UOT 004.056:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏHDİDLƏRİNİN KONSENSUS RANQLAŞDIRILMASI METODU

E-dövlətin informasiya təhlükəsizliyi təhdidləri informasiya sahəsində milli maraqlara qarşı yönəlir. İnformasiya sahəsində milli maraqlara çoxsaylı təhdidlər mövcuddur və kiber-müdafiəyə ayrılan resursların məhdudluğu şəraitində təhdidlərə qarşı effektiv əks-tədbirlər görmək üçün bu təhdidlərin çoxkriteriyalı ranqlaşdırılması zəruridir. Təklif edilən modeldə təhdidlər milli maraqlara yaratdıqları təhlükə səviyyələrini xarakterizə edən ekspert qiymətləndirmələri əsasında ranqlaşdırılır. Təhdidlərin konsensus ranqlaşdırılması üçün optimallaşdırma modeli təklif edilir.

Açar sözlər: *e-dövlət, informasiya təhlükəsizliyi, informasiya təhlükəsizliyi təhdidləri, təhdidlərin qiymətləndirilməsi, təhdidlərin ranqlaşdırılması, konsensus ranqlaşdırma.*

Giriş

İnformasiya təhlükəsizliyinin təmin edilməsi istənilən dövlətin daxili və xarici siyasətinin ən vacib məsələlərindən biridir [1]. Dövlətin informasiya təhlükəsizliyini informasiya sahəsində milli maraqların təmin olunduğu vəziyyət kimi müəyyən etmək 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 informasiya təhlükəsizliyi mühiti ilə qarşılaşır, bu mühit digər dövlətlərdən, transmilli terrorçuluq və cinayətkarlıq şəbəkəsindən, yeni texnologiyalardan qaynaqlanan təhdidlərlə xarakterizə edilir [2]. Belə təhdidlərə informasiya müharibəsi, kiberterrorizm, kibercinayətkarlıq, kibercasusluq, kibersabotaj, fərdi məlumatların oğurlanması və s. aid edilə bilər [2, 3].

İnformasiya sahəsinin müasir təhdidlərdən qorunması hazırkı zamanda milli təhlükəsizliyin təmin edilməsinin prioritet istiqamətlərindən biridir [4]. 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, informasiya təhlükəsizliyinin təmin edilməsi riskin müəyyən qiymətinə yol verməklə, təhlükəsizliyin tələb edilən səviyyəsinin optimallaşdırılması yolu ilə həyata keçirilir [5]. Buna görə, təhdidlər güman edilən nəticələr əsasında prioritetlərinə görə ranqlaşdırılmalı, strukturlaşdırılaraq təhdidlərin və müvafiq reaksiyaların iyerarxiyası işlənməlidir [6].

E-dövlətin informasiya təhlükəsizliyinə 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 [7].

Bu məqalənin məqsədi e-dövlətin informasiya təhlükəsizliyinə təhdidlərin ranqlaşdırılması üçün metodoloji yanaşmanın işlənməsidir. Yanaşmanın əsası kimi çoxkriteriyalı qərar qəbulu metodologiyası [8] götürülür. Məqalədə 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 kiber-təhlükəsizlik təhdidlərinin siyahısı tərtib edilib (rəsmi sənədlərin, elmi tədqiqatların və kütləvi informasiya vasitələrində olan məlumatların əsasında). Tutaq ki, informasiya təhlükəsizliyinin siyasi, hüquqi, iqtisadi, hərbi, texnoloji aspektlərini öyrənən alimlər, informasiya təhlükəsizliyinin 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 qiymətləndirməlidirlər. 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 $X^k = \left(X_{ij}^k\right)_{n\times m}$ $k = 1,2, \dots, p$ 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 sonrakı düsturlarda x_{ij}^k elementlərinin yuxarıdakı k indeksi yazılmır):

$$x_{ij} = \frac{X_{ij}}{\sum_{i=1}^{n} X_{ij}} \tag{1}$$

Bu ekspert qiymətləndirmələri əsasında hər bir ekspert tərəfindən kriteriya çəkilərinin müəyyən edilməsi $(w^C = (w_1^C, w_2^C, \dots, w_m^C))$, alternativlərin qiymətləndirilməsi $(A_1' > A_2' > \dots > A_n')$, 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 informasiya təhlükəsizliyinə təhdidlərin müəyyən edilməsi və onların qiymətləndirilməsi, kriteriyaların seçilməsi üçün informasiya sahəsində ölkənin milli maraqları identifikasiya edilməlidir. İnformasiya sahəsində ölkənin milli maraqlarını rəsmi dövlət sənədləri (milli təhlükəsizlik konsepsiyası, informasiya təhlükəsizliyi konsepsiyası, doktrinası, müvafiq qanunvericilik sənədləri) əsasında identifikasiya etmək olar. Məsələn, Rusiya Federasiyasının 2000-ci ildə qəbul edilmiş informasiya təhlükəsizliyi doktrinasında informasiya sahəsində ölkənin milli maraqlarının aşağıdakı komponentləri müəyyən edilir (2016-cı ildə qəbul edilmiş yeni doktrinada fərqli siyahı verilir) [9]:

- 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, kritik infrastrukturların, kiber-fiziki sistemlərin informasiya 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 informasiya təhlükəsizliyi problemləri əksər ölkələr üçün eynidir.

E-dövlətin informasiya təhlükəsizliyi təhdidlərinin ranqlaşdırılması məsələsinə operativ, taktiki və strateji idarəetmə səviyyələrində, qısa- və uzunmüddətli perspektivdə baxmaq olar. Təhdidlərin operativ səviyyədə ranqlaşdırılmasına misal olaraq, MS-ISAC (*ing. Multi-State Information Sharing and Analysis Center*) mərkəzinin müəyyən etdiyi kiber-təhlükəsizlik

səviyyəsini göstərmək olar, bu indikator bədniyyətli kiber aktivliyin və potensial ziyanın cari səviyyəsini göstərir [10].

Bu məqalədə strateji təhdidlərə baxılır. E-dövlətin informasiya təhlükəsizliyinə strateji təhdidlər milli miqyasda insidentlərlə nəticələnə bilən təhdidlərdir. İnformasiya təhlükəsizliyi baxımından dövlət üçün strateji təhdidlərin bir neçə əsas səviyyəsini ayırmaq olar. Strateji təhdidlərin iki əsas kateqoriyasını fərqləndirmək olar [11]:

- Baxılan zaman kəsiyində informasiya təhlükəsizliyinə davamlı təhlükə yaradan təhdidlər;
- Nəticəsi böyük, ehtimalı qeyri-müəyyən olan təhdidlər – hazırkı trendlərin dramatik inkişafı nəticəsində meydana çıxan daha əhəmiyyətli təhdidlər.

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

Son dövrlər əksər qabaqcıl ölkələrdə milli kibertəhlükəsizlik strategiyaları qəbul edilmişdir [12]. 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 [13]: kiber-casusluq, kiber-terrorizm, kiber-ekstremizm, kiber-cinayətkarlıq, kritik infrastruktura kiber hücumlar, fərdi verilənlərə kiberhücumlar.

Strateji təhdidlərin qiymətləndirilməsinin periodikliyinə gəlincə, nümunə kimi qeyd edək ki, milli səviyyədə risklərin qiymətləndirilməsinin Birləşmiş Krallıqda qəbul edilmiş qaydasına görə, belə risklərin qiymətləndirilməsi hər beş ildən bir həyata keçirilməlidir [14].

Təhdidlərin qiymətləndirilməsi üçün kriteriyalar

Təhdidlərin idarə edilməsinin həyat tsiklinə aşağıdakı iterativ mərhələləri aid etmək olar [15]: potensial təhdidlərin aşkarlanması, təhdidlərin analizi, təhdidlərin qiymətləndirilməsi, təhdidlərin dəyərləndirilməsi – prioritetlərinin müəyyən edilməsi (ranqlaşdırılması) və təhdidin potensial təsirlərinin azaldılması üçün uyğun əks-tədbirlərin seçilməsi və həyata keçirilməsi.

Təhdidin aşkarlanması (identifikasiyası) – fasiləsiz prosesdir, sistemi əhatə edən daxili və xarici mühit real təhdidlərin mövcudluğunu müəyyən etmək 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 informasiya təhlükəsizliyinə təhdidlərin xarici və daxili mənbələrini fərqləndirmək olar.

Təhdidlər boşluqlar vasitəsilə reallaşdırılır (kiber-hücum edilir), boşluqlara yenilənməmiş proqram təminatı aid ola bilər. Kiber-hücumlara paylanmış xidmətdən imtina (*ing. Distributed denial-of-service, DDoS*), kiber-casusluq 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/struktur dəyişikliklər 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 böyük miqyaslı və ehtimalı qeyri-müəyyən ola bilər. Lakin bu kəmiyyətlərin praktikada qiymətləndirilməsi problemlidir [16]. 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 [17].

Əlaqədar tədqiqatların icmalı

Çoxkriteriyalı qərar qəbuletmə metodları

Hazırda tədqiqatçılar tərəfindən çox sayda çoxkriteriyalı qərar qəbuletmə metodları (*ing. Multi Criteria Decision Making, MCDM*) təklif edilmişdir: AHP (*ing.Analytic Hierarchy Process*) [18], ANP (*ing.Analytic Network Process*) [19], TOPSIS (*ing.Technique for Order Preference by Similarity to Ideal Solution*) [20], VIKOR (*VIsekriterijumska Optimizacija i Kompromisno Resenje: multicriteria optimization and compromise solution*) [21], DEMATEL (*ing.Decision-Making Trial and Evaluation Laboratory*) [22], ELECTRE II (*ELimination Et Choix Traduisant la REalité: ELimination and Choice Translating REality*) [23], PROMETHEE II (*ing.Preference Ranking Organization METHod for Enrichment Evaluation*) [24] və s.

AHP metodu Tomas Saati (*ing. Thomas Saaty*) tərəfindən işlənilmişdir [18]. Onun əsas məqsədi subyektiv qərar qəbuletmə prosesini bir neçə atribut əsasında iyerarxik sistemdə modelləşdirməkdir. ANP metodu AHP metodunun ümumiləşdirilməsidir [19]. Adətən, bir çox qərar proseslərini iyerarxik strukturlaşdırmaq mümkün olmur. İyerarxiyanın yuxarı səviyyə elementlərinin aşağı səviyyə elementləri ilə qarşılıqlı əlaqələri və asılılıqları ola bilər. AHP belə qarşılıqlı asılılıq və əks-əlaqələri nəzərə almır. Saati tərəfindən işlənmiş ANP metodu bu nöqsanları aradan qaldırır.

Hwang C.L. və Yoon K. tərəfindən 1981-ci ildə işlənən TOPSIS metodu çoxatributlu və çoxkriteriyalı qərar qəbuletmə məsələləri (MADM/MCDM) üçün klassik yanaşmadır [20]. Pozitiv ideal həldən ən yaxın məsafədə və neqativ ideal həldən ən uzaq məsafədə olan alternativ seçilir.

VIKOR metodu mürəkkəb sistemlərin çoxkriteriyalı optimallaşdırılması üçün işlənmişdi. O, kriteriyaları konfliktli olan məsələlər üçün alternativlər çoxluğundan kompromis həllər müəyyən edir, bu həllər qərar qəbul edənlərə yekun qərara gəlməyə kömək edə bilər [21].

DEMATEL metodunu Gabus və Fontela 1973-cü ildə işləmişlər [22]. Bu metod faktorları kriteriyalar arasındakı qarşılıqlı əlaqələr kimi təsvir edir. Buna görə DEMATEL mürəkkəb faktorların assosiasiyalarını cəlb edən struktural modelin qurulması üçün tamamlanmış metoddur. Bu metod bir çox müxtəlif hallar üçün, məsələn, marketinq strategiyalarının işlənməsində, nəzarət sistemlərinin işlənməsində, təhlükəsizlik məsələlərinin həllində və qrup qərarlarının qəbulunda uğurla tətbiq olunub.

İlk ranqlaşdırma (*ing. outranking*) metodu ELECTRE I Roy tərəfindən 1968-ci ildə təklif edilmişdi [23]. Həmin vaxtdan bu metodun bir neçə versiyası işlənmişdir (ELECTRE I, ELECTRE II, ELECTRE III, ELECTRE IV, ELECTRE IS və ELECTRE TRI (ELECTRE Tree)). ELECTRE II ranqlaşdırma üçün istifadə edilir. ELECTRE III verilənlərin qeyri-dəqiqliyini və ya qeyri-müəyyənliyini nəzərə almaqla ELECTRE II metodunu təkmilləşdirmək üçün işlənmişdi.

PROMETHEE ranqlaşdırma metodudur, 1980-ci illərin ortalarında Brans və Vincke tərəfindən işlənmişdir. Onun riyazi modelinin qurulmasını qərar qəbul edənlərin başa düşməsi nisbətən asandır [24]. PROMETHEE ELECTRE metodunun təkmilləşdirilmiş formasıdır, cüt-cüt müqayisə mərhələsində ondan fərqlənir, istifadəsi daha asandır.

Baxılan ənənəvi MCDM metodları insanın mühakiməsindəki qeyri-müəyyənlikləri (*ing. ambiguities*) hələ də tam əks etdirə bilmir. Zadənin 1965-ci ildə təklif etdiyi qeyri-səlis çoxluqlar nəzəriyyəsi belə qeyri-müəyyənlikləri modelləşdirmək üçün geniş tətbiq edilir [25]. O, çoxkriteriyalı qərar qəbuletmədə əlyetər informasiyada olan qeyri-müəyyənlikləri də effektiv aradan qaldırır. Alternativlərin kriteriyalara görə qiymətləndirilməsi və kriteriyaların vaciblik çəkiləri linqvistik qiymətlərlə ifadə olunur [26]. Qeyri-səlis yanaşmanın tətbiqi ilə qeyri-səlis MCDM məsələlərinin qeyri-səlis AHP, qeyri-səlis TOPSIS [27], qeyri-səlis fuzzy VIKOR [28] kimi bəzi həll metodları işlənmişdir. Lakin ümumi qeyri-səlis MCDM məsələsinin həlli üçün ən yaxşı üsul yoxdur. Qeyri-səlis ranqlaşdırma metodlarının bir sıra nöqsanları vardır [28]: 1) oxşar qeyri-səlis ədədləri müqayisə etdikdə həssaslığın olmaması; 2) bəzi hallarda intuisiyaya zidd nəticələr; 3) hesablamaların çətinliyi. Buna görə son dövrlər tədqiqatçılar ən yaxşı alternativi seçmək üçün müxtəlif metodları birləşdirməyə cəhd edirlər [29-32].

Son dövrlər tədqiqatçılar çoxkriteriyalı qərar qəbuletmə metodlarının informasiya təhlükəsizliyi sahəsində tətbiq edilməsinə maraq göstərirlər. Məsələn, çoxkriteriyalı qərar qəbuletmə metodları təhdidlərin qeyri-müəyyənlik mühitində qiymətləndirilməsi [31], informasiya təhlükəsizliyi risklərinin [32] və onlara qarşı tədbirlərin qiymətləndirilməsi [33], informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi üzrə qərarların qəbulu [34], e-dövlətin informasiya təhlükəsizliyi strategiyasının qiymətləndirilməsi [35] və s. məsələlərinə tətbiq edilir.

Ranq aqreqasiyası metodları

Müxtəlif fərdi ranqları qrup konsensus ranqında birləşdirmək üçün Aqreqasiya funksiyasının seçilməsi üçün müxtəlif yanaşmalar vardır, bu barədə daha ətraflı məlumat üçün [36-38]-ə istinad etmək olar.

Bir neçə ranqlaşdırma nəticəsinin konsensus ranqlaşdırmasında birləşdirilməsi ranq aqreqasiyası kimi məlumdur [39]. Ranq aqreqasiyası yanaşmalarının əksəriyyəti yekun ranqlaşdırma yaratmaq üçün aşkar olmadan major səsvermə keçirir. Məsələn, ən sadə yanaşmada fərdi ranqların ortası hesablana bilər. Borda hesabı metodu [40] subyektləri onların mövqeləri əsasında sıralayır və subyektlərin hər bir səsverəndən aldığı balların sayını hesablayır. Ranq aqreqasiyasının iki metodu var: supervizorlu və supervizorsuz. Supervizorsuz ranq aqreqasiyası metodlarının əksəriyyəti subyekt üçün bütün ranqlaşdırma siyahılarında ondan aşağıda olan subyektləri sayır. Median ranq aqreqasiyası [40] subyektləri bütün ranqlaşdırma siyahılarında onların ranqlaşdırma medianları əsasında sıralayır. Bu metodların fundamental nöqsanlarından biri onların bütün ranqlaşdırmaları eyni emal etmələridir. Lakin müxtəlif sistemlərin dəqiqliyi müxtəlifdir və onlara fərqli yanaşılmalıdır. Adətən, supervizorlu ranq aqreqasiyası hər bir ranqlaşdırma siyahısının çəkisini nişanlanmış verilənlərdən istifadə edərək aqreqasiya funksiyasını öyrənməklə müəyyən edir [41]. Supervizorlu aqreqasiyada yüksək dəqiqlik əldə edilsə də, praktikada nişanlanmış verilənlər həmişə əlyetər olmur. [42]-də çəkili Borda hesabını optimallaşdırmaqla, ranqlaşdırma siyahılarının çəkilərinin supervizor olmadan öyrənilməsi modeli təklif edilir.

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 [36]. 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 metod. 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 ($j = 1, \dots, m$):

$$E_j = -k \sum_{i=1}^{n} x_{ij} log(x_{ij}), \quad (2)$$

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 aşağıdakı kimi müəyyən edilir ($j = 1, \dots, m$):

$$\varphi_j = 1 - E_j. \quad (3)$$

c) Kriteriya çəkilərinin müəyyən edilməsi. Hər bir C_j kriteriyası üçün çəki aşağıdakı kimi hesablanır ($j = 1, \dots, m$):

$$w_j^C = \frac{\varphi_j}{\sum_{j=1}^{m} \varphi_j} \tag{4}$$

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 (U^+) və pessimist (U^-) qiymətlər aşağıdakı kimi müəyyən edilir:

Optimist qiymətlər: $U^+ = (U_1^+, U_2^+, \dots, U_m^+)$ (5)

Pessimist qiymətlər: $U^- = (U_1^-, U_2^-, \dots, U_m^-)$ (6)

burada

$$U_j^+ = \begin{cases} \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{7}$$

$$U_j^- = \begin{cases} \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{8}$$

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:

$$d_j^+ = \sqrt{\sum_{i=1}^{n} \left(x_{ij} - U_j^+\right)^2} \tag{9}$$

$$d_j^- = \sqrt{\sum_{i=1}^{n} \left(x_{ij} - U_j^-\right)^2} \tag{10}$$

c) Hər bir C_j kriteriyası üçün dispersiya ölçüsü aşağıdakı kimi müəyyən edilir:

$$\xi_j = \frac{d_j^+}{d_j^+ + d_j^-} \tag{11}$$

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

$$w_j^C = \frac{\xi_j}{\sum_{j=1}^{m} \xi_j} \tag{12}$$

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

$$z_i = \sum_{j=1}^{m} w_j^C x_{ij}, \quad i = 1,2, \dots, n \tag{13}$$

Konsensus ranqlaşdırma üçün optimallaşdırma metodu

Hər bir ekspert standart çoxkriteriyalı qərar qəbuletmə prosesini yerinə yetirərək özünün verdiyi qiymətlər əsasında alternativlərin yekun ranqlarını ala bilər. Məsələ bu fərdi ranqları qrup konsensus ranqlarında aqreqasiya etməkdən ibarətdir [43].

Çəkili konsensus ranqlaşdırma məsələsini ümumi şəkildə aşağıdakı kimi ifadə etmək olar.

Tutaq ki, $r_i = (r_{i1}, r_{i2}, \dots, r_{in})$ – *i*-ci ekspertin təhdidlərə verdiyi ranqların 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 r^* çəkili konsensus ranqını tapmaqdır. Məqsəd r^* ilə bütün r_i-lər arasındakı çəkili məsafələri minimallaşdırmaqdır. Əgər $w = \left(w_1, w_2, \dots, w_p\right)^T$

ekspertlərə təyin edilmiş çəkilərin vektorudursa, onda çəkili konsensus ranqlaşdırması məsələsi aşağıdakı optimallaşdırma məsələsi kimi ifadə oluna bilər:

$$argmin_{\boldsymbol{w},r^*}(1-\lambda)\sum_{i=1}^{p} w_i\|r^*-r_i\|^2+\lambda\|w\|^2, \quad (14)$$

Şərtlər: $\sum_{i=1}^{p} w_i = 1,\ \ w_i \geq 0, \forall i$

burada $0 \leq \lambda \leq 1$ requlyarlaşdırma parametridir, çəkili məsafənin minimallaşdırılması ilə çəkilərin hamarlığı arasındakı balansı tənzimləyir (Bizim eksperimentlərdə empirik olaraq, $\lambda = 0.4$ götürülmüşdü). Sadəlik üçün r^* konsensus ranqlaşdırması ilə r_i fərdi ekspert ranqlaşdırması arasındakı uzlaşmamanı ölçmək üçün Evklid məsafəsi istifadə edilir. Buna görə $w_i\|r^*-r_i\|^2$ i-ci ekspertin ranq vektoru ilə r^* arasındakı çəkili məsafəni ölçür və (14) tənliyindəki birinci həddi hər bir ekspert üçün bu məsafəni minimallaşdırmaq üçün istifadə edilir. (14) tənliyindəki ikinci toplanan çəkilərin hamarlığını təmin edən requlyarlaşdırma həddidir.

Bu məsələ xətti məhdudiyyətlərlə kvadratik funksiyanın optimallaşdırılması məsələsidir və onun sürətli həlli üçün [44]-də aşağıdakı alqoritm təklif edilir.

$w_i = \frac{1}{p}, i = 1, \dots, p$ başlanğıc qiymətləri verilir və optimallaşdırma məsələsini həll etmək üçün aşağıdakı iki addım təkrarlanır:

Addım 1: w fiksə edilməklə r^* üçün optimal həll tapılır. Optimal həll çəkili ortadır:

$$r^* = \sum_{i=1}^{p} w_i r_i. \quad (15)$$

Addım 2: r^* fiksə edilməklə w üçün optimal həll tapılır. Tutaq ki,

$$d = \left(\|r^*-r_1\|^2, \|r^*-r_2\|^2, \dots \left\|r^*-r_p\right\|^2\right)^T \in \mathbb{R}^p.$$

Nəzərə alsaq ki,

$$(1-\lambda)\sum_{i=1}^{p} w_i\|r^*-r_i\|^2+\lambda\|w\|^2 = (1-\lambda)d^T w +$$

$$+\lambda w^T w = \lambda\left\|w-\frac{\lambda-1}{2\lambda}d\right\|^2 - \frac{(\lambda-1)^2}{4\lambda}\|d\|^2$$

Onda r^* fiksə edilməklə üçün optimallaşdırma məsələsi belə olacaq:

$$argmin_{\boldsymbol{w}}\left\|w-\tfrac{\lambda-1}{2\lambda}d\right\|^2, \quad (16)$$

Şərtlər: $\sum_{i=1}^{p} w_i = 1,\ \ w_i \geq 0, \forall i.$

Bu, xətti məhdudiyyətlərlə p dəyişənin kvadratik funksiyasının optimallaşdırılması məsələsidir (dəyişənlərin sayı ekspertlərin sayına bərabərdir). Bu məsələni sadəcə $\frac{\lambda-1}{2\lambda}d$ vektorunu $(p-1)$-simpleksə proyeksiyalamaqla da həll etmək mümkündür, effektiv proyeksiyalama alqoritmi üçün [45]-ə müraciət etmək olar.

w və r^* yığılana kimi Addım 1 və 2 ilə iterativ yenilənir. Sonra r^* artmaya görə nizamlanaraq çəkili konsensus ranqlaşdırma alınır.

Yığılma: Sadəlik üçün (14) tənliyini D və w və r^*-in başlanğıc qiymətlərini w_0 və r_0^* kimi işarə edək. İlkin qiymətlərin verilməsindən başlayaraq, ikiaddımlı proseduru təkrarlayırıq: $r_i^* = argmin\, D(w_{i-1}, r_{i-1}^*)$ və $w_i = argmin\, D(w_{i-1}, r_i^*)$, burada i iterasiyanı işarə etmək üçün istifadə edilib. Deməli, $D(w_i, r_i^*) \leq D(w_{i-1}, r_i^*) \leq D(w_{i-1}, r_{i-1}^*)$. Buna görə hər iterasiyada D ciddi azalır və həmişə müsbət qalır. Beləliklə, bu prosedur üçün çox vaxt yığılma əldə edilə bilər.

Təklif edilmiş metodologiyanı yoxlamaq üçün növbəti bölmədə ədədi misal təqdim olunur.

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 – kiber-casusluq;
- A_2 – kiber-terrorizm;
- A_3 – kiber-cinayətkarlıq;
- A_4 – kritik infrastruktura kiber hücumlar;
- 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 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 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-də hər bir ekspertin verdiyi qiymətlər əsasında kriteriyaların çəkilərinin müxtəlif metodlar ilə müəyyən edilməsinin nəticələri göstərilir.

Cədvəl 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-də verilmiş kriteriya çəkilərindən istifadə etməklə (13) düsturu ilə təhdidlərin qiymətləndirilməsini almaq olar. Nəticələr Cədvəl 3-də təqdim olunur.

Cədvəl 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 3-dən göründüyü kimi, müxtəlif ekspertlər konkret təhdid üçün kriteriya çəkilərinin təyin edilməsi metodundan asılı olaraq müxtəlif qiymətlər ala bilərlər. 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 3-dəki təsviri bir qədər dəyişməklə Cədvəl 4-də belə aqreqasiya ssenarisini asanlıqla almaq olar.

Cədvəl 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 5-də müxtəlif çəki təyinetmə metodlarının nəticələrinin hər bir ekspert üzrə aqreqasiyası göstərilib.

Cədvəl 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. (28) düsturu ilə tapılmış ekspertlərin çəkilərindən istifadə etməklə hesablanmış yekun qərar nəticələri cədvəl 6-da göstərilib.

Cədvəl 6

Ekspertlərin qiymətləndirmələrinin 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 6-dan görünür ki, təhdid A_4 (kritik infrastruktura kiber hücumlar) ən yüksək ranqa malikdir, sonra A_1 (kiber-casusluq), A_2 (kiber-terrorizm), A_5 (fərdi verilənlərə kiberhücumlar) və A_3 (kiber-cinayətkarlıq) təhdidləri gəlir. Beləliklə, üç müxtəlif kriteriya üzrə üç ekspert tərəfindən qiymətləndirilmiş beş təhdiddən ən təhlükəlisi A_4-dür.

Nəticə

E-dövlətin informasiya təhlükəsizliyinə təhdidlərin siyahısı genişlənir, bu təhdidlərin potensial təsirlərini optimal şəkildə azaltmaq üçün dövlətin reaksiya verməsi baxımından onların prioritetləri də dəyişir. Əgər 2000-ci illərin əvvəlində təhdidlər, hər şeydən əvvəl iqtisadi xarakter daşıyırdısa, indi siyasi, xarici və hərbi sahələrdə təhdidlər daha da aktuallaşır. Təhdidlərin ranqlaşdırılması informasiya təhlükəsizliyi üçün çox vacib prosesdir. O, informasiya təhlükəsizliyinin təmin edilməsinə ayrılmış resurslar daxilində uyğun tədbirlərin prioritetini müəyyən etməyə imkan verir. Bu işdə milli informasiya təhlükəsizliyinin əsas təhdidlərinin ranqlaşdırılması zamanı siyasi və intellektual elitanı təmsil edən ekspertlərin qiymətləndirməsində uzlaşmama dərəcəsini minimallaşdırmaq üçün model təklif edilir. Elitanın ölkənin informasiya təhlükəsizliyi haqqında baxışlarında uzlaşmanın olmaması özlüyündə problemdir və təəssüf ki, az

tədqiq olunmuşdur. Bu baxışları aşkarlamağın geniş yayılmış metodu anket sorğusu metodudur və gələcəkdə ekspert sorğusu verilənlərinin statistik analizi, o cümlədən klaster analizi və korrelyasiya analizi, verilənlərin ümumiləşdirilməsi və nəticələrin interpretasiyası üzrə tədqiqatların aparılması nəzərdə tutulur.

Ədəbiyyat

1. Libicki M. C. Conquest in cyberspace: National security and information warfare. Cambridge University Press, 2007, 336 p.
2. European Union Agency For Network and Information Security: ENISA Threat Landscape Report 2017 (ETL 2017). January 2018, 114 p.
3. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity // Journal of Computer and System Sciences, 2014, vol.80, no.5, pp.973–993.
4. Sabillon R., Cavaller V., Cano J. National cyber security strategies: Global trends in cyberspace // International Journal of Computer Science and Software Engineering, 2016, vol.5, no.5, pp.67–81.
5. Jerman-Blažič B. An economic modelling approach to information security risk management // International Journal of Information Management, 2008, vol.28, no.5, pp.413–422.
6. Pierazzi F., Apruzzese G., Colajanni M., Guido A., Marchetti M. Scalable architecture for online prioritization of cyber threats / Proceedings of the 9th NATO International Conference on Cyber Conflicts, 2017, pp.1–22.
7. İmamverdiyev Y. N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatların müasir vəziyyətinin analizi // İnformasiya cəmiyyəti problemləri, 2012, № 2(6), s.19–26.
8. Zavadskas E. K., Turskis Z., and Kildienė S. State of art surveys of overviews on MCDM/MADM methods //Technological and economic development of economy, 2014, vol.20, no.1, pp.165–179.
9. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 9 сент. 2000 г. № Пр-1895.
10. Multi-State Information Sharing & Analysis Center (MSISAC). http://msisac.cisecurity.org/alert-level/
11. Lundberg R., and Willis H. H. Deliberative risk ranking to inform homeland security strategic planning // Journal of Homeland Security and Emergency Management, 2016, vol.13, no.1, pp.3–33.
12. İmamverdiyev Y.N. Yeni nəsil milli kibertəhlükəsizlik strategiyaları // İnformasiya cəmiyyəti problemləri, 2013, №2, s.42–51.
13. Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012, 253 p.
14. OECD: National Risk Assessments: A Cross Country Perspective. OECD Publishing, Paris, 2018, 308 p. http://dx.doi.org/10.1787/9789264287532-en.
15. Robinson N., Gribbon L., Horvath V., Robertson K., Cyber-security threat characterization: A rapid comparative analysis. RAND Corporation. 2013, 9 p.
16. Почуев С.И., Большаков В. П. Методический подход к решению задачи ранжирования степени угроз национальной безопасности // Информост, 2007, №6 (53), с.34–36.
17. Changwen Q., and You H. A method of threat assessment using multiple attribute decision making / Proc. of the 6th IEEE International Conference on Signal Processing, 2002, vol.2, pp.1091–1095.
18. Saaty T.L. The analytic hierarchy process. New York: McGraw-Hill, 1980, 287 p.
19. Saaty T.L. Decision making with dependence and feedback: The analytic network process. Pittsburgh: RWS Publications, 1996, 370 p.

20. Hwang C.L. and Yoon K. Multiple attribute decision making: Methods and applications, vol.186. New York: Springer, 1981, 259 p.
21. Opricovic S. Multicriteria optimization of civil engineering systems. PhD Thesis, Faculty of Civil Engineering, Belgrade, 1998, 302 p.
22. Gabus A. and Fontela E. The DEMATEL observer. Battelle Geneva Research Center, Geneva, Switzerland, 1976.
23. Roy B. and Bertier B. La méthode ELECTRE II: une méthodede classement en presence de critèresmultiples. Note de Travail 142, Groupe Metra, Direction Scientifique, 1971.
24. Brans J. P. and Vincke P. A preference ranking organisation method: the PROMETHEE method for MCDM // Management Science, 1985, vol.31, no.6, pp.647–656.
25. Zadeh L. A. Fuzzy sets // Information and Control, 1965, vol.8, no.3, pp.338–353.
26. Buckley J. J., Feuring T., and Hayashi Y., Fuzzy hierarchical analysis revisited // European Journal of Operational Research, 2001, vol.129, no.1, pp.48–64.
27. Torfi F., Farahani R. Z., and Rezapour S. Fuzzy AHP to determine the relative weights of evaluation criteria and Fuzzy TOPSIS to rank the alternatives // Applied Soft Computing, 2010, vol.10, no.2, pp.520–528.
28. Alguliyev R. M., Aliguliyev R. M., and Mahmudova R. S. Multicriteria personnel selection by the modified fuzzy VIKOR method // The Scientific World Journal, 2015, vol.2015, Article ID 612767, pp.1–16.
29. Büyüközkan G., and Çifçi G. A novel hybrid MCDM approach based on fuzzy DEMATEL, fuzzy ANP and fuzzy TOPSIS to evaluate green suppliers // Expert Systems with Applications, vol.39, no.3, pp.3000–3011.
30. Alguliyev R. M., Aliguliyev R. M., and Mahmudova R. S. A fuzzy TOPSIS+ Worst-case model for personnel evaluation using information culture criteria // International Journal of Operations Research and Information Systems, 2016, vol.7, no.4, pp.38–66.
31. Deng Y. A threat assessment model under uncertain environment // Mathematical Problems in Engineering, 2015, vol. 2015, Article ID 878024, 12 pages. http://dx.doi.org/10.1155/2015/878024
32. Ou Yang Y. P., Shieh H. M., Leu J. D., & Tzeng G. H. A VIKOR-based multiple criteria decision method for improving information security risk // International Journal of Information Technology & Decision Making, 2009, vol.8, no.2, pp.267–287.
33. Yang Y. P. O., Shieh H. M., & Tzeng, G. H. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment // Information Sciences, 2013, vol.232, pp.482–500.
34. Shameli-Sendi A., Shajari M., Hassanabadi M., Jabbarifar M., & Dagenais M. Fuzzy multi-criteria decision-making for information security risk assessment // The Open Cybernetics & Systemics Journal, 2012, vol.6, no.1, pp.26–37.
35. Syamsuddin I., and Hwang J. A new fuzzy MCDM framework to evaluate e-government security strategy / Proc. of the 4th International Conference on Application of Information and Communication Technologies, 2010, pp.1–5.
36. Yu L., and Lai K. K. A distance-based group decision-making methodology for multi-person multi-criteria emergency decision support // Decision Support Systems, 2011, vol.51, no.2, pp.307–315.
37. Alfares H.K., Duffuaa S.O. Determining aggregate criteria weights from criteria rankings by a group of decision makers // International Journal of Information Technology & Decision Making, 2008, vol.7, no.4, pp.769–781.
38. Cabrerizo F.J., Alonso S., Herrera-Viedma E. A consensus model for group decision making problems with unbalanced fuzzy linguistic information // International Journal of Information Technology & Decision Making, 2009, vol.8, no.1, pp.109–131.

39. Manmatha R., Rath T., and Feng F. Modeling score distributions for combining the outputs of search engines / Proc. of the 24th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, 2001, pp.267–275.
40. Van Erp M., and Schomaker L. Variants of the Borda count method for combining ranked classifier hypotheses / Proc. of the 7th International Workshop on Frontiers in Handwriting Recognition, 2000, pp.443–452.
41. Liu Y.-T., Liu T.-Y., Qin T., Ma Z.-M., and Li H. Supervised rank aggregation / Proc.of the 16th International Conference on World Wide Web, 2007, pp.481–490.
42. Klementiev A., Roth D., and Small K. An unsupervised learning algorithm for rank aggregation / Proc. of the European Conference on Machine Learning, 2007, pp.616–623.
43. Imamverdiyev Y. N. Consensus ranking method of information security threats of a nation state / II Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", 2017, pp.12–13.
44. Wang D., and Li T. Weighted consensus multi-document summarization // Information Processing & Management, 2012, vol.48, no.3, pp.513-523.
45. Duchi J., Shalev-Shwartz S., Singer Y., and Chandra T. Efficient projections onto the l_1-ball for learning in high dimensions / Proc. of the 25th International Conference on Machine Learning, 2008, pp.272–279.

УДК 004.056:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Метод консенсусного ранжирования угроз информационной безопасности электронного государства

Угрозы информационной безопасности электронного государства нацелены на национальные интересы в информационной сфере. Существует множество угроз национальным интересам в информационной сфере, и для эффективного противодействия этим угрозам в условиях ограниченных ресурсов, выделяемых на киберзащиту, необходимо многокритериальное ранжирование этих угроз. В предлагаемой модели угрозы ранжируются на основе экспертных оценок, которые характеризуют уровни угроз, нацеленных на национальные интересы. Предложена оптимизационная модель для консенсусного ранжирования угроз.

Ключевые слова: *электронное государство, информационная безопасность, угрозы информационной безопасности, оценка угроз, ранжирование угроз, консенсусное ранжирование.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

A consensus ranking method for information security threats of an e-government

Threats to information security of the e-government are aimed at national interests in the information sphere. There are many threats to national interests in the information sphere, and in order to effectively counter these threats in the face of limited resources allocated to cyber defense, multi-criteria ranking of these threats is necessary. In the proposed model, threats are ranked on the basis of expert assessments that characterize the levels of threats to national interests. An optimization model for consensus threat ranking is proposed.

Keywords: *e-government, information security, information security threats, threat assessment, threat ranking, consensus ranking.*