nəsil şəxsiyyət vəsiqəsinin tətbiqi ilə bağlı əlavə tədbirlər haqqında" // Azərbaycan Respublikası Prezidentinin 2014-cü il 28 noyabr tarixli 893 nömrəli Sərəncamı ilə təsdiq edilmişdir. // Respublika. – 2014, 29 noyabr, – s. 2.
5. Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası // Azərbaycan Respublikası Prezidentinin 2007-ci il 23 may tarixli sərəncamı ilə təsdiq edilmişdir. – Bakı: Azərbaycan Respublikasının Qanunvericilik Toplusu, 2007, 31 May, № 05, Maddə 535. s.1388-1412.
6. İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin 708 saylı Fərmanı // 26 sentyabr 2012-ci ildə imzalanmışdır. // URL: http://e-qanun.gov.az/framework/24353.
7. Əliquliyev, R. M. E-dövlətin informasiya təhlükəsizliyi: Aktual tədqiqat istiqamətləri / R. M. Əliquliyev, Y. N. İmamverdiyev // – Bakı: İnformasiya cəmiyyəti problemləri, – 2010. №1, – s. 3–13.
8. Əliquliyev, R. M. İnformasiya təhlükəsizliyi insidentləri. / R.M. Əliquliyev, Y.N. İmamverdiyev. – Bakı: İnformasiya Texnologiyaları, – 2012. – 212 s.

9. Əliquliyev, R. M. İnformasiya təhlükəsizliyi təhdidlərinin ranqlaşdırılmasının bir metodu haqqında / R. M. Əliquliyev, Y. N. İmamverdiyev, S.A. Derekhshandeh // – Bakı: İnformasiya texnologiyaları problemləri, – 2011. №1, – s. 46-56.
10. Əliquliyev, R. M. İnformasiya təhlükəsizliyinin multidissiplinar elmi-nəzəri problemləri / R. M. Əliquliyev, Y. N. İmamverdiyev, R. Ş. Mahmudov // – Bakı: İnformasiya cəmiyyəti problemləri, – 2017. №2, – s. 32–43.
11. Həmzəyev, R. F. E-dövlətdə CERT-komandaları şəbəkəsinin yaradılması / R. F. Həmzəyev, Y. N. İmamverdiyev // Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı"nın materialları, – Bakı: – 17 – 18 may – 2013, – s. 92-95.
12. Həsənov, Ə. Azərbaycan Respublikasında informasiya fəaliyyəti və təhlükəsizliyi siyasəti // – Bakı: "Geostrategiya" jurnalı, – 2014, № 01(19), – s. 3–15.
13. İmamverdiyev, Y. N. APT (Advanced Persistent Threat)-hücumların aşkarlanması üçün konseptual yanaşma // – Bakı: Milli təhlükəsizlik və hərbi elmlər, – 2018, №1(4), – s. 93-103.
14. İmamverdiyev, Y. N. E-dövlət üçün bulud texnologiyaları əsasında mobil elektron imza // İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, – Bakı: – 17 may, – 2015, – s. 138-141.
15. İmamverdiyev, Y. N. E-dövlətin informasiya təhlükəsizliyi təhdidlərinin konsensus ranqlaşdırılması metodu // – Bakı: İnformasiya texnologiyaları problemləri, – 2018. №2, – s.34-45.
16. İmamverdiyev, Y. N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya problemləri // – Bakı: İnformasiya cəmiyyəti problemləri, – 2014. № 2, – s. 24-30.
17. İmamverdiyev, Y. N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi modeli // – Bakı: İnformasiya texnologiyaları problemləri, – 2019. №1, – s. 47-58.

18. İmamverdiyev, Y. N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli // – Bakı: İnformasiya cəmiyyəti problemləri, – 2013. № 1 (7), – s. 20-31.
19. İmamverdiyev, Y. N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatların müasir vəziyyətinin analizi // – Bakı: İnformasiya cəmiyyəti problemləri, – 2012. № 2(6), – s. 19-26.
20. İmamverdiyev, Y. N. İnformasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması problemləri // – Bakı: İnformasiya cəmiyyəti problemləri, – 2015, №1, – s. 12-23.
21. İmamverdiyev, Y. N. İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərinin optimal planlaşdırılması modeli // – Bakı: İnformasiya texnologiyaları problemləri, – 2018. №2, – s. 80-91.
22. İmamverdiyev, Y. N. İnformasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması problemləri // İnformasiya təhlükəsizliyi üzrə III respublika elmi-praktiki seminarı, – Bakı: – 8 dekabr, – 2017, – s. 76-79.
23. İmamverdiyev, Y. N. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiya modeli // – Bakı: İnformasiya cəmiyyəti problemləri, – 2019. №1, – s. 14-20.
24. İmamverdiyev, Y. N. Kiberqoşunlar: funksiyaları, silahları və kadr potensialı // – Bakı: İnformasiya cəmiyyəti problemləri, – 2015. №2, – s. 15-25.
25. İmamverdiyev, Y. N. Milli İnternet infrastrukturunun dayanıqlığının qiymətləndirilməsi modeli // "Müdafiə və təhlükəsizlik" mövzusunda elmi-praktik konfrans, – Bakı: Azərbaycan Respublikası Silahlı Qüvvələrinin Hərbi Akademiyası, – 28 noyabr, – 2017, – s. 39.
26. İmamverdiyev, Y. N. Milli kiber-təhlükəsizlik üçün entropiya çəkiləri və dinamik indeks // – Bakı: İnformasiya cəmiyyəti problemləri, – 2018. №2, – s.16-27.
27. İmamverdiyev, Y. N. Yeni nəsil milli kibertəhlükəsizlik strategiyaları // – Bakı: İnformasiya cəmiyyəti problemləri, – 2013. № 2, – s. 42-51.
28. İmamverdiyev, Y. N. İnformasiya təhlükəsizliyi mütəxəssislərini sertifikatlaş-dırma sistemləri / Y. N. İmamverdiyev, A. E. Əliyev // Elmi-praktik konfrans

"İnformasiya sistemləri və metodların hərbi-dəniz kadrlarının hazırlanmasında rolu", – Bakı: – , – 2008, – s. 129-134.
29. İmamverdiyev, Y.N. Elektron dövlətin informasiya təhlükəsizliyi üçün diffuziya indeksi modeli // "Elektron dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı, – Bakı: – 4 dekabr, – 2014, – s.75-78.
30. İmamverdiyev Y.N., Etibarlı və təhlükəsiz elektron hökümət yaradılmasının bəzi məsələləri // 1-ci Beynəlxalq konfrans "Kibernetika və informatika problemləri", – Bakı: – 26 – 28 oktyabr, – 2006, c. 2, – s. 80-82.
31. Mehdiyev, R.Ə. Beynəlxalq informasiya təhlükəsizliyinin möhkəmləndirilməsinə ümumi yanaşmalar. Təhlükəsizlik məsələlərinə cavabdeh olan yüksək vəzifəli şəxslərin beynəlxalq görüşündə nitq. Yekaterinburq, 9 sentyabr 2011. URL: https://news.milli.az/politics/70342.html
32. Musayev, V. Y. İnformasiya təhlükəsizliyi sahəsində beynəlxalq çağırışlar, təşəbbüslər və öhdəliklər / V. Y. Musayev, Y. N. İmamverdiyev // İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, – Bakı: – 17 may, – 2015, – s. 102-105.
33. Алгулиев, Р. М. Пути повышения точности методов оценки рисков информационной безопасности / Р. М. Алгулиев, Я. Н. Имамвердиев, С. А. Дераkшанде // – Москва: Информационные технологии, – 2010. №12, – с. 6-11.
34. Алгулиев, Р. М. Методы обнаружения живучести в биометрических системах / Р. М. Алгулиев, Я. Н. Имамвердиев, В. Я. Мусаев // – Москва: Вопросы защиты информации, – 2009. 86 (3), – с. 16-21.
35. Алгулиев, Р.М. Модели и методы обеспечения информационной безопасности в компьютерных сетях / Автореф. дис. … док. тех. наук / – Баку, 2002. – 48 с.
36. Алгулиев, Р.М. Теоретико-игровая модель принятия решений Администратором Безопасности по борьбе с угрозами в корпоративных сетях // – Баку: Доклады АН Азербайджана, – 1999, 55 (3-4), – с. 54-60.

37. Алиев, Р. А. Методы и алгоритмы координации в промышленных системах управления / Р. А. Алиев, М. И. Либерзон, – Москва: Радио и связь, – 1987. – 208 с.
38. Алтунин, А.Е. Модели и алгоритмы принятия решений в нечетких условиях / А. Е. Алтунин. – Тюмень: Изд-во Тюменского государственного университета, – 2000. – 352 с.
39. Атаманчук, Г. В. Теория государственного управления: учебник / Г. В. Атаманчук. – Москва: Омега-Л, – 2010. – 526 с.
40. Бачило, И. Л. Правовая платформа построения электронного государства / И. Л. Бачило // – Москва: Информационное право, – 2008. №4, – с. 3-9.
41. Виттих, В. А. К определению понятия "ситуационное управление" / В. А. Виттих // Материалы XIV Международной конференции "Проблемы управления и моделирования в сложных системах", – Самара: – 19 – 22 июня, – 2012, – с. 112-115.
42. Добрынин, Н.М. Государственное управление: Теория и практика. Современная версия новейшей истории государства: Учебник. Т. 1 / Н.М. Добрынин; Науч. ред. А.Н. Митин. – Новосибирск: Наука, 2010. – 407 с.
43. Додонов, А. Г. Живучесть информационных систем / А. Г. Додонов, Д. В. Ландэ. – Киев: Наукова думка, – 2011. – 256 с.
44. Дремин, И. М. Вейвлеты и их использование / И. М. Дремин, О. В. Иванов, В. А. Нечитайло // – Москва: Успехи физических наук, – 2001. 171 (5), – с.465-501.
45. Еркин, А. В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // – Москва: Информационное общество, – 2012. Вып. 1, – с. 68-74.
46. Имамвердиев, Я. Н. Метод биометрического хеширования на основе ортогональных преобразований для защиты шаблонов отпечатков пальцев // – Москва: Вопросы защиты информации, – 2010. №4, – с. 18-23.

47. Имамвердиев, Я. Н. Метод обнаружения переделанных отпечатков пальцев на основе фрактальных характеристик // – Москва: Информационные технологии, – 2012. № 9, – с. 11-16.
48. Имамвердиев, Я. Н. Метод определения качества изображений отпечатков пальцев на основе дискретных вейвлет-преобразований // – Москва: Вопросы защиты информации, – 2010. №1, – с. 44-47.
49. Имамвердиев, Я. Н. Метод оценки рисков информационной безопасности в взаимосвязанных информационных инфраструктурах // – Орел: Информационные системы и технологии, – 2019. №1 (111), – с. 102-112.
50. Имамвердиев, Я. Н. Метод построения ансамбля классификаторов в мультибиометрических системах // – Москва: Приложение к журналу “Информационные технологии”, – 2011. №9, – с. 24-31.
51. Имамвердиев, Я. Н. Модели оценки живучести национальной инфраструктуры Интернета // – Москва: Телекоммуникации, – 2018. №12, – с.36-45.
52. Имамвердиев, Я. Н. Модель координации инвестиций в двухуровневых иерархических системах управления информационной безопасностью // – Москва: Экономическая безопасность и качество, – 2018. №3 (32), – с. 41-47.
53. Имамвердиев, Я. Н. Модель ситуационного управления информационной безопасностью электронного правительства // – Москва: Информационные технологии, – 2014. №8, – с. 24-33.
54. Имамвердиев, Я. Н. Нечеткая когнитивная модель стратегического управления информационной безопасностью электронного правительства // – Москва: Информационные технологии, – 2015. №6, – с. 440-447.
55. Имамвердиев, Я. Н. Разработка методов и алгоритмов синтеза асимметричных криптографических систем на эллиптических кривых / Автореф. дис. … канд. тех. наук / – Баку, 2006. – 20 с.

56. Имамвердиев, Я. Н. Создание CERT-команды для научной компьютерной сети AzScienceNet // – Bakı: İnformasiya cəmiyyəti problemləri, – 2011. №1, – s. 15-26.
57. Имамвердиев, Я. Н. Архитектура инфраструктуры доверия электронным документам в среде электронного государства / Я. Н. Имамвердиев, М. Ш. Гаджирагимова // – Москва: Телекоммуникации, – 2011. №11, – с. 18-26.
58. Имамвердиев, Я. Н. Метод оптимального слияния значений соответствия в мультибиометрических системах / Я. Н. Имамвердиев, Л. В. Сухостат // – Москва: Информационные технологии, – 2013. № 1, – с. 9-14.
59. Имамвердиев, Я. Н. Метод объединения решений классификаторов для задачи распознавания диктора / Я. Н. Имамвердиев, Л. В. Сухостат // – Минск: Информатика (ОИПИ НАН Беларуси), – 2015. 45 (1), – с. 17-25.
60. Камаев, В. А., Натров, В. В. Моделирование и анализ состояния информационной безопасности организации // – Тула: Известия ТулГУ. Технические науки, – 2011. Вып. 3, – с. 148-155.
61. Ляшенко, Е. Н. Разработка модели координации сил и средств в иерархической системе гражданской защиты населения / Е. Н. Ляшенко, В. Г. Шерстюк // Технологический аудит и резервы производства, – 2015, 4 (2), – с. 4-10.
62. Максимов, В. И. Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач / В. И. Максимов, Е. К. Корноушенко // Труды Института проблем управления РАН, – 1999, Т. 2, – с. 95-109.
63. Месарович, М. Теория иерархических многоуровневых систем : пер. с англ. / М. Месарович, Д. Мако, И. Такахара. – Москва: Мир, – 1973. – 344 с.
64. Омельченко, А. В. Теория графов / А. В. Омельченко. – Москва: МЦНМО, – 2018. – 416 с.
65. Павлов, А. Н. Мультифрактальный анализ сложных сигналов / А. Н. Павлов, В. С. Анищенко // Успехи физических наук, – 2007, 177 (8), – с. 859-876.

66. Почуев, С. И. Методический подход к решению задачи ранжирования степени угроз национальной безопасности / С. И. Почуев, В. П. Большаков // Информост, –2007, 53 (6), – с. 34-36.
67. Стюгин, М. А. Информационная безопасность «по существу» // Сб. науч. трудов: Актуальные проблемы безопасности информационных технологий, – Красноярск: СибГАУ, 2007, – с. 102-123.
68. Халиков, М.И. Система государственного и муниципального управления: учебное пособие / М.И. Халиков. – 3-е изд., – Москва: Флинта, – 2014. – 448 с.
69. Ходаков, В. Е. О развитии основ теории координации сложных систем / В. Е. Ходаков, Н. А. Соколова, Д. Л. Кирийчук // – Херсон (Украина): Проблеми інформаційних технологій, – 2014. № 02 (016), – с. 12-21.
70. Юдин, Е. Б. Моделирование устойчивости Интернет в условиях распространения вирусов и случайных отказов элементов сети // – Омск: Омский научный вестник, 2010. №1 (87), – с. 190-194.
71. Abbasi, A. Enhancing response coordination through the assessment of response network structural dynamics / A. Abbasi, A. Sadeghi-Niaraki, M. Jalili, et al. // PloS One, – 2018, 13 (2), e0191130. – p. 1-17.
72. Abdi, H. Principal component analysis / H. Abdi, and L. J. Williams // Wiley interdisciplinary reviews: Computational statistics, – 2010, 2 (4), – p. 433-459.
73. Abdullayeva, F. Analysis of security vulnerabilities in biometric systems / F. Abdullayeva, Y. Imamverdiyev, V. Musayev, et al. // Proc. of the 2nd International Conference "Problems of Cybernetics and Informatics"(PCI), Baku, – 2008, – p. 60-63.
74. Axelrod, R. Structure of decision: The cognitive maps of political elites. – NJ: Princeton University Press, – 1976. – 404 p.
75. Alberts, C. Managing information security risks: The OCTAVE (SM) approach / C. Alberts, A. Dorofee. – Boston, MA: Addison-Wesley Longman Publishing Co., –2002. – 512 p.

76. Alguliev, R. Quadratic Boolean programming model and binary differential evolution algorithm for text summarization / R. Alguliev, R. Aliguliyev, M.Hajirahimova // – Baku: Problems of Information Technology, – 2012, 2, – p. 20-29.
77. Alguliev, R. e-Government information security management research challenges / R. Alguliev, Y. Imamverdiyev // IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, – 2009, – p. 1-5.
78. Alguliev, R. Some conceptual views on information security of the society / R. Alguliev, Y. Imamverdiyev, F. Yusifov // Journal of Communication and Computer, – 2012, 9, – p. 644-648.
79. Alguliyev, R. Cyber-physical systems and their security issues / R. Alguliyev, Y. Imamverdiyev, L. Sukhostat // Computers in Industry, – 2018, 100, – p. 212-223.
80. Al-Kuwaiti, M. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability / M. Al-Kuwaiti, N. Kyriakopoulos, S. Hussein // IEEE Communications Surveys and Tutorials, – 2009, 11 (2), – p. 106-124.
81. Alonso-Fernandez, F. A comparative study of fingerprint image-quality estimation methods / F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, et al. // IEEE Transactions on Information Forensics and Security, – 2007, 2 (4), – p. 734-743.
82. Alsmadi, I. Security challenges for expanding e-governments' services // International Journal of Advanced Science and Technology, – 2011, 37 (12), – p. 47-61.
83. Aminanto, M. Deep learning in intrusion detection system: An overview / M. Aminanto, K. Kim // International Research Conference on Engineering and Technology, Legian Bali, Indonesia– 2016, p. 1–12.
84. ANSI T1A1.2 Working Group on network survivability performance. Technical report on enhanced network survivability performance. – 2001, – 68 p.

85. Ansink, E. International environmental agreements with support / E. Ansink, H. P. Weikard, & C. Withagen // Journal of Environmental Economics and Management, – 2019, 97, – p. 241-252.
86. Antunes, N. Defending against web application vulnerabilities / N. Antunes, M. Vieira // Computer, – 2012, 45 (2), – p. 66–72.
87. Anuar, N. A risk index model for security incident prioritization / N. Anuar, S. Furnell, M. Papadaki, et al. // Proc. of the 9th Australian Information Security Management Conference, Perth, Western Australia, Australia, – 2011, – p.25-39.
88. Arakala, A. Fuzzy extractors for minutiae-based fingerprint authentication / A. Arakala, J. Jeffers, K. Horadam // Proc. of the 2nd International Conference on Biometrics, Seoul, Korea, – 2007, – p. 760-769.
89. Atif, A. A case analysis of information systems and security incident responses / A. Atif, S. Maynard, G. Shanks // International Journal of Information Management, – 2015, 35 (6), – p. 717-723.
90. Aue, F. LDA at work: Deutsche Bank's approach to quantifying operational risk / F. Aue, M. Kalkbrener // Journal of Operational Risk, – 2007, 1 (4), – p. 49-93.
91. Aung, Z. A framework for modeling interdependencies in Japan's critical infrastructures / Z. Aung, K. Watanabe // International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, – 2009, – p. 243-257.
92. Avritzer, A. Survivability models for the assessment of smart grid distribution automation network designs / A. Avritzer, S. Suresh, D. Menasché, et al. // Proc. of the 4th ACM/SPEC International Conference on Performance Engineering, Prague Czech Republic, – 2013, – p. 241-252.
93. Basel Committee on Banking Supervision, International convergence of capital measurement and capital standards: A Revised Framework. – Basel: Bank for International Settlements, – 2004, – 254 p.
94. Bayramoglu, B. Climate agreements in a mitigation-adaptation game / B. Bayramoglu, M. Finus, and J. F. Jacques // Journal of Public Economics, – 2018, 165 (9), – pp. 101-113.

95. Bazen, A. Systematic methods for the computation of the directional fields and singular points of fingerprints / A. Bazen, S. Gerez // IEEE Trans. Pattern Analysis and Machine Intelligence, – 2002, 24 (7), – p. 905-919.
96. Bdeir, F. Networks of inter-organisational coordination during disease outbreaks / Ph.D. thesis/ – The University of Sydney, 2014. – 350 p.
97. Belanger, F., Carter, L. Trust and risk in e-government adoption / F. Belanger, L. Carter // Journal of Strategic Information Systems, – 2008, 17 (2), – p. 165-176.
98. Benabdallah, S. Security issues in e-government models: what governments should do? / S. Benabdallah, S. Guemara-ElFatmi, N. Boudriga // IEEE International Conference on Systems, Man and Cybernetics, Tunisia, Tunisia, – 2002, – p. 398-403.
99. Benzel, T. A strategic plan for cybersecurity research and development // IEEE Security & Privacy, – 2015, 13 (4), – p. 3–5.
100. Beynon, M. The Dempster-Shafer theory of evidence: an alternative approach to multicriteria decision modelling / M. Beynon, B. Curry, P. Morgan // Omega, – 2000, 28 (1), – p. 37–50.
101. Bhuyan, M. Detecting distributed denial of service attacks: Methods, tools and future directions / M. Bhuyan, H. Kashyap, D. Bhattacharyya, et al. // The Computer Journal, – 2013, 57 (4), – p. 537-556.
102. Bojadziev, G. Fuzzy logic for business, finance, and management (Advances in Fuzzy Systems: Applications and Theory − v. 23), 2nd edition. / G. Bojadziev, M. Bojadziev. – NJ: World Scientific Publishing Company, – 2007. – 232 p.
103. Boutaba, R. A network management viewpoint on security in e-services / R. Boutaba, B. Ishibashi, B. Shihada // IFIP 18th World Computer Congress TC11: Certification and Security in E-Services, Montréal, Québec, Canada, – 2003, – p. 17–45.
104. Butler, K. A survey of BGP security issues and solutions / K. Butler, T. Farley, P. McDaniel, J. Rexford // Proc. of the IEEE, – 2010, 98 (1), – p. 100-122.

105. Chandola,V. Anomaly detection: A survey / V. Chandola, A. Banerjee, V. Kumar // Journal of ACM Computing Surveys (CSUR), – 2009, 41 (3), – p. 1-58.
106. Chang, D. Applications of the extent analysis method on fuzzy AHP / D.Chang // European Journal of Operational Research, – 1996, 95 (3), – p. 649-655.
107. Chen, Y. Cyber security management and e-government / Y. Chen, P. Chong, B. Zhan // Electronic Government, – 2004, 1 (3), – p. 316-327.
108. Chen, Y. Fingerprint quality indices for predicting authentication performance / Y. Chen, S. Dass, A. Jain // Proc. of International Conference on Audio- and Video-Based Biometric Person Authentication, Rye Brook, NY, USA, – 2005, – p. 160-170.
109. Chen, Y. Combining SVMs with various feature selection strategies / Y. Chen, C. Lin // Studies in Fuzziness and Soft Computing. – Springer Nature Switzerland, – 2006, v. 207, – p. 315-324.
110. Chernobai, A. Operational risk. A guide to Basel II capital requirements, models, and analysis / A. Chernobai, S. Rachev, F. Fabozzi. – New Jersey: John Wiley Sons, – 2007. – 300 p.
111. Chua, A. An analysis of the delayed response to hurricane Katrina through the lens of knowledge management / A. Chua, S. Kaynak, S. Foo // Journal of the American Society for Information Science and Technology, – 2007, 58 (3), – p. 391-403.
112. Cichonski, P. Computer security incident handling guide / P. Cichonski, T. Millar, T. Grance, K. Scarfone. – NIST Special Publication 800-61, – 2012. – 147 p.
113. Clancy, C. Secure smartcard based fingerprint authentication / C. Clancy, N. Kiyavash, D. Lin // ACM SIGMM Workshop on Biometrics Methods and Applications, Berkeley, California, USA, – 2003, – p. 45-52.
114. Coles, S. An introduction to statistical modeling of extreme values / S. Coles. London: Springer-Verlag, – 2001. – 224 p.

115. Colesca, S. Increasing e-trust: A solution to minimize risk in e-government adoption / S. Colesca // Journal of Applied Quantitative Methods, – 2009, 4 (1), – p. 31-44.
116. Comfort, L., Ko, K., Zagorecki, A. Coordination in rapidly evolving disaster response systems: the role of information / L. Comfort, K. Ko, A. Zagorecki // American Behavioral Scientist, – 2004, 48 (3), – p. 295–313.
117. Conklin, W. Barriers to adoption of e-government / W. Conklin // Proc. of the 40th Annual Hawaii International Conference on System Sciences, Waikoloa, Hawaii, USA, – 2007, – p. 98–105.
118. Could it happen in your country? URL: http://research.dyn.com/2012/11/could-it-happen-in-your-countr/
119. Cruz, M. Modeling, measuring and hedging operational risk. – New York: John Wiley & Sons, – 2002. – 346 p.
120. Cunningham, P. A taxonomy of similarity mechanisms for case-based reasoning // IEEE Transactions on Knowledge and Data Engineering, – 2009, 21 (11), – p. 1532-1543.
121. De Muro, P. Composite indices of development and poverty: An application to MDGs / P. De Muro, M. Mazziotta, A. Pareto // Social indicators research, – 2011, 104 (1), – p. 1-18.
122. Debraj, R. Coalition formation. Handbook of game theory (eds. H. P. Young, S. Zamir). / R. Debraj, R. Vohra. – 2014, v. 4, – p. 239-326.
123. Delcambre, L., Giuliano, G. Digital government research in academia / L. Delcambre, G. Giuliano // IEEE Computer Society, – 2005, 38 (12), – p. 33.
124. Deng, L. A tutorial survey of architectures, algorithms, and applications for deep learning / L. Deng // APSIPA Transactions on Signal and Information Processing, – 2014, 3, – p. 1-29.
125. Dhamija, R., Dusseault, L. The seven flaws of identity management usability and security challenges / R. Dhamija, L. Dusseault // IEEE Security and Privacy, – 2008, 6 (2), – p. 24-29.

126. Dhillon, G. Current directions in IS security research: towards socio-organizational perspectives / G. Dhillon, J. Backhouse // Information Systems Journal, – 2001, 11 (2), –p.127-153.
127. Djidjev, H. A faster algorithm for computing the girth of planar and bounded genus graphs // ACM Transactions on Algorithms, – 2010, 7 (1), p. 1-16.
128. Dodis, Y. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Y. Dodis, L. Reyzin, A. Smith // International conference on the theory and applications of cryptographic techniques, Interlaken, Switzerland, – 2004, – p. 523-540.
129. Dolev, D. Internet resiliency to attacks and failures under BGP policy routing / D. Dolev, J. Sugih, M. Osnat, et al. // Computer Networks, – 2006, 50 (16), – p. 3183-3196.
130. Dorogovs, P. Overview of government e-service security challenges / P. Dorogovs, A. Romanovs // IEEE 3rd Workshop on Advances in Information, Electronic and Electrical Engineering, Vilnius, Lithuania, – 2015, – p. 1-5.
131. Dunne, P. Solving coalitional resource games / P. Dunne, S. Kraus, E. Manisterski, et al. // Artificial Intelligence, – 2010, 174 (1), – p. 20-50.
132. Ebrahim, Z. E-government adoption: architecture and barriers / Z. Ebrahim, Z. Irani // Business Process Management Journal, – 2005, 11 (5), – p. 589-611.
133. El Kettani, M. NCSecMM: A National Cyber Security Maturity Model for an Interoperable National Cyber Security Framework / M. El Kettani, T. Debbagh // Proc. of the 9th European Conference on e-Government, London, UK, – 2009, – p. 236-247.
134. Elgendy, A. Optimizing dynamic flexible job shop scheduling problem based on genetic algorithm / A. Elgendy, H. Mohammed, A. Elhakeem // International Journal of Current Engineering and Technology, – 2017, 7 (2), – p. 368-373.
135. Eloff, J. Information security management – a new paradigm / J. Eloff, M. Eloff // Proc. of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology, Fourways, South Africa, – 2003, – p. 130-136.

136. European Union Agency for Network and Information Security: ENISA Threat Landscape Report 2017 (ETL 2017). –2018. – 114 p.
137. Evangelopoulos, N. E. Latent semantic analysis / N. E. Evangelopoulos // Wiley Interdisciplinary Reviews: Cognitive Science, – 2013, 4 (6), – p. 683-692.
138. Fawcett, T. An introduction to ROC analysis / T. Fawcett // Pattern Recognition Letters, –2006, 27 (8), – p. 861-874.
139. Fiore, U. Network anomaly detection with the restricted Boltzmann machine / U. Fiore, F. Palmieri, A. Castiglione, A. Santis // Neurocomputing, – 2013, 122 (12), – p. 13-23.
140. Finus, M. Membership rules and stability of coalition structures in positive externality games / M. Finus, and B. Rundshagen // Social Choice and Welfare, – 2009, 32 (3), – p. 389-406.
141. Firdhous, M. Trust management in Cloud Computing: A critical review / M. Firdhous, O. Ghazali, S. Hassan // International Journal on Advances in ICT for Emerging Regions, – 2011, 4 (2), – p. 24–36.
142. Fountain, J. Central issues in the political development of the virtual state. / – M. Castells and G. Cardoso (eds.), The network society: From knowledge to policy. – Washington, D.C., Brookings Institution Press, – 2006. – p. 149-182.
143. Frachot, A. Loss distribution approach in practice. The Basel handbook: A guide for financial practitioners / A. Frachot, O. Moudoulaud, T. Roncalli. – 2003, – p. 527–555.
144. Fudenberg, D. Game theory / D. Fudenberg, J. Tirole. – Cambridge, MA: MIT Press, – 1991. –579 p.
145. FVC2000: The First International Fingerprint Verification Competition. URL: http://bias.csr.unibo.it/fvc2004/databases.asp.
146. FVC2004: The Third International Competition for Fingerprint Verification Algorithms, URL: http://bias.csr.unibo.it/fvc2004/.
147. Gao, N. An intrusion detection model based on deep belief networks / N. Gao, L. Gao, Q. Gao // Proc. of the 2nd International Conference on Advanced Cloud and Big Data, Huangshan, China, – 2014, – p. 247–252.

148. Gehem, M. Assessing cyber security: A meta-analysis of threats, trends, and responses to cyber attacks / M. Gehem, A. Usanov, E. Frinking, et al. – The Hague: The Hague Centre for Strategic Studies, – 2015. – 102 p.
149. Girma, A. Advanced machine language approach to detect DDoS attack using DBSCAN clustering technology with entropy / A. Girma, M. Garuba, R. Goel // Information Technology - New Generations, – 2017, – p. 125-131.
150. Global Cybersecurity Index 2017 – ITU. Geneva, 2017. 78 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-pdf-E.pdf.
151. Global Cybersecurity Index Cyberwellness Profiles. Geneva, 2015. 528 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
152. Glykas, M. (ed.) Fuzzy cognitive maps: Advances in theory, methodologies, tools and applications. – Berlin: Springer, – 2010. – 428 p.
153. Gordon, L. The economics of information security investment / L. Gordon, M. Loeb // ACM Transactions on Information and System Security, – 2002, 5 (4), – p. 438-457.
154. Grossklags, J. Secure or insure: An economic analysis of security interdependencies and investment types / Ph.D. Thesis / – University of California, Berkeley, 2009. – 244 p.
155. Grönlund, Å. Introducing e-gov: History, definitions, and issues / Å. Grönlund, T. Horan // Communications of the Association for Information Systems, – 2004, 15 (1), – p. 713-729.
156. Grubesic, T. A geographic perspective on commercial Internet survivability / T. Grubesic, M. O'Kelly, A. Murray // Telematics and Informatics, – 2003, 20 (1), – p. 51-69.
157. Gustafsson, M. Safe online e-services building legitimacy for e-government. A case study of public e-services in education in Sweden / M. Gustafsson, E. Wihlborg // JeDEM-eJournal of eDemocracy and Open Government, – 2014, 5 (2), – p. 155-173.

158. Haimes, Y. Risk analysis in interdependent infrastructures / Y. Haimes, J. Santos, K. Crowther, et al. // International Conference on Critical Infrastructure Protection, Hanover, NH, USA, – 2007, – p. 297-310.

159. Hall, C. Resilience of the Internet interconnection ecosystem / C. Hall, R. Anderson, R. Clayton, et al. // Economics of Information Security and Privacy III, Springer, New York, NY, – 2013, – p. 119-148.

160. Hao, F. Combining crypto with biometrics effectively / F. Hao, R. Anderson, J. Daugman // IEEE Transactions on Computers, – 2006, 55 (9), – p. 1081-1088.

161. Heegaard, P. Network survivability modeling / P. Heegaard, K. Trivedi // Computer Network, – 2009, 53 (8), – p. 1215-1234.

162. Heeks, R. Understanding e-governance for development / R. Heeks // Electronic Journal on Information Technology in Developing Countries, –2001, 11 (3), Article 3, – p. 1-27.

163. Hinton, G. Reducing the dimensionality of data with neural networks / G. Hinton, R. Salakhutdinov // Science, – 2006, 313 (5786), – p. 504-507.

164. Hof, S. Securing e-government / S. Hof, P. Reichstädter // International Conference on Electronic Government, Zaragoza, Spain, – 2004, – p. 336-341.

165. Holm, H. A large-scale study of the time required to compromise a computer system // IEEE Transactions on Dependable and Secure Computing, – 2014, 11 (1), – p. 2-15.

166. Hong, K. An integrated system theory of information security management / K. Hong, Y. Chi, L. Chao, et al. // Information Management Computer Security, – 2003, 11 (5), – p. 243-248.

167. Hossain, L. Disaster response preparedness coordination through social networks / L. Hossain, M. Kuti // Disasters, – 2010, 34 (3), – p. 755-786.

168. Hossain, L. Actor centrality correlates to project based coordination / L. Hossain, A. Wu, K. Chung // Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, Banff, Alberta, Canada, – 2006, – p. 363-372.

169. Howard, M. E-government across the globe: How will “e” change government? // Government Finance Review, – 2001, 17 (4), – p. 6-9.

170. Hu, X.Y. Regular and irregular progressive edge-growth Tanner graphs / X.Y. Hu, E. Eleftheriou, D. Arnold // IEEE Transactions on Information Theory, – 2005, 51 (1), – p. 386-398.

171. Huynh, T. An integrated trust and reputation model for open multi-agent systems / T. Huynh, N. Jennings, N. Shadbolt // Autonomous Agents and Multi-Agent Systems, – 2006, 13 (2), – p. 119-154.

172. Xiao, L. K-means algorithm based on particle swarm optimization algorithm for anomaly intrusion detection / L. Xiao, Z. Shao, G. Liu // The 6th World Congress on Intelligent Control and Automation, Dalian, China, – 2006, – p. 5854-5854.

173. Xie, L. Modeling and quantifying the survivability of telecommunication network systems under fault propagation / L. Xie, P. Heegaard, Y. Jiang // Meeting of the European Network of Universities and Companies in Information and Communication Engineering, Chemnitz, Germany, – 2013, – p. 25-36.

174. Xu, H. Spectral minutiae: A fixed-length representation of a minutiae set / H. Xu, R. Veldhuis, T. Kevenaar, et al. // Proc. of Computer Vision and Pattern Recognition Workshop, Anchorage, AK, USA, – 2008, – p. 1-6.

175. Imamverdiyev, Y. A hypergame model for information security // 6th International Conference on Information Security and Cryptology (ISCTurkey), Ankara, Turkey, – 2013, – p. 65-70.

176. Imamverdiyev, Y. A model of fusion of information on image quality based on the Dempster-Shafer theory for biometric systems interoperability // Journal of Automation and Information Sciences, – 2010, 42 (2), – p. 66-74.

177. Imamverdiyev, Y. An application of extreme value theory to e-Government information security risk assessment // 7th IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, – 2013, – p. 349-352.

178. Imamverdiyev, Y. An information security incident prioritization method // 7th IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, – 2013, – p. 183-187.
179. Imamverdiyev, Y. Architecture of e-government information security management system // Proc. of the 3rd International Conference "Problems of Cybernetics and Informatics" (PCI), Baku, – 2010, – p. 79-82.
180. Imamverdiyev, Y. Consensus ranking method of information security threats of a nation state // II Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", Kropyvnytskyi, Ukraine,– 2017, – p. 12-13.
181. Imamverdiyev, Y. E-government information security trust assessment model // International Journal of Research Studies in Computer Science and Engineering, – 2016, 3 (2), – p. 1-6.
182. Imamverdiyev, Y. E-services security assessment model // 10th IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, – 2016, – p. 1-4.
183. Imamverdiyev, Y. Deep learning method for denial of service attack detection based on restricted Boltzmann machine / Y. Imamverdiyev, F. Abdullayeva // Big Data, – 2018, 6 (2), – p. 1-17.
184. Imamverdiyev, Y. A method for cryptographic key generation from fingerprints / Y. Imamverdiyev, L. Sukhostat // Automatic Control and Computer Sciences, – 2012, 46 (2), – p. 66-75.
185. Imamverdiyev, Y. Biometric cryptosystem based on discretized fingerprint texture descriptors / Y. Imamverdiyev, A. Teoh, J. Kim // Expert Systems with Applications, – 2013, 40, – p.1888-1901.
186. ITU National Cybersecurity Strategy Guide. – Geneva, – 2012. – 122 p.
187. Jabid, T. Local directional pattern (LDP) - A robust image descriptor for object recognition / T. Jabid, M. Kabir, O. Chae // Proc. the 7th IEEE International Conference on Advanced Video Signal based Surveillance, Boston, MA, USA, – 2010, – p.482-487.

188. Jain, A. Filterbank-based fingerprint matching / A. Jain, S. Prabhakar, L. Hong, et al. // IEEE Transactions on Image Processing, – 2000, 9 (5), – p. 846–859.
189. Jan van Bon (ed.) Foundations of ITIL V3. 1st edition. – Zaltbommel (NL): Van Haren Publishing, – 2007. – 360 p.
190. Jøsang, A. Artificial reasoning with subjective logic / A. Jøsang // Proc. of the 2nd Australian Workshop on Commonsense Reasoning, Perth, Western Australia, Australia, – 1997, v. 48, – p. 34-50.
191. Joshi, J. Digital government security infrastructure design challenges / J. Joshi, A. Ghafoor, W. Aref, et al. // IEEE Computer, – 2001, 34 (2), – p.66-72.
192. Juels, A. A fuzzy vault scheme / A. Juels, M. Sudan // Proc. of IEEE International Symposium on Information Theory, Lausanne, Switzerland, – 2002, – p. 408.
193. Juels, A. A fuzzy commitment scheme / A. Juels, M. Wattenberg // Proc. of the 6th ACM Conference on Computer and Communications Security, Singapore, – 1999, – p. 28-36.
194. Kacem, I. Approach by localization and multiobjective evolutionary optimization for flexible job-shop scheduling problems / I. Kacem, S. Hammadi, P. Borne // IEEE Transactions on Systems, Man, and Cybernetics, Part C, – 2002, 32 (1), – p. 1-13.
195. Kahan, J. Theories of coalition formation. / J. Kahan, A. Rapoport. – New York: Psychology Press, – 2014. – 384 p.
196. Kapucu, N. Interorganizational coordination in dynamic context: Networks in emergency response management / N. Kapucu // Connections, – 2005, 26 (2), – p. 33-48.
197. Karokola, G. Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models / G. Karokola, S. Kowalski, L. Yngström // Information Security for South Africa, Johannesburg, South Africa, – 2011, – p. 1-9.
198. Kaspersky DDoS attacks in Q3 2017, Kaspersky, URL: https://securelist.com/ddos-attacks-in-q3-2017/83041/

199. Katz, M. Fractals and the analysis of waveforms / M. Katz // Computers in Biology and Medicine, – 1988, 18 (3), – p. 145-156.

200. Kelkboom, E. Binary biometrics: an analytic framework to estimate the performance curves under Gaussian assumption / E. Kelkboom, G. Molina, J. Breebaart, et al. // IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, – 2010, 40 (3), – p. 555-571.

201. Kennedy, J. A new optimizer using particle swarm theory / J. Kennedy, R. Eberhart // Proc. of the 6th International Symposium on Micro Machine and Human Science, Nagoya, Japan, – 1995,– p. 39-43.

202. Kevenaar, T. Face recognition with renewable and privacy preserving binary templates / T. Kevenaar, G. Schrijen, M. van der Veen, A. Akkermans, F. Zuo // Proc. of the 4th IEEE Workshop on Automatic Identification Advanced Technologies, Buffalo, NY, USA, – 2005, – p. 21-26.

203. Kim, J. Error performance and decoder hardware comparison between EG-LDPC and BCH codes / J. Kim, J. Cho, W. Sung // Proc. of the IEEE Workshop on Signal Processing Systems, San Francisco, CA, USA, – 2010, – p. 392-397.

204. Klimburg, A. (ed.) National cyber security framework manual. – Tallinn: NATO CCD COE Publication, – 2012. – 235 p.

205. Koong, K. Identity theft in the USA: Evidence from 2002 to 2006 / K. Koong, L. Liu, S. Bai, et al. // International Journal of Mobile Communications, – 2008, 6 (2), – p. 199-216.

206. Kosfeld, M. Institution formation in public goods games / M. Kosfeld, A. Okada, A. Riedl // American Economic Review, – 2009, 99 (4), – p. 1335-1355.

207. Kosko, B. Fuzzy cognitive maps // International Journal of Man-Machine Studies, – 1986, 24 (1), – p. 65-75.

208. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D. Interdependencies between critical infrastructures: Analyzing the risk of cascading effects / P. Kotzanikolaou, M. Theoharidou, D. Gritzalis // International Workshop on Critical Information Infrastructures Security, Lucerne, Switzerland, – 2011, – p. 104-115.

209. Krackhardt, D. Graph theoretical dimensions of informal organizations // Computational organization theory, 1994, p. 89-111.

210. Kryszczuk, K. A. Error handling in multimodal biometric systems using reliability measures / K. Kryszczuk, J. Richiardi, P. Prodanov, A. Drygajlo // Proc. of the 13th European Signal Processing Conference, Antalya, Turkey, – 2005, – p. 1-4.

211. Kunreuther, H. Interdependent security / H. Kunreuther, G. Heal // Journal of Risk and Uncertainty, – 2003, 26 (2-3), – p. 231-249.

212. Kuypers, M. An empirical analysis of cyber security incidents at a large organization/ M. Kuypers, T. Maillart, E. Paté-Cornell. Working Paper. – 2016, – 22 p.

213. Lambrinoudakis, C. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy / C. Lambrinoudakis, S. Gritzalis, F. Dridi, et al. // Computer Communications, – 2003, 26 (16), – p. 1873-1883.

214. Larochelle, H. Classification using discriminative restricted Boltzmann machines / H. Larochelle, Y. Bengio // Proc. of the 25th ACM International Conference on Machine Learning, Helsinki, Finland, – 2008, – p. 536-543.

215. Laszka, A. A survey of interdependent information security games / A.Laszka, M. Felegyhazi, L. Buttyan // ACM Computing Surveys (CSUR), – 2015, 47 (2), Article No 23, – p. 1-38.

216. Leventakis, G. A risk assessment framework for interconnected and interdependent surface transport networks / G. Leventakis, A. Sfetsos, N. Moustakidis, et al. // Organization, Technology Management in Construction: An International Journal, – 2013, 5 (Special), – p. 811-819.

217. Li, H. A discrete hybrid differential evolution algorithm for solving integer programming problems / H. Li, L. Zhang // Engineering Optimization, – 2014, 46 (9), –p. 1238-1268.

218. Li, P. An effective biometric cryptosystem combining fingerprints with error correction codes / P. Li, X. Yang, H. Qiao, et al. // Expert Systems with Applications, – 2012, 39 (7), – p. 6562-6574.

219. Li, Y. A hybrid malicious code detection method based on deep learning / Y. Li, R. Ma, R. Jiao // International Journal of Security and Its Applications, – 2015, 9 (5), – p. 205-216.

220. Libicki, M. Conquest in cyberspace: National security and information warfare. – Cambridge University Press, – 2007. – 336 p.

221. Lim, M. An efficient dynamic reliability-dependent bit allocation for biometric discretization / M. Lim, A. Teoh, K. Toh // Pattern Recognition, – 2012, 45 (5), – p. 1960-1971.

222. Liu, Y. Survivability analysis of telephone access network / Y. Liu, V. Mendiratta, K. Trivedi // Proc. of the 15th Int. Symposium on Software Reliability Engineering, Saint-Malo, Bretagne, France, – 2004, – p. 367-377.

223. Lopes, R. Fractal and multifractal analysis: A review / R. Lopes, N. Betrouni // Medical Image Analysis, – 2009, 13 (4), – p. 634-649.

224. Ma, T. A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks / T. Ma, F. Wang, J. Cheng, et al. // Sensors, – 2016, 16 (10), – p. 1-23.

225. Maiorana, E. Biometric cryptosystem using function based on-line signature recognition // Expert Systems with Applications, – 2010, 37 (4), – p. 3454-3461.

226. Malone, T. What is coordination theory and how can it help design cooperative work systems? / T. Malone, K. Crowston // Proc. of the ACM conference on Computer-Supported Cooperative Work, Los Angeles, CA, USA, 1990, p. 357-370.

227. Maltoni, D., Maio D., Jain A., Prabhakar S. Handbook of fingerprint recognition. (2nd ed.) / D. Maltoni, D. Maio, A. Jain, S. Prabhakar. – London: Springer-Verlag, – 2009. – 494 p.

228. Mandelbrot, B. A multifractal walk down Wall Street // Scientific American, – 1999, 280 (2), – p. 70-73.

229. Mandelbrot B. The fractal geometry of nature. – San-Francisco: W.H. Freeman and Comp, – 1982. – 459 p.

230. Marsh, S. Formalizing trust as a computational concept / Ph.D. thesis / – University of Stirling (Scotland, UK), 1994. – 184 p.

231. Mazziotta, M. A well-being index based on the weighted product method / M. Mazziotta, A. Pareto. Topics in Theoretical and Applied Statistics. – Springer, Cham, – 2016. – p. 253-259.

232. McGinty, M. International environmental agreements among asymmetric nations // Oxford Economic Papers, – 2007, 59 (1), – p. 45-62.

233. Mehta, M. Security in e-services and applications / M. Mehta, S. Singh, Y. Lee // Network Security: Current Status and Future Directions (Douligeris C., Serpanos D. (eds)). – John Wiley Sons, – 2007, – p.157-178.

234. Merkle, J. Provable security for the fuzzy fingerprint vault / J. Merkle, M. Niesing, M. Schwaiger, et al. // Proc. of the 5th International Conference on Internet Monitoring and Protection, Barcelona, Spain, – 2010, – p. 65-73.

235. Moon, T. Error correction coding – mathematical methods and algorithms. – Hoboken, New Jersey: John Wiley Sons, – 2005, – 800 p.

236. Muhajarine, N. The Canadian Index of wellbeing: Key findings from the healthy populations domain / N. Muhajarine, R. Labonte, B. Winquist // Canadian Journal of Public Health, – 2012, 103 (5), – e342-e347.

237. Munda, G. Noncompensatory/nonlinear composite indicators for ranking countries: a defensible setting / G. Munda, M. Nardo // Applied Economics, – 2009, 41 (12), – p. 1513-1523.

238. Myerson, R.B. Game theory: Analysis of Conflict. – Harvard University Press, – 1997. – 587 p.

239. Nagar, A. Securing fingerprint template: Fuzzy vault with minutiae descriptors / A. Nagar, K. Nandakumar, A. Jain // Proc. of the 19th International Conference on Pattern Recognition, Tampa, Florida, USA, – 2008, – p.1-4.

240. Naghizadeh, P. Closing the price of anarchy gap in the interdependent security game / P. Naghizadeh, M. Liu // Information Theory and Applications Workshop, San Diego, CA, USA, – 2014, – p. 1-8.

241. Nandakumar, K. A fingerprint cryptosystem based on minutiae phase spectrum // Proc. of IEEE Workshop on Information Forensics Security, Seattle, WA, USA, – 2010, – p. 1-6.

242. Nandakumar, K. Fingerprint based fuzzy vault: Implementation and performance / K. Nandakumar, A. Jain, S. Pankanti // IEEE Transactions on Information Forensics and Security, – 2007, 2 (4), – p. 744-757.

243. Nanni, L. Local binary patterns for a hybrid fingerprint matcher / L. Nanni, A. Lumini // Pattern Recognition, – 2008, 41 (11), – p. 3461-3466.

244. Narlikar, A. International trade and developing countries: bargaining coalitions in the GATT & WTO. – London: Routledge, – 2003. – 256 p.

245. National Cyber Security Index (NCSI) Methodology. e-Governance Academy, 2015. URL: http://ncsi.ega.ee/methodology/

246. Nnolim, A. An architectural and process model approach to information security management / A. Nnolim, A. Steenkamp // Information Systems Education Journal, – 2008, 6 (31), – p. 1-27.

247. Norris, D. Advancing e-government at the grassroots: Tortoise or hare? / D. Norris, M. Moon // Public Administration Review, – 2005, 64 (1), p. 65-75.

248. OECD: Handbook on constructing composite indicators. Methodology and user guide. – Paris: OECD Publications, – 2008. – 162 p.

249. OECD: National risk assessments: A cross country perspective. Paris: OECD Publishing, – 2018. – 308 p.

250. Ojala, T. A comparative study of texture measures with classification based on feature distribution / T. Ojala, M. Pietikäinen, D. Harwood // Pattern Recognition, – 1996, 29 (1), – p. 51-50.

251. Palvia, S. E-government and e-governance: Definitions/domain framework and status around the world / S. Palvia, S. Sharma // Proc. 5th International. Conference on E-governance, Hyderabad, India, – 2007, – p. 1-12.

252. Pan, Q. A discrete differential evolution algorithm for the permutation flowshop scheduling problem / Q. Pan, M. Tasgetiren, Y. Liang// Computers Industrial Engineering, – 2008, 55 (4), – p. 795-816.

253. Papageorgiou, E. Review study on fuzzy cognitive maps and their applications during the last decade // IEEE International Conference on Fuzzy Systems, Taipei, Taiwan, – 2011, – p. 828-835.

254. Papakostas, G. Training fuzzy cognitive maps by using Hebbian learning algorithms: A comparative study / G. Papakostas, A. Polydoros, D. Koulouriotis, et al. // IEEE International Conference on Fuzzy Systems, Taipei, Taiwan, – 2011, – p. 851-858.

255. Patcha, A., Park, J. A game theoretic formulation for intrusion detection in mobile ad hoc networks // International Journal of Network Security, – 2006, 2 (2), – p. 131-137.

256. Petrovici, A. Identifying fingerprint alteration using the reliability map of the orientation field / A. Petrovici, C. Lazar // The Annals of the Univeristy of Craiova, Series Automation, Computers, Electronics and Mechatronics, – 2010, 7 (34), – p. 45-52.

257. Pietikäinen, M. Computer vision using local binary patterns / M. Pietikäinen, A. Hadid, G. Zhao, T. Ahonen. – London: Springer, – 2011. – 212 p.

258. Polikarpova, N. On the fractal features in fingerprint analysis // Proc. of the 13th International Conference on on Pattern Recognition, Vienna, Austria, – 1996, v. 3, – p. 591-595.

259. Ranise, S. On the verification of security-aware e-services // Journal of Symbolic Computation, – 2012, 47 (9), – p. 1066-1088.

260. Richardson, T. Design of capacity-approaching irregular low-density parity-check codes / T. Richardson, M. Shokrollahi, R. Urbanke // IEEE Transactions on Information Theory, – 2001, 47 (2), – p. 619-637.

261. Rosato, V. Modelling interdependent infrastructures using interacting dynamical models / V. Rosato, L. Issacharoff, F. Tiriticco, et al. // International Journal of Critical Infrastructures, – 2008, 4 (1-2), – p. 63-79.

262. Roy, S. A survey of game theory as applied to network security / S. Roy, C. Ellis, S. Shiva, et al. // Proc. of the 43rd Hawaii International Conference on System Sciences, , Hawai,USA, – 2010, – p. 1-10.

263. Saad, W. Distributed coalition formation games for secure wireless transmission / W. Saad, Z. Han, T. Basar, et al. // Mobile Networks and Applications, – 2011, 16 (2), – p. 231-245.

264. Saaty, T. L. How to make a decision: the analytic hierarchy process // European Journal of Operational Research, – 1990, 48(1), – p. 9-26.

265. Sabater, J. Review on computational trust and reputation models / J. Sabater, C. Sierra // Artificial intelligence review, – 2005, 24 (1), – p. 33-60.

266. Salama, M. Hybrid intelligent intrusion detection scheme / M. Salama, H. Eid, R. Ramadan, et al. // Soft Computing in Industrial Applications, v. 96. Springer, Berlin, Heidelberg, – 2011, – p. 293-303.

267. Sallhammar, K. Using stochastic game theory to compute the expected behavior of attackers / K. Sallhammar, S. Knapskog, B. Helvik // International Symposium on Applications and the Internet, Trento, Italy, – 2005, – p. 102-105.

268. Sasaki, Y. Hypergames and bayesian games: A theoretical comparison of the models of games with incomplete information / Y. Sasaki, K. Kijima// Journal of Systems Science and Complexity, – 2012, 25 (4), – p. 720-735.

269. Schwester, R. Examining the barriers to e-government adoption // Electronic Journal of e-Government, – 2009, 7 (1), – p. 113-122.

270. Skopik, F. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing / F. Skopik, G. Settanni, R. Fiedler // Computers & Security, – 2016, 60 (7), – p. 154-176.

271. Smith, S. R. Determining key factors in e-government information system security / S. Smith, R. Jamieson // Information Systems Management, – 2006, 23 (2), – p. 23-32.

272. Sood, A. Targeted cyberattacks: A superset of advanced persistent threats / A. Sood, R. Enbody // IEEE Security Privacy, – 2013, 11 (1), – p. 54-61.

273. Sterbenz, J. Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation / J. Sterbenz, E. Çetinkaya, M. Hameed, et al. // Telecommunication systems, – 2013, 52 (2), – p. 705-736.

274. Stoianov, A. Security issues of biometric encryption / A. Stoianov, T. Kevenaar, M. van der Veen // IEEE Toronto International Conference Science and Technology for Humanity, Toronto, Ontario, Canada, – 2009, – p. 34-39.

275. Storn, R. Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces / R. Storn, K. Price // Journal of Global Optimization, – 1997, 11 (4), – p. 341-354.

276. Stylios, C. Fuzzy cognitive map in modeling supervisory control systems / C. Stylios, P. Groumpos// Journal of Intelligent Fuzzy Systems: Applications in Engineering and Technology, – 2000, 8 (2), – p. 83-98.

277. Sukhostat, L. A comparative analysis of pitch detection methods under the influence of different noise conditions / L. Sukhostat, Y. Imamverdiyev// Journal of Voice, – 2015, 29 (4), – p. 410-417.

278. Svendsen N. Connectivity models of interdependency in mixed-type critical infrastructure networks / N. Svendsen, S. Wolthusen// Information Security Technical Report, –2007, 12 (1), – p. 44-55.

279. Tabansky, L., Cybersecurity in Israel. SpringerBriefs in Cybersecurity / L. Tabansky, I. Ben-Israel. – Heidelberg: Springer Cham, – 2015. – 84 p.

280. Tabassi, E., Wilson, C., Watson, C. Fingerprint image quality. NIST Research Report NISTIR 7151 / E. Tabassi, C. Wilson, C. Watson. – National Institute of Science and Technology, – 2004, – 72 p.

281. Tang, T. Deep learning approach for network intrusion detection in software defined networking / T. Tang, L. Mhamdi, D. McLernon, et al. // IEEE International Conference on Wireless Networks and Mobile Communications, Fez, Morocco, – 2016, – p. 258-263.

282. Terán, J. Mathematical models of coordination mechanisms in multi-agent systems / J. Terán, J. Aguilar, M. Cerrada // CLEI Electronic Journal, – 2013, 16 (2), Paper 5, – 12 p.

283. Theoharidou, M. Risk assessment methodology for interdependent critical infrastructures / M. Theoharidou, P. Kotzanikolaou, D. Gritzalis // International Journal of Risk Assessment and Management, – 2011, 15 (2-3), – p. 128-148.

284. Tøndel, I. Information security incident management: Current practice as reported in the literature / I. Tøndel, M. Line, M. Jaatun // Computers Security, – 2014, 45 (9), – p. 42-57.

285. Tong, V. Biometric fuzzy extractors made practical: A proposal based on FingerCodes / V. Tong, H. Sibert, J. Lecoeur, et al. // Proc. of the 2nd International Conference on Biometrics, Seoul, Korea, – 2007, – p.604-613.

286. Tuyls, P. Practical biometric authentication with template protection / P. Tuyls, A. Akkermans, T. Kevenaar, et al. // Proc. of International Conference on Audio- and Video based Biometric Person Authentication, Hilton Rye Town, NY, USA, – 2005, – p. 436-446.

287. Uddin, M. S. Towards coordination preparedness of soft-target organisation / M. S. Uddin, L. Hossain // International Conference on Electronic Government, Linz, Austria, – 2009, – p. 54-64.

288. UN E-Government Survey 2014: E-Government for the Future We Want. UN Department of Economic and Social Affairs. New York, – 2014. – 284 p.

289. Vasic, B. Combinatorial construction of low density parity-check codes for iterative decoding / B. Vasic, O. Milenkovic // IEEE Transactions on Information Theory, – 2004, 50 (6), – p. 1156-1176.

290. von Solms, B. Information security - The fourth wave // Computers Security, – 2006, 25 (3), – p. 165-168.

291. Wang, D. Weighted consensus multi-document summarization / D. Wang, T. Li // Information Processing Management, – 2012, 48 (3), – p. 513-523.

292. Wang, D. An incident prioritization algorithm based on BDIM / D. Wang, Z. Zhan, H. Shi // Proc. of the 2nd International Conference on Computer Modeling and Simulation, Sanya, Hainan, China, – 2010, v. 3, – p. 536-540.

293. Wang, J. E-government security management: key factors and countermeasure // Proc. of the 5th International Conference on Information Assurance and Security, Xi'an, China, – 2009, – p. 483-486.

294. Wang, J. A Value-at-Risk approach to information security investment / J. Wang, A. Chaudhury, H. Rao // Information Systems Research, – 2008, 19 (1), – p. 106-120.

295. Wang, M. Modeling misperceptions in games / M. Wang, K. Hipel, N. Fraser // Behavioral Science, – 1988, 33 (3), – p. 207-223.

296. Wasserman, S. Social network analysis: Methods and applications / S. Wasserman, K. Faust. – Cambridge: Cambridge University Press, – 1994. – 857 p.

297. Wendt, H. Wavelet leader multifractal analysis for texture classification / H. Wendt, P. Abry, S. Jaffard, et al. // Proc. of the 16th IEEE International Conference on Image Processing, Cairo, Egypt, – 2009, – p. 3785-3788.

298. West-Brown, M. Handbook for Computer Security Incident Response Teams (CSIRTs). 2nd Edition / M. West-Brown, D. Stikvoort, K. Kossakowski, et al. Carnegie Mellon University Software Engineering Institute, – 2003. – 223 p.

299. Whitson, T. Best practices in electronic government: comprehensive electronic information dissemination for science and technology / T. Whitson, L. Davis // Government Information Quarterly, – 2001, 18 (4), – p. 79-91.

300. Wiander, T. Holistic information security management in multi organization environment / T. Wiander, R. Savola, K. Karppinen, et al. // Proc. of the IEEE International Symposium on Industrial Electronics, Montreal, Quebec, Canada, – 2006, v. 4, – p. 2942-2947.

301. Willemson, J. On the Gordon Loeb model for information security investment // Proc. of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, England, UK, – 2006, – p. 1-12.

302. Wilson, D. Improved heterogeneous distance functions / D. Wilson, T. Martinez // Journal of Artificial Intelligence Research, – 1997, 6 (1), – p. 1-34.
303. Wimmer, M. E-government: aspects of security on different layers / M. Wimmer, B. von Bredow // Proc. of the 12th International Workshop on Database and Expert Systems Applications, Munich, Germany, – 2001, – p. 350-355.
304. Yadav, S. Detection of application layer DDoS attack by feature learning using stacked autoencoder / S. Yadav, S. Subramanian // International Conference on Computational Techniques in Information and Communication Technologies, – 2016, New Delhi, India, – p. 361-366.
305. Yang, S. Automatic secure fingerprint verification system based on fuzzy vault scheme / S. Yang, I. Verbauwhede // Proc. of IEEE 2005 International Conference on Acoustics, Speech and Signal Processing, Philadelphia, PA, USA, – 2005, – p. 609-612.
306. Yao, S. Modeling and analysis of network survivability under attack propagation / S. Yao, J. Guan, S. Ding, et al. // International Conference on Applications and Techniques in Information Security, Melbourne, VIC, Australia,– 2014, – p. 96-108.
307. Yoon, S. Altered fingerprints: analysis and detection / S. Yoon, J. Feng, A. Jain, // IEEE Transactions on Pattern Analysis and Machine Intelligence, – 2012, 34 (3), – p. 451-464.
308. Yu, L. A distance-based group decision-making methodology for multi-person multi-criteria emergency decision support / L. Yu, K. Lai // Decision Support Systems, –2011, 51 (2), – p. 307-315.
309. Yunis, M. A conceptual model for the development of a national cybersecurity index: An integrated framework / M. Yunis, K. Koong // Proc. of the 21st Americas Conference on Information Systems, Fajardo, Puerto Rico, – 2015, – p. 1-13.
310. Zadeh, L. Fuzzy sets // Information and Control, – 1965, 8 (3), – p. 338-353.

311. Zeng, Z. E-government information security in the web environment based on role based access control technology / Z. Zeng, T. Chen, Y. Zhang // Proc. of the International Seminar on Business and Information Management, Wuhan, China, – 2008, – p. 210-213.

312. Zhou, X. Template protection and its implementation in 3D face recognition systems // Proc. SPIE 6539, Biometric Technology for Human Identification IV, 2007, Paper 65390L. DOI: 10.1117/12.719845.

313. Zhou, P. Weighting and aggregation in composite indicator construction: a multiplicative optimization approach / P. Zhou, B. Ang, D. Zhou // Social Indicators Research, – 2010, 96 (1), – p. 169-181.

İXTİSARLARIN VƏ ŞƏRTİ İŞARƏLƏRİN SİYAHISI

BK	Baş Koordinator
DE	Diferensial Evolyusiya
EDMO	Elektron Dövlət Milli Operatoru
eID	Elektron identifikasiya
ƏM	Əlaqələndirmə Mərkəzi
GA	Genetik alqoritm
İKT	İnformasiya və kommunikasiya texnologiyaları
İnT	İnformasiya təhlükəsizliyi
İTD	İnformasiya təhlükəsizliyi domeni
Kİ	Kritik İnfrastruktur
Kİİ	Kritik İnformasiya İnfrastrukturu
KİİO	Kritik İnformasiya İnfrastrukturu Operatoru
MİTM	Milli İnformasiya Təhlükəsizliyi Mərkəzi
AI3	Average Internet Interruption Index – İnternet kəsintilərinin ortalama indeksi
AFIS	Automated Fingerprint Identification System
AHP	Analytic Hierarchy Process – İyerarxiyaların analizi prosesi
AS	Autonomous System – Avtonom sistem
BCH	Bose-Chaudhuri-Hocquenghem – Bouz-Çodhuri-Hokinqem
CBR	Case Based Reasoning – Presedentlər əsasında mühakimə
CERT	Computer Emergency Response Team – Kompüter insidentlərini cavablandırma komandası
DBN	Deep Belief Network – Dərin inam şəbəkəsi
DCI	Dynamic Cybersecurity Index – Dinamik kibertəhlükəsizlik indeksi
DDoS	Distributed denial-of-service – Paylanmış xidmətdən imtina hücumu
DNN	Deep Neural Network – Dərin neyron şəbəkəsi
DNS	Domain Name System – Domen adları sistemi
ECC	Error-Correcting Code – Səhvlərin islahı kodu

EER	Equal Error Rate – Bərabər səhv faizi
FAR	False Acceptance Rate – Yanlış qəbul faizi
FCM	Fuzzy Cognitive Map – Qeyri-səlis koqnitiv xəritə
FCS	Fuzzy Commitment Scheme – Qeyri-səlis bağlama sxemi
FRR	False Rejection Rate – Yanlış rədd faizi
FVC	Fingerprint Verification Contest – Barmaq izi sistemlərinin qiymətləndirilməsi müsabiqəsi
GAR	Genuine Acceptance Rate
GCI	Global Cybersecurity Index – Qlobal kiber-təhlükəsizlik indeksi
ISP	Internet Service Provider – İnternet xidmətləri provayderi
LBP	Local Binary Pattern – Lokal binar şablon
LDA	Loss Distribution Approach – itkinin ehtimal paylanması
LDP	Local Direction Pattern – Lokal istiqamət şablonu
LDPC	Low-Density Parity-Check – Aşağı sıxlıqlı cütlük yoxlaması
NAP	Network Access Point – şəbəkə giriş nöqtələri
NCSecMS	National Cybersecurity Management System Maturity Model
NCSI	National Cyber Security Index – Milli kibertəhlükəsizlik indeksi
NIST	National Institute of Standards and Technology
PEG	Progressive Edge-Growth
PoP	Point of Presense – Qlobal qoşulma nöqtələri
PSO	Particle Swarm Optimization – sürü optimallaşdırma alqoritmi
RBM	Resticted Boltzman Machine – Məhdud Bolsman maşını
RTIR	Request Tracker for Incident Response
SCI	Static Cybersecurity Index – Statik kibertəhlükəsizlik indeksi
SVM	Support Vector Machine – Dayaq vektorları metodu
TN	True Negatives
TP	True Positives